SAP NetWeaver Identity Management Installation Guide

SAP

Content

1 SAP NetWeaver Identity Management Installation Guide

This installation guide is the starting point for the installation of SAP NetWeaver Identity Management.

2   Identity Center Installation Overview

SAP NetWeaver Identity Management Identity Center is the primary component for identity management.

The Identity Center includes functions for identity provisioning, workflow, password management, logging and reporting. It uses a centralized repository, called the identity store, to provide a uniformed view of the data, regardless of the data's original source.

Architecture Overview

The architecture of the Identity Center is designed to provide maximum flexibility, scalability and security in a single software solution. This allows identity management across multiple applications and databases both within the organization and in an extranet environment. The Identity Center manages all of its activities from a core database and supports Microsoft SQL Server, Oracle and IBM DB2. All components in the solution interact with the database to ensure that all identity management activities are properly executed.
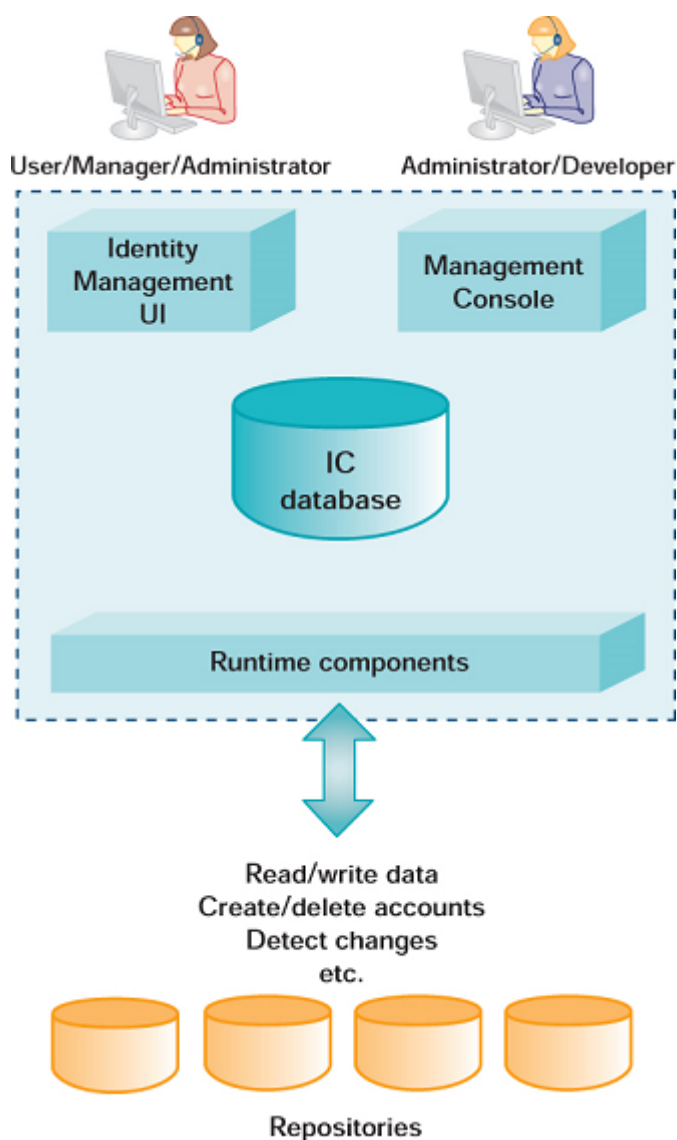
The Identity Center consists of the following components:

- **Identity Center Database**: All information about provisioning/workflow tasks and jobs, the identity store, scheduling information, state information and audit/logs is kept in this database.
- **Runtime Components**: The Runtime Components (dispatchers, runtime engines and event agents) act as local or remote agents for the Identity Center and are responsible for processing both provisioning and synchronization tasks. They are also responsible for performing reconciliation and bootstrapping. Event agents can be configured to take action based on changes in different types of repositories such as directory servers, message queues or others. This mechanism is optional and its only purpose is to initiate synchronization based on changes in repositories in addition to the scheduled operations.
- **Identity Management UI**: The Identity Management User Interface is used for all end-user registration/self service, password resets and approval of tasks. It also contains monitoring information for administrators of the Identity Center.
- **Management Console**: The administrator interface in the Microsoft Management Console is used for configuring the Identity Center, including provisioning/workflow tasks and jobs.

Licensing

There is no explicit license for SAP NetWeaver Identity Management. It depends on a licensed SAP NetWeaver, and contains functionality for license auditing using the LAW (License Administrator Workbench).

For more information about licensing, see the Related Information section.

Related Information

SAP Licenses
Global License Auditing Service

2.1 Installation Planning

This section contains information about the sizing criteria for the solution, some typical system landscapes and an overview of the installation process for each of the landscapes.

For sizing information see *SAP NetWeaver Identity Management Sizing Guide*.

How you upgrade an Identity Center from Identity Management 7.1 to 7.2 is described in the document *SAP NetWeaver Identity Management Migrating from Identity Management 7.1 to 7.2*.

For information about how you upgrade to a newer version of Identity Management 7.2, see *Upgrading an Identity Center*.

Related Information

2.1.1 Identity Center Components

In the description of the system landscapes, the following names are used to identify the different servers/components of the Identity Center.

Table 1:

Component	Name	Description
DB	Database server	The Identity Center database runs on this server.
MC	Management Console	This component is used for configuration of the Identity Center.
RT	Runtime Components	This can be one or more servers, where the Identity Center runtime engines are running.
UI	User Interface	The Identity Management User Interface runs on SAP NetWeaver AS Java.

2.1.2 System Landscapes

The system landscape for the Identity Center can look very different depending on the environment and the role of the installation.

The following landscapes are described:

- Small (S), Demo/development
- Medium (M), Test/QA
- Extra Large (XL), Production

Size S – Demo/development

This is the smallest possible scenario with all components installed on the same server:
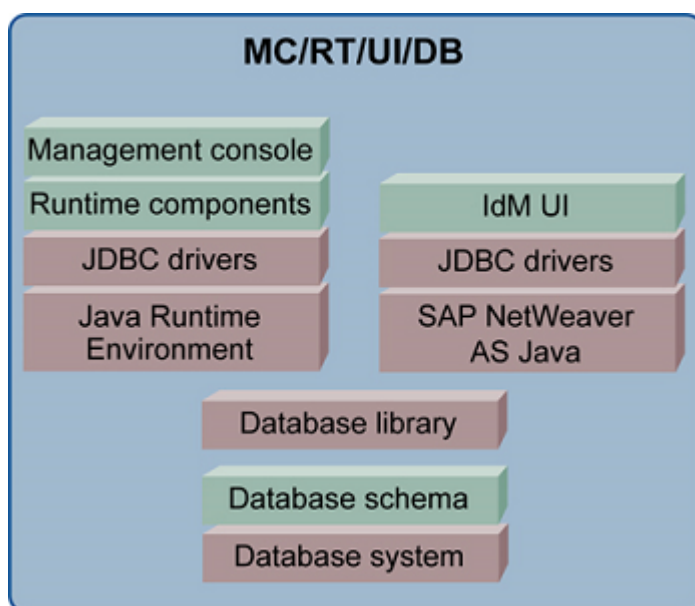
This configuration is ideal for demo, development and functional prototyping.

> **i Note**
>
> Depending on your environment, you may need more than one server. You are not able to use the same Oracle database for both SAP NetWeaver AS Java and the Identity Center. In that case this requires separate servers.
>
> If you run the Identity Center database on Oracle on a 64-bit system, while you are using a 32- bit Java Runtime Environment, those must run on separate servers.

Size M – Test/QA

In this scenario, each component is installed on a separate server:
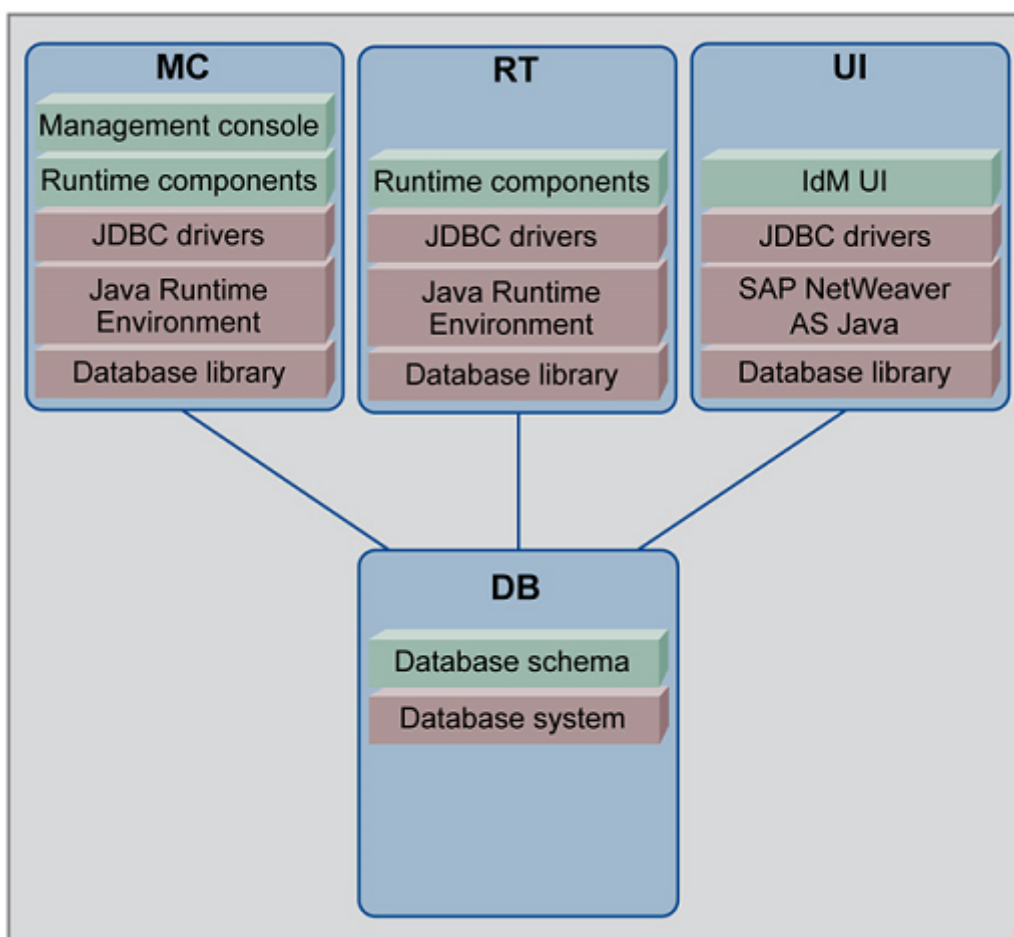
This scenario is used to set up a duplicate of the production environment, typically for testing and QA purposes. It has lower requirements on performance and availability. If desired, some of the components may be combined on the same server, for example Identity Management User Interface and Runtime Components.

Size XL – Production

This is a production system with high availability and high performance:
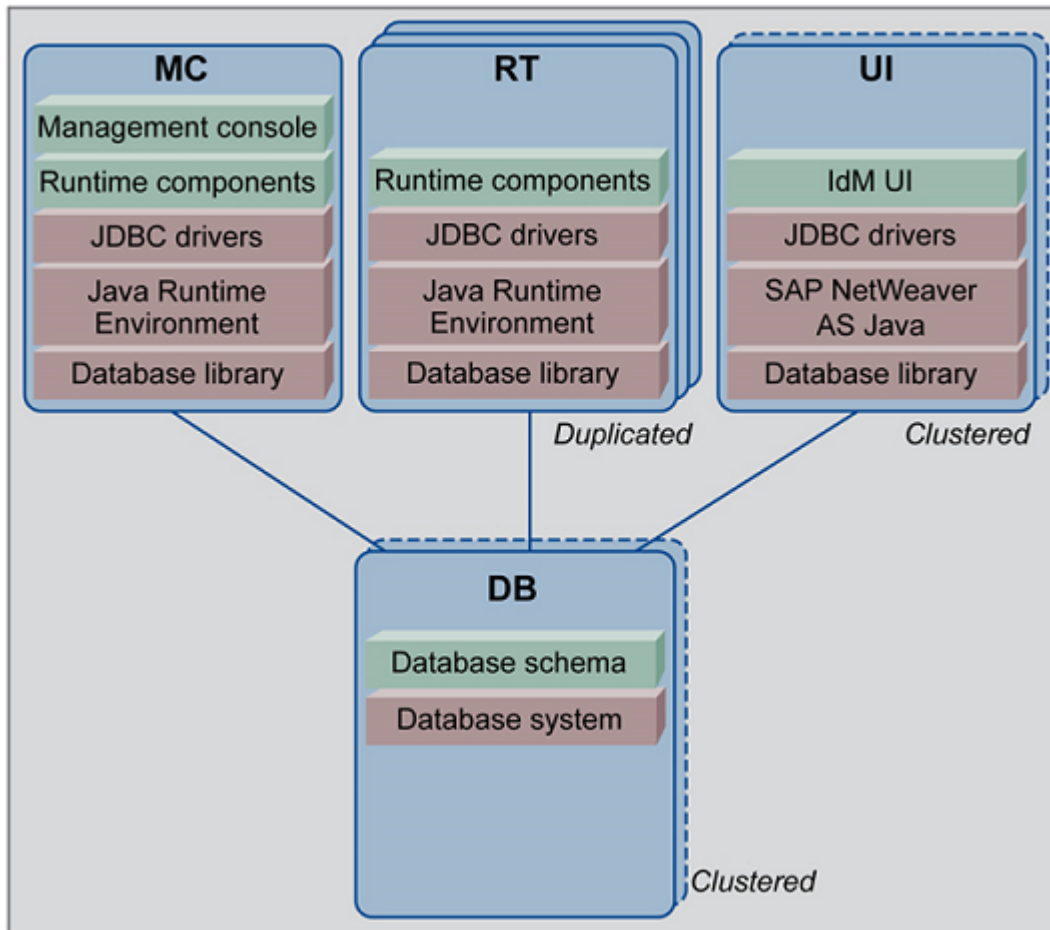
The components are installed on different servers, but in addition the servers are either clustered or duplicated.

The database server must be clustered to ensure high availability of the data.

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.

2.1.3 Overview of the Installation Process

The installation process involves the same steps, but depending on the system landscape, they will be performed on different servers. All installations assume that the operating system is already installed and that SAP NetWeaver AS Java is correctly installed and configured on the server running the Identity Management User Interface.

Related Information

2.1.3.1   Installation Process: S - Demo/development system

Context

The installation process of a Demo/development system (size S), consists of the following steps:

Procedure

1. Install the database system.
2. Install the Identity Center database schema.
3. Install the Java Runtime Environment.
4. Install the database client.
5. Install the JDBC drivers.
6. Install the Management Console.
7. Install the Runtime Components.
8. Install and configure SAP NetWeaver AS Java.
9. Install the Identity Management User Interface.

Next Steps

Post-installation: Configure the Java Runtime Environment.

Post-installation: Add the JDBC drivers to the CLASSPATH extension.

2.1.3.2   Installation Process: M - Test/QA System

Context

The installation process of a Test/QA System (size M), consists of the following steps:

Procedure

1. DB: Install the database system.
2. DB: Install the Identity Center database schema.
3. MC/RT: Install the Java Runtime Environment.
4. MC/RT/UI: Install the database client.
5. MC/RT/UI: Install the JDBC drivers
6. MC: Install the Management Console.
7. MC/RT: Install the Runtime Components.
8. UI: Install and configure SAP NetWeaver AS Java.
9. UI: Install the Identity Management User Interface

Next Steps

MC: Post-installation: Configure the Java Runtime Environment

MC/RT: Post-installation: Add the JDBC drivers to the CLASSPATH extension.

2.1.3.3 Installation Process: XL - Production System

Context

The installation process of a Production system (size XL), consists of the following steps:

Procedure

1. DB/UI: Prepare the environment for load balancing, high performance, clustered database and high availability as required.
2. DB: Install the database system as a clustered DB system.
3. MC/RT: Install the Java Runtime Environment.
4. DB: Install the Identity Center database schema.
5. MC/RT/UI: Install the database client on all cluster nodes.
6. MC/RT/UI: Install the JDBC drivers on all cluster nodes.
7. MC: Install the Management Console.
8. MC/RT: Install the Runtime Components on all cluster nodes.
9. UI: Install and configure SAP NetWeaver AS Java.
10. UI: Install the Identity Management User Interface.

Next Steps

MC: Post-installation: Configure the Java Runtime Environment on all cluster nodes.

MC/RT: Post-installation: Add the JDBC drivers to the CLASSPATH extension on all cluster nodes.

2.2 Installation Preparation

This section contains information about installation preparation.

Related Information

Installing the Database System [page 16]

2.2.1 Installing the Database System

SAP Identity Management supports the following database systems:

- Microsoft SQL Server
- Oracle
- IBM DB2

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

Microsoft SQL Server

The Identity Center supports the following versions of Microsoft SQL Server:

- Microsoft SQL Server 2005
- Microsoft SQL Server 2008
- Microsoft SQL Server 2012

> ⓘ Note
>
> Microsoft SQL Server 2005 Express Edition is not supported.

> ⓘ Note
>
> The collation used by the Identity Center database is SQL_Latin1_General_CP1_CI_AS. The default collation for Microsoft SQL Server is SQL_Latin1_General_CP850_BIN2# , and this should be changed before installing the Identity Center database. If the collations do not match, this may lead to performance problems with the Identity Center database.

Oracle

The Identity Center supports the following versions of Oracle:

- Oracle version 10.2

> ℹ **Note**
>
> SAP recommends using 10.2.0.2.

- Oracle version 11g Release 2
- Oracle version 12.1

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

For the database installation guides used with SAP systems, see *Installation & Upgrade Documentation*.

IBM DB2

The Identity Center supports the following versions of IBM DB2:

- IBM DB2 10.1 (and higher) for Linux, UNIX and Windows

The installation is available from the SAP Software Download Center on the SAP Support Portal. In the SAP Software Download Center, go to ▌▶ *Files for your Databases* ❭ *Databases* ❭.

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

For more information about IBM DB2, see *IBM DB2 database software*.

> ℹ **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.

Related Information

Installation & Upgrade Documentation
IBM DB2 database software

2.2.2 Installing the Database Client

The database libraries for the database system you are using must be installed on all servers.

Microsoft SQL Server Client Libraries

The client libraries for Microsoft SQL Server are included with the installation of the Designtime Components to be used by the Management Console (and the Windows Runtime Engine). It is not necessary to install them separately.

For other operating systems, see, for example *FreeTDS*.

Oracle Client

The Oracle client must be installed and correctly configured on all servers connecting to the Identity Center database. The client software is part of the Oracle database installation package.

> ### i Note
>
> If you are using Oracle as your database system, make sure to install the 32-bit version of the Oracle client if you run a 32-bit Java Virtual Machine on Microsoft Windows. This will be the case on the server running the Identity Center Management Console.

Oracle 11

For Oracle 11, the 32-bit client must be downloaded separately.

If you install the 32-bit and 64-bit client on the same server, remove the 32-bit client from PATH.

IBM DB2

The IBM DB2 database client is provided as a part of the database installation. Install the database client on all servers connecting to the database.

2.2.3 Installing the Java Runtime Environment

The Runtime Components of the Identity Center require a Java Virtual Machine. It must be installed on all the servers running one of the following components:

- Dispatcher
- Java runtime engine
- Event service and Event agent

It is recommended to use the SAP JVM, where versions 5.1 (Java 1.5) and 6.1 (Java 1.6) are required for the Runtime Components. Each version of SAP NetWeaver AS Java includes a SAP JVM:

Table 2:

SAP NetWeaver AS Java	Java Virtual Machine
SAP NetWeaver AS Java 7.0	4.1 (Java 1.4) In addition, servers running one of the above mentioned components require Java Virtual Machine 5.1 (Java 1.5) or 6.1 (Java 1.6).
EhP1 for SAP NetWeaver Composition Environment 7.1	5.1 (Java 1.5)
SAP NetWeaver Composition Environment 7.2	6.1 (Java 1.6)
SAP NetWeaver 7.3	6.1 (Java 1.6)
EhP1 for SAP NetWeaver 7.3	6.1 (Java 1.6)
SAP NetWeaver 7.4	6.1 (Java 1.6)

The SAP Note 1442124 gives an overview of how to download the SAP JVM separately.

> **i Note**
>
> The SAP Note 1367498 gives an overview of the installation prerequisites for the SAP JVM. Make sure you install the mentioned Microsoft libraries.

> **i 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.

> **i Note**
>
> SAP NetWeaver AS Java 7.0 is not supported when using IBM DB2 as the database system.

To configure the Java Runtime Environment for the Management Console, see *Configuring the Java Runtime Environment*.

To configure the Java Runtime Environment for the Runtime Components, see *SAP NetWeaver Identity Management Identity Center Initial Configuration*.

Java Cryptographic Extension Jurisdiction Policy Files

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

2.2.4 Installing the JDBC Drivers

The JDBC drivers are used by the Runtime Components to access databases, both the Identity Center database and other data sources that are accessed via JDBC.

The SAP NetWeaver AS Java running the Identity Management User Interface needs the JDBC driver to access the Identity Center database.

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

- Runtime Components
  - Dispatcher (JDBC driver to the Identity Center database)
  - IC Java runtime engine (JDBC driver(s) to the Identity Center database and any databases/data sources that are accessed)
  - Event service and event agent (JDBC driver(s) to the Identity Center database and any databases/data sources that are accessed)
- Management Console (needed for import/export)
- Identity Management User Interface (JDBC driver to the Identity Center database)

Related Information

2.2.4.1 Microsoft SQL Server JDBC Driver

The JDBC drivers can be downloaded from *Microsoft SQL Server Web Page*.

Which JDBC driver you should use (the recommended JDBC driver versions) depends on which version of Java you are using and which version of Microsoft SQL Server you are running:

Table 3:

Database version	Version of Java Runtime Environment		
	SAP JVM 4.1 (Java 1.4)	SAP JVM 5.1 (Java 1.5)	SAP JVM 6.1 (Java 1.6)
Microsoft SQL Server 2005/32-bit	JDBC 1.2	JDBC 1.2	JDBC 1.2
Microsoft SQL Server 2005/64-bit	JDBC 1.2	JDBC 1.2	JDBC 1.2
Microsoft SQL Server 2008/64-bit	JDBC 1.2	JDBC 3.0	JDBC 4.0
Microsoft SQL Server 2012/64-bit	JDBC 1.2	JDBC 3.0	JDBC 4.0

> **i Note**
>
> For Java Virtual Machine version 4.1 (Java 1.4) you should use JDBC 1.2 for all supported Microsoft SQL Server databases.

JDBC driver 1.2

Given the release of the Microsoft SQL Server JDBC Driver 3.0, the Microsoft SQL Server JDBC team has discontinued the download for Microsoft SQL Server JDBC Driver 1.2. Support for the JDBC 1.2 driver ended in June 25, 2011.

SAP still supports and you can download the JDBC 1.2 driver from the SAP Support Portal.

The recommended procedure for installing is described in the file `install.txt`, which is part of the download. The major steps are repeated here:

1. Download the `sqljdbc_1.2<version>.exe` file to a temporary location.
2. Install the JDBC driver by running this self-extracting archive, and enter an install directory. It is recommended to store this in the directory: `C:\Program Files\Microsoft SQL Server 2005 JDBC Driver`.
   The JDBC driver is: `com.microsoft.sqlserver.jdbc.SQLServerDriver`.
3. The CLASSPATH must be set to the following file (assuming that the drivers were extracted to the default location as shown above): `C:\Program Files\Microsoft SQL Server 2005 JDBC Driver \sqljdbc_1.2\enu\sqljdbc.jar`

   > **i Note**
   >
   > It is not recommended to use JDBC driver1.2 for the dispatcher transferring data to Business Warehouse, especially for the initial data transfer. For details, see SAP Note 1586820 .

JDBC driver 3

The JDBC driver for Microsoft SQL Server 2008 and Microsoft SQL Server 2012 can be downloaded here: *Microsoft SQL Server JDBC Driver 3.0* . Follow the installation instructions on that page.

It is recommended to install the JDBC driver to: `C:\Program Files\Microsoft SQL Server JDBC Driver 3.0`.

The JDBC driver name is: `com.microsoft.sqlserver.jdbc.SQLServerDriver`.

There are two `.jar` files included with the installation:

- `sqljdbc.jar` is the JDBC 3.0 driver that should be used with Java 1.5 installations (SAP JVM 5.1).
- `sqljdbc4.jar` is the JDBC 4.0 driver that should be used with Java 1.6 installations (SAP JVM 6.1).

The CLASSPATH must be set to the correct file: `C:\Program Files\Microsoft SQL Server JDBC Driver 3.0\sqljdbc_3.0\enu\sqljdbc.jar` or `C:\Program Files\Microsoft SQL Server JDBC Driver 3.0\sqljdbc_3.0\enu\sqljdbc4.jar`.

For more information, see *System Requirements for the JDBC Driver*.

Related Information

Microsoft SQL Server Web Page
Microsoft SQL Server JDBC Driver 3.0
System Requirements for the JDBC Driver

2.2.4.2 Oracle JDBC Driver

Oracle 10

The Oracle version 10 JDBC drivers (ojdbc14.jar) can be downloaded from *Oracle Web Site*. Download and install this according to the installation description. Make sure the file is in CLASSPATH.

Oracle 11

For Oracle 11, you use the following JDBC drivers:

Table 4:

SAP JVM 4.1/5.1 (Java 1.4/1.5)	SAP JVM 6.1 (Java 1.6)
SAP NetWeaver 7.0 (SAP JVM 4.1/Java 1.4)	SAP NetWeaver Composition Environment 7.2
EhP1 for SAP NetWeaver Composition Environment 7.1 (SAP JVM 5.1/Java 1.5)	SAP NetWeaver 7.3
	EhP1 for SAP NetWeaver 7.3
	SAP NetWeaver 7.4
`ojdbc14.jar`	`ojdbc6.jar`

`ojdbc6.jar` is included with Oracle 11. Install the JDBC driver according to the installation description.

Related Information

[Oracle Web Site](#) ↪

2.2.4.3 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\`
- Unix: `/opt/ibm/db2/V10.1/java` where `/opt/ibm/db2/V10.1/` is where IBM DB2 is installed.

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.

2.2.4.4 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 by the vendor of the database or other data source.

2.2.5 Installing SAP NetWeaver AS Java

Install one of the following versions of SAP NetWeaver AS Java on all servers that are going to host the Identity Management User Interface.

- SAP NetWeaver AS Java as of Release 7.0 SP14 or higher
- Enhancement Package 1 for SAP NetWeaver Composition Environment 7.1
- SAP NetWeaver Composition Environment 7.2
- SAP NetWeaver 7.3
- Enhancement Package 1 for SAP NetWeaver 7.3
- SAP NetWeaver 7.4

> ℹ **Note**
>
> Some of the upcoming enhancements may only be available on EhP1 for NW CE 7.1, SAP NetWeaver 7.2 or later, as they utilize new capabilities of the underlying technology

Related Information

Installation Information for SAP NetWeaver 7.0
SAP NetWeaver CE 7.1 Including Enhancement Package 1
SAP NetWeaver CE 7.2
SAP NetWeaver 7.3 Including Enhancement Package 1
SAP NetWeaver 7.4

2.3 Installation

The Identity Center consists of three separate downloads on the download area of SAP NetWeaver Identity Management 7.2 on SAP Support Portal.

- Designtime components
- Runtime Components
- User Interface

> ℹ **Note**
>
> Make sure that all necessary prerequisites are present before installing each of the Identity Center components.

Designtime Components

The designtime components consist of the following modules:

- Identity Center database schema (Microsoft SQL Server/Oracle/IBM DB2)
- Management Console

- Microsoft Active Directory Password hook

For details, see the following sections in the *SAP NetWeaver Identity Management Installation Guide*:

- *Installing the Identity Center Database on MS SQL Server*
- *Installing the Identity Center Database on Oracle*
- *Installing the Identity Center Database on IBM DB2*
- *Installing the Management Console*
- *SAP NetWeaver Identity Management Password Hook Configuration Guide*

Runtime Components

For details, see *Installing the Identity Center Runtime Components*

> ℹ **Note**
>
> If the Runtime Components are installed on the same system as the Management Console, they must be installed to the same folder.

Identity Management User Interface

For details, see *Installing and Configuring the Identity Management User Interface*.

2.4   Post-Installation

This section contains information about post-installation steps.

Related Information

2.4.1 Configuring the Java Runtime Environment

The Java Runtime Environment must be configured both for the Management Console and the Runtime Components.

Management Console

After the installation you must configure the Java Runtime Environment for the Management Console. Specify which Java Runtime Environment the Management Console should use:

1. Choose ▌ *Tools* ❭ *Options* ▌ to open the *Options* dialog box:
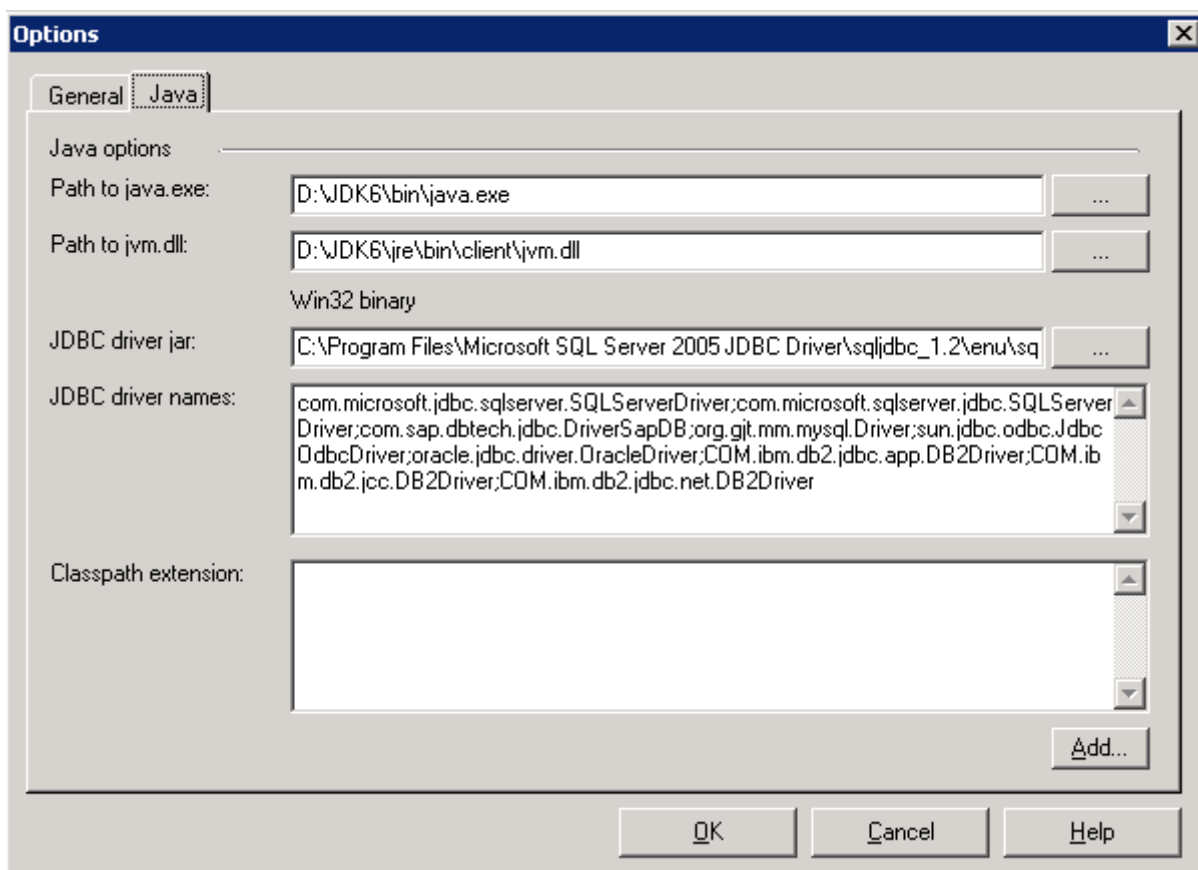
Fill in the fields *Path to java.exe* and *Path to jvm.dll*.

> **ℹ Note**
>
> Make sure that you choose `java.exe` and `jvm.dll` from the same Java version.

You will see whether you have chosen a 32-bit or 64-bit Java version below the field.

2. Choose *OK*.

Runtime Components

To configure the Java Runtime Environment for the Runtime Components, see *SAP NetWeaver Identity Management Identity Center Initial Configuration*.

2.4.2 Adding JDBC Driver(s) and Libraries

JDBC driver(s) to the databases (or other data sources) that the Runtime Components will access must be available on all servers with the Runtime Components as described in Installing the JDBC drivers.

Adding the JDBC Driver for the Dispatcher(s)

The dispatcher only needs JDBC driver to the Identity Center database, so to avoid that the dispatcher needs to load all JDBC drivers and libraries added to the CLASSPATH extension, you can add this separately:

1. Choose ▎ *Tools* ❯ *Options* ▎ and select the *Java* tab.
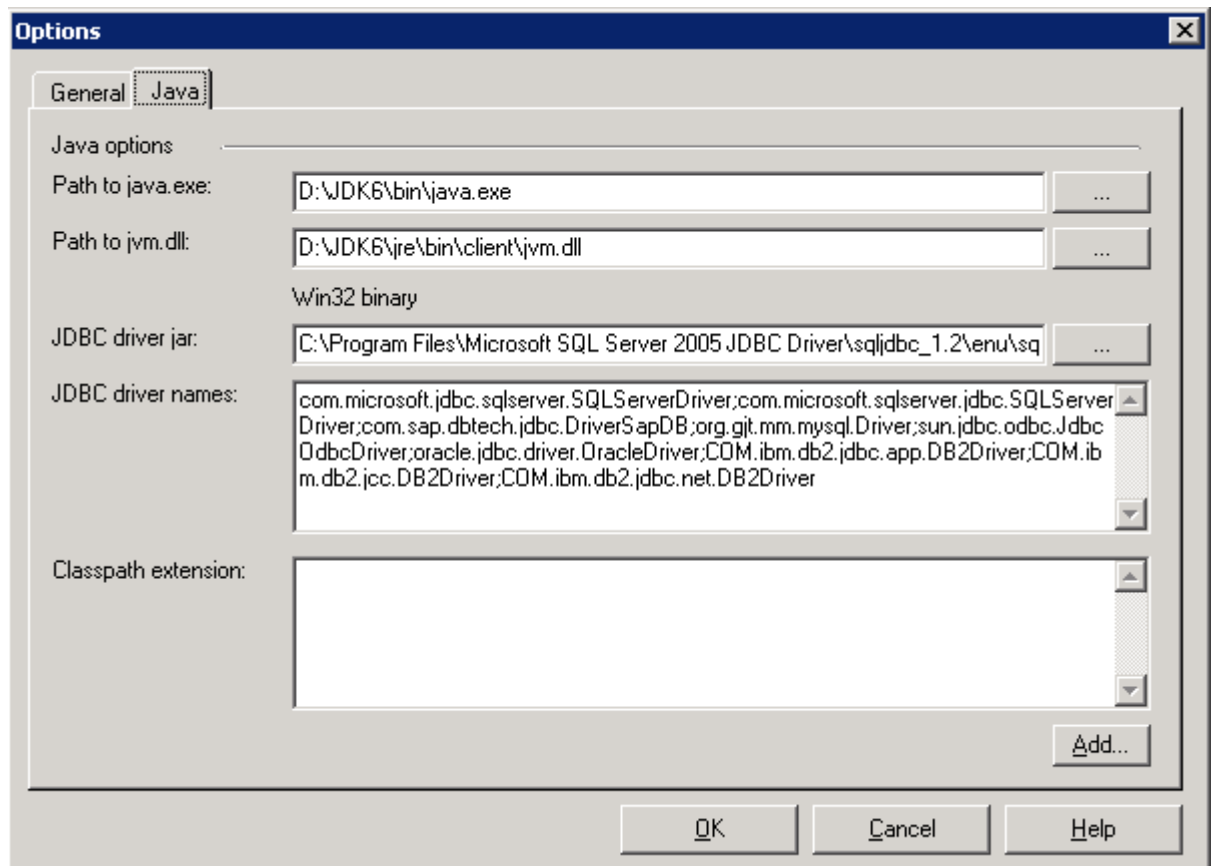
Add the JDBC driver to the Identity Center database in the *JDBC driver jar* field.
2. Choose *OK*. You will be asked to regenerate the dispatcher scripts.

Adding the JDBC Drivers and Libraries for the Runtime Engine

The JDBC drivers and other libraries required by the runtime engine must be added to the CLASSPATH extension. How this can be done depends on the environment:

- If the Management Console is installed on the same server, you can use the following methods:
  - Choose ▶ *Tools* ❯ *Options* ❯ and add the JDBC driver to the Identity Center's CLASSPATH extension.
  - Add the JDBC driver to the CLASSPATH environment variable.
- If only the Runtime Components are installed on the server, you must add the JDBC driver to the CLASSPATH environment variable.

Related Information

2.5 Updating an Identity Center

> ℹ Note
>
> How you upgrade an Identity Center from Identity Management 7.0 to 7.1 is described in the document *SAP NetWeaver Identity Management Identity Center Installation Overview* for version 7.1.

> ℹ Note
>
> How you upgrade an Identity Center from Identity Management 7.1 to 7.2 is described in the document *SAP NetWeaver Identity Management Migrating from Identity Management 7.1 to 7.2*.

To update an Identity Center 7.2 to a newer version of 7.2, each of the components must be updated. This also applies to updating to a Service Pack (SP), which involves updating all components.

Related Information

2.5.1 Updating Demo/Development or Test/QA (Size S or M) Environment

Context

Perform the update in the following sequence:

Procedure

1. Update the database schema.
2. Update the Management Console.
3. Update the Runtime Components.
4. Update the Identity Management User Interface.

   The update procedure for each component is described in the component's installation description.

2.5.2 Updating Production Environment

Context

When updating a production environment with high availability requirements, do as follows:

Procedure

1. Remove the access to the Identity Management User Interface.
2. Stop dispatchers and event services.
3. Back up your system.
4. Update the database schema.
5. Update the Identity Management User Interface.
6. Provide access to the Identity Management User Interface.
7. Update the Management Console.
8. Update the Runtime Components.

9. (Optionally) Update the Windows runtime engine.

10. Start the dispatchers and event services.

    The update procedure for each component is described in the component's installation description.

3 Installing the Management Console

This document describes how to install the Management Console of the Identity Center.

> ℹ **Note**
>
> If the Management Components are to be installed on the same server as the Runtime Components, make sure that they are installed to the same directory.

> ℹ **Note**
>
> If you upgrade from Identity Center 7.1 to 7.2, note that the installation path has changed. Please see the document *SAP NetWeaver Identity Management Migration guide – Identity Management 7.1 to 7.2* for details.

Prerequisites

Before you can install the Management Console, make sure that the following prerequisites are present:

- Database client

  > ℹ **Note**
  >
  > If you are using Oracle as your database system, make sure to install the 32-bit version of the Oracle client if you run a 32-bit Java Virtual Machine. The Management Console requires a 32-bit version of the database client. Use "Oracle provider for OLE DB" when configuring the connection from the Management Console to the database.

- Java Runtime Environment (Runtime Components)

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

- JDBC driver for the Identity Center database (Runtime Components)
- Any JDBC drivers or other connectivity software needed to access the data sources (Runtime Components)

The prerequisites are described in detail in the *Identity Center Installation Overview* section.

Related Information

Identity Center Installation Overview [page 7]

3.1 Installing the Management Console

Context

To install the Management Console, proceed as follows:

Procedure

1. Navigate to the download area of SAP NetWeaver Identity Management 7.2 on SAP Support Portal and download the installation kit for *Identity Center Designtime*.
2. Unpack the installation kit.
3. Run the file `setup.exe` located in the /setup folder.
4. The wizard leads you through the installation. Keep the default values or enter values specific for your installation.

   When the installation is completed you may need to restart your computer.

3.2 Updating the Management Console

Context

> **i Note**
>
> If you upgrade from Identity Center 7.1 to 7.2, note that the installation path has changed. Please see the document *SAP NetWeaver Identity Management Migration guide – Identity Management 7.1 to 7.2* for details.

> **i Note**
>
> If you are upgrading from a previous version, it is recommended to uninstall before installing the new version.
>
> Before you install a new version, it is important that the Management Console is closed.

To update the Management Console, proceed as follows:

Procedure

1. Run the installation job as described in *Installing the Management Console*.
2. After the update, a restart may be required.

Related Information

[Installing the Management Console [page 32]](#)

4   Installing the Identity Center Runtime Components

This section describes how to install the Runtime Components of the Identity Center.

The Runtime Components can either be installed on Microsoft Windows or on a Unix platform. There are separate descriptions for Microsoft Windows and Unix. On Unix you also need to adapt the configuration files that are used by the Runtime Components.

For information about how you configure the Runtime Components to run jobs, see *SAP NetWeaver Identity Management Identity Center Initial Configuration*.

> **i Note**
>
> If the Runtime Components are to be installed on the same server as the Management Console, make sure that they are installed to the same directory.

> **i Note**
>
> If you upgrade from Identity Center 7.1 to 7.2, note that the installation path has changed. Please see the document *SAP NetWeaver Identity Management Migration guide – Identity Management 7.1 to 7.2* for details.

Prerequisites

Before you can install the Runtime Components, make sure that the following prerequisites are present:

- Database libraries

  > **i Note**
  >
  > If you are using Oracle as your database system, make sure to install the 32-bit version of the Oracle client if you run a 32-bit Java Virtual Machine on Microsoft Windows.

- Java Runtime Environment

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

- JDBC driver for the Identity Center database
- Any JDBC drivers or other connectivity software needed to access the data sources (Runtime Components)
- The installer needs a Java VM to run.

> **i Note**
>
> If you have only SAP JVM installed on the system, you must add the \bin folder in the installation directory to the PATH environment variable, for instance c:\usr\sap\sapjvm_5\bin.

The prerequisites are described in detail in *Identity Center Installation Overview* section.

Related Information

4.1   Using the SAP Java Connector (JCo)

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

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

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

Related Information

4.1.1 Installing Additional Microsoft runtime DLLs for the SAP Java Connector (JCo)

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

These 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.

4.1.2 Updating the SAP Java Connector (JCo)

Context

To update the SAP Java Connector from 2.x to 3.x, proceed as follows:

Procedure

1. Download the JCo from the SAP Service Marketplace at `http://service.sap.com/connectors` under
   SAP Java Connector > *Tools & Services* .
2. Unpack the relevant SAP JCo 3.x zip file.
3. Stop all dispatchers.
4. Replace the Jco-related dll, jar, and (if available) pdb files of your installation located, for example, in
   `<DRIVE>:\usr\sap\IdM\Identity Center\Java` with the new files contained in the root directory of the downloaded archive.
5. Start all dispatchers again.

4.2   Installing the Runtime Components on Microsoft Windows

Context

To install the Runtime Components on Microsoft Windows, proceed as follows:

Procedure

1. Navigate to the download area of SAP NetWeaver Identity Management 7.2 on SAP Support Portal and download the installation kit for *Identity Center Runtime*.
2. Unpack the installation kit.
3. Run the file install.exe located in the `/RuntimeComponents\Setup\CDROM_Installers\Windows\Disk1\InstData\NoVM` 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.

   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, for instance: `install.exe LAX_VM c:\usr\sap\sapjvm_5\bin\java.exe`

4.3   Installing the Runtime Components on a Unix Platform

Context

> ⓘ Note
>
> A graphical environment (X) is required on the Unix system.

To import the Runtime Components on a Unix Platform, proceed as follows:

Procedure

1. The Identity Center installation kit contains installers for several Unix platforms in sub-folders of the `\RuntimeComponents\Setup\CDROM_Installers` folder. Copy the folder corresponding to your Unix platform to the Unix server where you want to perform the installation.

   > ℹ **Note**
   >
   > Make sure to transfer the files as Binary.

2. Log in as root on the Unix system and navigate to the folder where you copied the installation files.
3. Make the install.bin file located in the folder `\<platform>\Disk1\InstData\NoVM` executable.
4. Set JAVA_HOME to point to the Java Runtime Environment (recommended SAP JVM 5).
5. Run the installer `install.bin`. The wizard leads you through the installation. Keep the default values or enter values specific for your installation. The default installation path is `/opt/sap/idm/identity center`. You can remove the space to avoid a path containing space.

   For information about how to configure the runtime environment, see the document *SAP NetWeaver Identity Management Identity Center Initial Configuration*.

4.4   Updating the Runtime Components

> ℹ **Note**
>
> If you upgrade from Identity Center 7.1 to 7.2, note that the installation path has changed. Please see the document *SAP NetWeaver Identity Management Migration guide – Identity Management 7.1 to 7.2* for details.

> ℹ **Note**
>
> Before you install a new version, it is important that any services (dispatchers/event agents) are stopped.

An update is performed by running the installation job as described in *Installing the Runtime Components on Microsoft Windows* and *Installing the Runtime Components on Unix*. After the update, you may be prompted to restart the server. This will be the case if any services were running while you performed the update.

Related Information

Installing the Runtime Components on Microsoft Windows [page 37]

5 Installing the Identity Center Database

This section describes how to install an Identity Center database on the supported database systems.

SAP NetWeaver Identity Management supports the following database systems:

* Microsoft SQL Server
* Oracle
* IBM DB2

Choose the installation description that corresponds to your database system.

5.1 Installing the Identity Center Database on MS SQL Server

This section describes how you install, upgrade and remove an Identity Center database on MS SQL Server.

The following description uses the variable `<prefix>` to indicate that the database name can be modified for each installation. The default prefix is `mxmc`. If you want several Identity Center databases within the same SQL Server, each Identity Center database must have a different `<prefix>`. For details, see *Installing the Identity Center Database with a Given Prefix*.

Make sure the necessary configuration is done on the server running the database. See *Configuring Microsoft SQL Server* for details.

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

5.1.1 Database Script Files

The script files are included in the installation kit for *Identity Center Designtime*.

Context

To locate the script files, proceed as follows:

Procedure

1. Navigate to the download area of SAP NetWeaver Identity Management 7.2 on SAP Support Portal and download the installation kit for *Identity Center Designtime*.
2. Unpack the installation kit.
3. The script files are located in the `/Database/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.

The following scripts are used to install, upgrade or remove the Identity Center database:

Table 5:

Script	Description	Account (run as)
`mxmc-install.cmd`	Creates an Identity Center database. Calls the script `mxmc-xinstall.cmd` with default values for database prefix, host name and user name (`sa`).	The script prompts for the password for `sa` and the passwords for the database users created during the installation.
`mxmc-update.cmd`	Updates an Identity Center database. Calls the script `mxmc-xupdate.cmd` with default values for database prefix, host name and user name `mxmc_oper`.	The script prompts for the password for the `mxmc_oper` user.
`mxmc-remove.cmd`	Removes an Identity Center 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	Account (run as)
`mxmc-xinstall.cmd`	Creates an Identity Center 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.
`mxmc-xupdate.cmd`	Updates an Identity Center with a given prefix. Requires the parameters database prefix, host name, user name `<Prefix>_oper`) and password.	Runs as `<prefix>_oper`. Run the script without parameters to see what is required.
`mxmc-xremove.cmd`	Removes an Identity Center database with a given prefix. Requires the parameters database prefix, host name, user name (`sa`) and password.	Runs as `sa`. Run the script without parameters to see what is required.
`mxmc-versions.cmd`	Lists all databases installed on the given server. For Identity Center databases, version information is included. Requires the parameters host name, user name (`sa`) and password.	Runs as `sa`. Run the script without parameters to see what is required.

> ℹ **Note**
>
> Microsoft SQL Server 2008 and higher enforces the password policy of the Microsoft Windows domain. This may restrict which passwords are accepted.

When you have run one of the scripts, a log file is created. The name of the log file is `<prefix>_logfile.log`.

5.1.2 Database Roles and Users

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

Table 6:

Role	Description	Login
`db_owner`	This role is allowed to change the table structure of the Identity Center database.	`<prefix>_oper`

Role	Description	Login

`<prefix>_admin_role`	This role is assigned to the administrator of the Identity Center. This role is allowed to change all information within the Identity Center, and execute the necessary procedures for creating jobs and groups, and maintaining these.	`<prefix>_oper`
		
		`<prefix>_admin`

`<prefix>_user_role`	This role can view jobs and groups within the Identity Center, but is not allowed to change any information, except scheduling information.	`<prefix>_oper`
		
		`<prefix>_user`

`<prefix>_rt_role`	This role is used by the runtime engine, and functionality is limited to table and procedure access necessary for the runtime engine.	`<prefix>_oper`
		
		`<prefix>_rt`

`<prefix>_prov_role`	This role can be used by other systems giving input to the provisioning module of the Identity Center. This role is used as login for the Identity Management User Interface.	`<prefix>_prov`
`<prefix>_transport_role`	This role is used to provide access to performing an export or import of a configuration in the Administration User Interface.	`<prefix>_prov`

5.1.2.1 Creating Additional Logins

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

Make sure you assign correct roles to the logins.

> ### i Note
>
> If you want to add logins after the Identity Center database is installed, this can be done using the database's administrative tools. Make sure you assign the correct roles.

5.1.3 Configuring 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. The collation used by the Identity Center database is SQL_Latin1_General_CP1_CI_AS.

Even if running the server with SQL_Latin1_General_CP850_BIN2, the Identity Center database will use the collation SQL_Latin1_General_CP1_CI_AS.

Mixed mode security

Logging on using the accounts listed in the table above requires that the Microsoft SQL Server supports *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.

> **i 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 enable the sa user and set a password in the SQL Server Management Studio.

TCP/IP connection

In Microsoft SQL Server 2005 TCP/IP may initially not be enabled. If not already enabled, this has to be done manually.

This is done in the computer management (My computer/Manage...). Locate the "Protocols for MSSQLSERVER" (as shown below), and enable the TCP/IP protocol.

After this is done, the Microsoft SQL Server must be restarted.
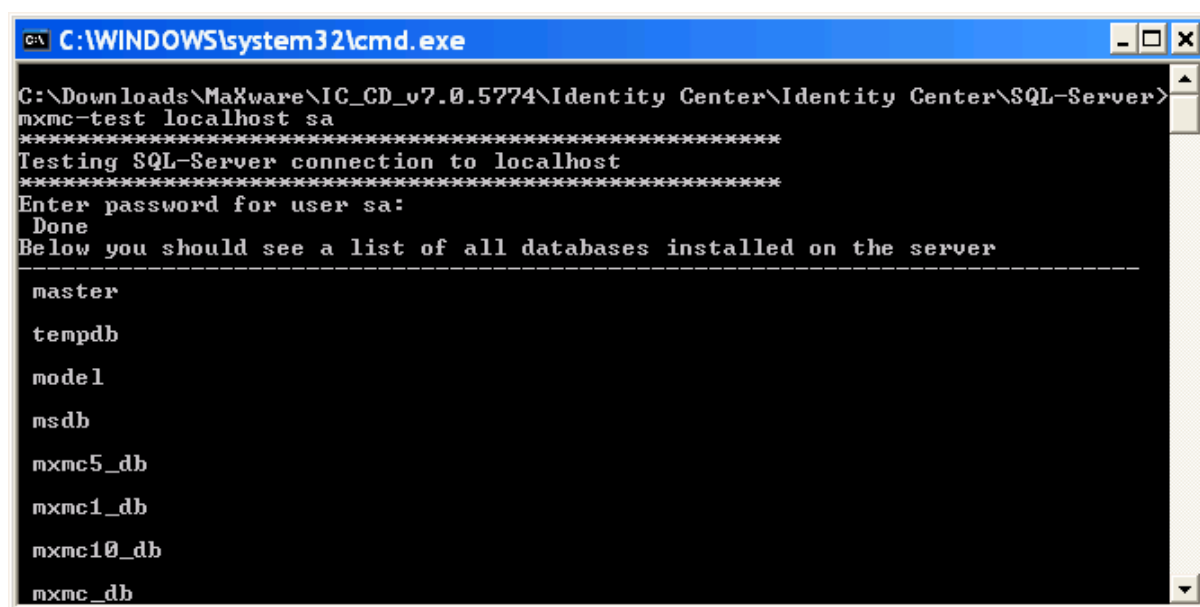
5.1.4 Testing the Database Connection

Context

You can verify that you are able to connect to the database where you want to install the Identity Center database.

Procedure

1. Open a command prompt and navigate to the directory where the database installation scripts are located.
2. Run the command file `mxmc-test.cmd`. The command file requires the following parameters:
   - Host name of the computer running the SQL Server
   - User name for the `sa` account
   - (Optionally) Password for this account.

   If you do not specify the password on the command line, you are prompted for it when you run the command file.
3. The result of the command file is a list of available databases or an error message. If you receive an error message, there is a problem with your database installation or configuration, and the Identity Center database installation scripts will not be able to access the database. You need to correct the problem before you continue. Please see the SQL Server documentation for details.

5.1.5 Installing the Identity Center Database

Context

The Identity Center database is installed by running a command file that calls the necessary script files in the specified sequence.
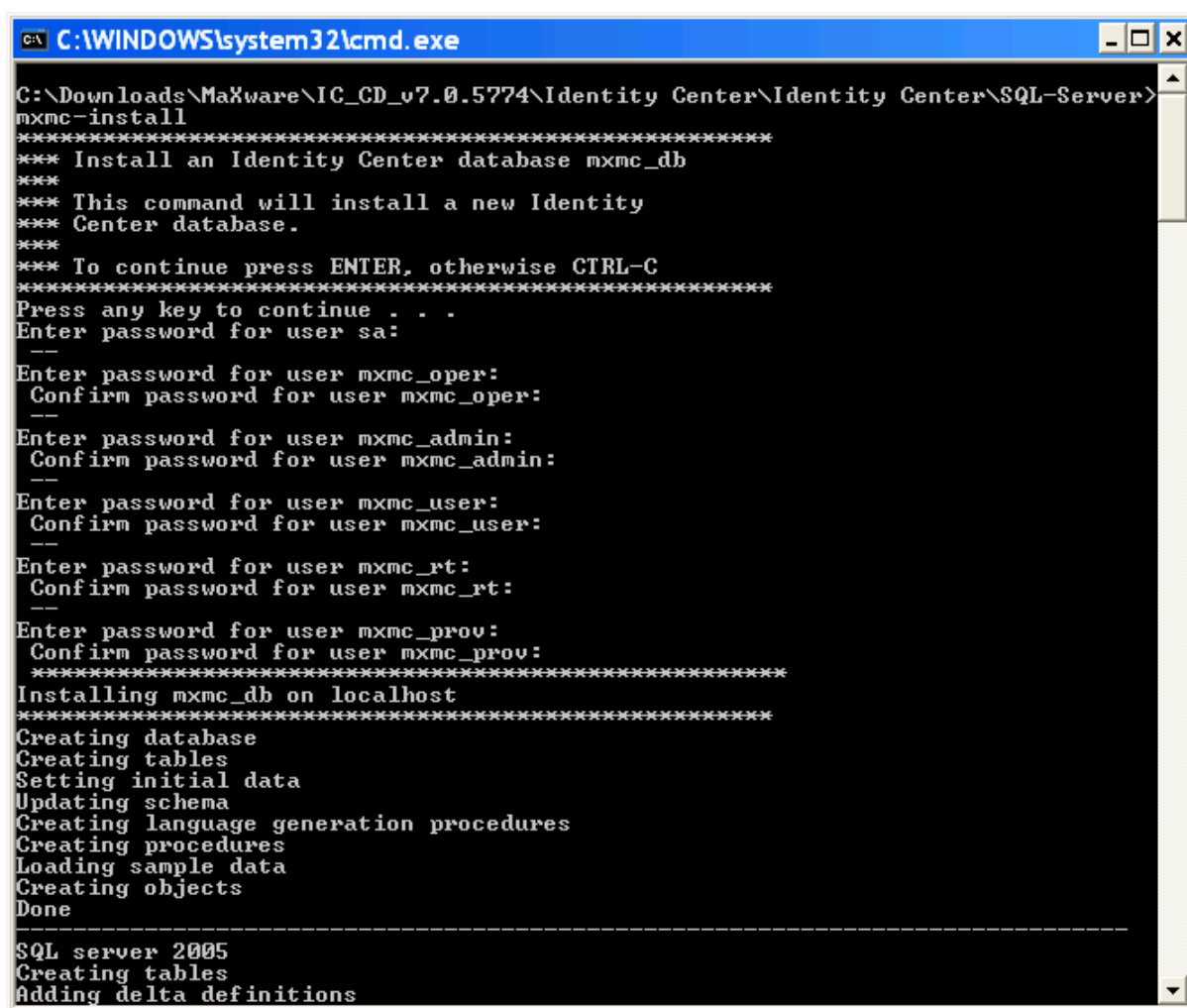
Procedure

1. Open a command prompt and navigate to the directory where the script files are located.

   > **i Note**
   >
   > Do not run the scripts directly from Microsoft Windows Explorer.

2. Run the command file `mxmc-install.cmd`.

```
C:\WINDOWS\system32\cmd.exe                                          _ □ ×

C:\Downloads\MaXware\IC_CD_v7.0.5774\Identity Center\Identity Center\SQL-Server>
mxmc-install
*************************************************************
*** Install an Identity Center database mxmc_db
***
*** This command will install a new Identity
*** Center database.
***
*** To continue press ENTER, otherwise CTRL-C
*************************************************************
Press any key to continue . . .
Enter password for user sa:
--
Enter password for user mxmc_oper:
 Confirm password for user mxmc_oper:
--
Enter password for user mxmc_admin:
 Confirm password for user mxmc_admin:
--
Enter password for user mxmc_user:
 Confirm password for user mxmc_user:
--
Enter password for user mxmc_rt:
 Confirm password for user mxmc_rt:
--
Enter password for user mxmc_prov:
 Confirm password for user mxmc_prov:
*************************************************************
Installing mxmc_db on localhost
*************************************************************
Creating database
Creating tables
Setting initial data
Updating schema
Creating language generation procedures
Creating procedures
Loading sample data
Creating objects
Done
-------------------------------------------------------------
SQL server 2005
Creating tables
Adding delta definitions
```

You are prompted for the password for `sa`.

You are also prompted for the password for all logins created by the Identity Center installation scripts. You must confirm all passwords to ensure that you do not accidentally enter the wrong password.

When the file completes without error messages, the database is installed correctly. You can also check the log file `<prefix>_logfile.log`.

3. Close the command prompt window.

Results

The database is now installed and ready for use by the Identity Center. See *Installing the Management Console* and *Identity Center Installation Overview* for more information.

Related Information

Identity Center Installation Overview [page 7]
Installing the Management Console [page 31]

5.1.6 Installing the Identity Center Database with a Given Prefix

You may want to install more than one Identity Center on the same SQL Server.

Context

In this case, you must replace the prefix `MXMC_` with another value. This prefix is also prepended to the logins, users and role names. You can do this by running the command file `mxmc-xinstall.cmd`.

Procedure

1. Open a command prompt and navigate to the directory where the script files are located.
2. Run the command file mxmc-xinstall.cmd. The parameters to the command file are:
   ○ Prefix
   ○ Host name of the computer running the SQL Server
   ○ User name for the sa account

- Password for sa
- Password for <prefix>_oper
- Password for <prefix>_admin
- Password for <prefix>_user
- Password for <prefix>_rt
- Password for <prefix>_prov

3. Close the command prompt window.

   Start the Identity Center configuration interface and add an Identity Center configuration for the database. See the Identity Center help file for details.

5.1.7 Updating the Identity Center Database

Context

> ℹ **Note**
>
> Before updating the Identity Center database, make sure there is a backup of the database.

> ℹ **Note**
>
> If you upgrade from Identity Center 7.1 to 7.2, note that the database structure has changed and you need to run the Migration tool in addition to the database update. Please see the document *SAP NetWeaver Identity Management Migration guide – Identity Management 7.1 to 7.2* for details.

To update an Identity Center database, proceed as follows:

Procedure

1. Open a command prompt and navigate to the directory containing the Identity Center script files.
2. Run the command file `mxmc-update.cmd`. You are prompted for the password for `mxmc_oper`.

3. Close the command prompt window.

5.1.8 Updating the Identity Center Database with a Given Prefix

Context

> **i Note**
>
> Before updating the Identity Center database, make sure there is a backup of the database.

> **i Note**
>
> If you upgrade from Identity Center 7.1 to 7.2, note that the database structure has changed and you need to run the Migration tool in addition to the database update. Please see the document *SAP NetWeaver Identity Management Migration guide – Identity Management 7.1 to 7.2* for details.
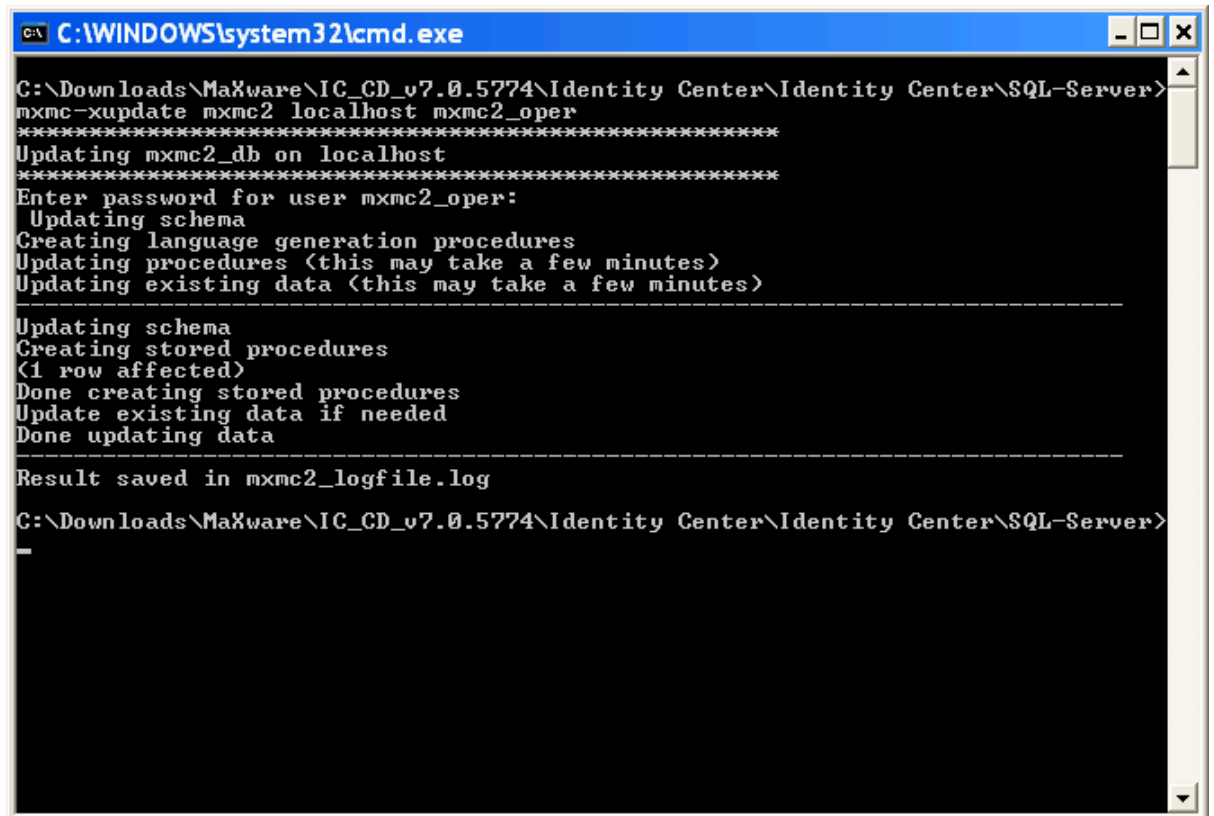
> **i Note**
>
> Make sure the Identity Center database is updated to version 7.4, update 63.

To update an Identity Center database with a given prefix, proceed as follows:

Procedure

1. Open a command prompt and navigate to the directory containing the Identity Center script files.
2. Run the command file `mxmc-xupdate.cmd`. The command file has four parameters:
   - Prefix
   - Host name of the computer running the SQL Server
   - User name for the <prefix>_oper account
   - (Optionally) Password for this account

If you do not provide the password for the `<prefix>_oper` user on the command line, you are prompted for it when you run the command file.

3. Close the command prompt window.

5.1.9 Removing an Identity Center Database

Context

To remove an Identity Center database, proceed as follows:

Procedure

1. Open a command prompt and navigate to the directory containing the Identity Center script files.
2. Run the command file `mxmc-remove.cmd`. You are prompted for the password for `sa`.

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

3. Close the command prompt window.

5.1.10 Removing an Identity Center Database with a Given Prefix

Context

To remove an Identity Center database with a given prefix, proceed as follows:

Procedure

1. Open a command prompt and navigate to the directory containing the Identity Center script files.
2. Run the command file `mxmc-xremove.cmd`. The command file has four parameters:
   - Prefix
   - Host name of the computer running the SQL Server
   - User name for the `sa` account
   - (Optionally) Password for `sa`

If you do not provide the password for sa on the command line, you are prompted for this password.

3. Close the command prompt window.

5.1.11 Enabling Full-Text Search

You can enable full-text search on the Identity Center 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 may take some time to complete. For performance reasons, you should disable full-text search while doing a bulk load in the database. This is done by stopping the service `SQL Server FullText Search` in the Control Panel (Administrative Tools/Services) before the bulk load and enabling it again when the bulk load is complete.

The full-text index is created with the language defined for the database server. If you need to specify 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 how to administer the full-text search, see the documentation for the Microsoft SQL Server.

Related Information

Enabling Full-Text Search on an Identity Center Database [page 54]
Enabling Full-Text Search for an Identity Center Database with a Given Prefix [page 55]
Configuring the Stop Word List [page 56]

5.1.11.1 Enabling Full-Text Search on an Identity Center Database

Context

To enable full-text search, proceed as follows:

Procedure

1. Open a command prompt and navigate to the directory containing the Identity Center script files.
2. Run the command file `mxmc-enable-fulltext.cmd`. You are prompted for the password for `mxmc_oper`.

3. Full-text is enabled on the database.

5.1.11.2 Enabling Full-Text Search for an Identity Center 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 containing the Identity Center script files.
2. Run the command file `mxmc-xenable-fulltext.cmd`. The command file has four parameters:

   - Prefix
   - Host name of the computer running the SQL Server
   - User name for the `<prefix>_oper` account
   - (Optionally) Password for `<prefix>_oper`

   ```
   C:\WINDOWS\system32\cmd.exe

   C:\Downloads\MaXware\IC_CD_v7.0.6579\Identity Center\Identity Center\SQL-Server>
   mxmc-xenable-fulltext mxmc3 localhost mxmc3_oper
   ***************************************************
   Enabling fulltext search for mxmc3_db on localhost
   ***************************************************
   Enter password for user mxmc3_oper:
   -------------------------------------------------------------------------------
   Enable fulltext
   *** Enabling FullText
   -------------------------------------------------------------------------------
   Result saved in mxmc3_logfile.log

   C:\Downloads\MaXware\IC_CD_v7.0.6579\Identity Center\Identity Center\SQL-Server>
   ```

   If you do not provide the password for `<prefix>_oper` on the command line, you are prompted for this password.
3. Full-text is enabled on the database.

5.1.11.3 Configuring the Stop Word List

The stop word (noise word) list is a list that contains words that are not indexed.

These are words like `a`, `the`, `or`, and that 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 it is also considered a stop word. To be able to search for privileges with names containing the word `only`, the stop word list must be modified.

> **i Note**
>
> Make sure to modify the stop word list for all relevant languages.

The process is different depending on the version of Microsoft SQL Server.

Related Information

5.1.11.3.1 Customizing Stop Word List in Microsoft SQL Server 2008 and Higher

Microsoft SQL Server 2008 and higher uses stop words stored in the database.

To customize the list, you need to make a copy of the system stop word list and assign it to be used with the full-text index (ftfull) for Identity Management. This can be done using these commands or from the user interface of the SQL Server Management Studio.

> **Sample Code**
>
> ```
> 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
> ```

It is also possible to view the stop words using queries. This example shows listing languages blocking the word `only`.

> **Sample Code**
>
> ```
> -- To list all entries of 'only' stopwords in the stoplist (can be many
> languages):
> 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:

It is also possible to test how a string will be interpreted by the full text indexing engine:

⊟ Sample Code

```
-- To test a stoplist
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:

5.1.11.3.2 Customizing Noise Word List in Microsoft SQL Server 2005

Modify the `noise<lng_code>.txt` files in the installation folder of the Microsoft SQL Server, remove `only` and other things you want to include from ENG, ENU (and others) and then drop & recreate full-text index:

⊟ Sample Code

```
drop fulltext index on mxi_values
drop fulltext catalog ftfull
CREATE FULLTEXT CATALOG ftfull WITH ACCENT_SENSITIVITY=OFF AS DEFAULT
CREATE FULLTEXT INDEX ON mxi_values(searchvalue) KEY INDEX IX_MXI_VALUES_Value_ID
```

5.1.12 Enabling and Disabling the 7.2 Approval Mechanism

As of SAP NetWeaver Identity Management 7.2 SP4, you can choose to use an improved approval mechanism, which provides better performance and more functionality.

For new installations, this mechanism is enabled by default, but when upgrading it has to be enabled manually. It is also possible to disable the 7.2 approval mechanism.

The 7.2 approval mechanism provides the following:

- 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 the Identity Center Management Console.

> ℹ **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 do no updates.

Related Information

5.1.12.1 Enabling the 7.2 Approval Mechanism on an Identity Center Database

Context

To enable the 7.2 approval mechanism, proceed as follows:

Procedure

1. Stop any running dispatchers.
2. Open a command prompt and navigate to the directory containing the Identity Center script files.
3. Run the script `mxmc-enable-72-approvals.cmd`. You are prompted for the password for `mxmc_oper`.
4. Start the dispatchers.

5.1.12.2 Enabling the 7.2 Approval Mechanism on an Identity Center Database with a Given Prefix

Context

To enable the 7.2 approval mechanism, proceed as follows:

Procedure

1. Stop any running dispatchers.
2. Open a command prompt and navigate to the directory containing the Identity Center script files.
3. Run the script `mxmc-xenable-72-approvals.cmd`. The command file has the following parameters:
   - Prefix
   - Host name of the computer running the SQL Server
   - User name for the `<prefix>_oper` account
   - (Optionally): Password for `<prefix>_oper`
4. Start the dispatchers.

5.1.12.3 Disabling the 7.2 Approval Mechanism on an Identity Center Database

Context

To disable the 7.2 approval mechanism, proceed as follows:

Procedure

1. Stop any running dispatchers.
2. Open a command prompt and navigate to the directory containing the Identity Center script files.
3. Run the script `mxmc-disable-72-approvals.cmd`. You are prompted for the password for mxmc_oper.
4. Start the dispatchers.

5.1.12.4 Disabling the 7.2 Approval Mechanism on an Identity Center Database with a Given Prefix

Context

To disable the 7.2 approval mechanism, proceed as follows:

Procedure

1. Stop any running dispatchers.
2. Open a command prompt and navigate to the directory containing the Identity Center script files.
3. Run the script `mxmc-xdisable-72-approvals.cmd`. The command file has the following parameters:
    ○ Prefix
    ○ Host name of the computer running the SQL Server
    ○ User name for the `<prefix>_oper` account
    ○ (Optionally) Password for `<prefix>_oper`
4. Start the dispatchers.

5.2   Installing the Identity Center Database on Oracle

This section describes how you install, upgrade and remove an Identity Center database on Oracle.

> **i Note**
>
> The Identity Center database must be installed on a separate database server. It is not possible to use a SAP installed Oracle database.

The installation of the Identity Center database consists of running an SQL script that uses values from a configuration file called `include.sql`. See *Preparing the Installation*. The values in this file should be modified for each installation.

The following description uses the variable `<prefix>` to indicate that the database name can be modified for each installation. If you for some reason want several Identity Center databases within the same Oracle installation, each Identity Center database must have a different `<prefix>`. This is done by modifying the PREFIX parameter in the `include.sql` file. The default `<prefix>` is `mxmc`.

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

Related Information

5.2.1 Prerequisites and Recommendations

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, that is, an empty database. For details, see the documentation for your Oracle system.
- **Character set**
  When installing the Identity Center database on Oracle, make sure that the database has been created with the AL32UTF8 character set to be able to store data in the Japanese character set using UTF-8.
- **Database naming**
  If you plan to install remote Oracle clients accessing your database on the server, it may be a good idea to use the same database name (SID) on the Oracle server and the Oracle clients. For example, if your server name is SERVER1, you may choose a database name as ORCL_DBSERVER1, and use this name when defining the connections strings in the Management Console and database names in Identity Management User Interface.
- **Create as Container database**
  If you use Oracle 12.1 (12c Release 1), make sure the *Create as Container database* option is not selected.
- **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.

5.2.2 Installing the Oracle Database on Unix

If running the script files directly on Unix, you must run the scripts as a user that has permissions to create and execute files.

Context

> **i Note**
>
> If you run the script files with the command `./<script-file>.sh` and you receive a `Permission denied` error, although you have the right permission to execute the file, use `sh <script-file>.sh` instead.

It is also possible to run the script files from the server running the Management Console which has the Oracle client for Microsoft Windows installed. You need to install the 32-bit version of the Oracle client if you run a 32-bit Java Virtual Machine on Microsoft Windows.

If you are installing the schema in a shell on Unix/Linux and experience problems with national characters in translated values of attribute names in the Identity Management User Interface you can check the following:

Procedure

1. Start a terminal session on the host you used to install the Identity Center database schema.
2. Check if the environment variable `<NLS_LANG>` is set to .AL32UTF8.
3. If not set, or set to a different value, change it for the current terminal session by running the following statement:

   > **⊜ Sample Code**
   >
   > ```
   > export NLS_LANG=.AL32UTF8
   > ```

4. Run the `mxmc-update.sh` script to reload the language file.
5. In SQL Developer or SQL Plus as mxmc_oper user run the following SQL command:

   > **⊜ Sample Code**
   >
   > ```
   > exec mxp_init_ids_lang(<idstore number>);
   > ```

   This will run the update script which reloads the language file with the contents interpreted as UTF8, and then reapply the language to the attributes in your system.

5.2.3 Database Script Files

Context

The script files are included in the installation kit for `Identity Center Designtime`.

To locate the script files, proceed as follows:

Procedure

1. Navigate to the download area of SAP NetWeaver Identity Management 7.2 on SAP Support Portal and download the installation kit for `Identity Center Designtime`.
2. Unpack the installation kit.
3. The script files are located in the `/Database/Oracle` folder.

   > **i 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.

The following scripts are used to install or upgrade the Identity Center database:

Table 7:

Script	Description	Account (run as)
`mxmc-install.cmd` (Microsoft Windows) `mxmc-install.sh` (Unix)	Creates an Identity Center database.	`SYSTEM`
`mxmc-update.cmd` (Microsoft Windows) `mxmc-update.sh` (Unix)	Upgrades an Identity Center database	`<prefix>_OPER`
`mxmc-remove.cmd` (Microsoft Windows) `mxmc-remove.sh` (Unix)	Removes an Identity Center database.	`SYSTEM`

5.2.4 Database Roles and Users

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

Table 8:

Role	Description	Default user
`db_owner`	This 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 the database administration without distributing the password to the SYSTEM user.	`<prefix>_OPER`
`<prefix>_ADMIN_ROLE`	This role is assigned to the administrator of the Identity Center. This role is allowed to change all information within the Identity Center, and execute the necessary procedures for creating jobs and groups, and maintaining these.	`<prefix>_ADMIN`
`<prefix>_USER_ROLE`	This role can view jobs and groups within the Identity Center, but is not allowed to change any information, except scheduling information.	`<prefix>_USER`
`<prefix>_RT_ROLE`	This role is used by the runtime engine, and functionality is limited to table and procedure access necessary for the runtime engine.	`<prefix>_RT`
`<prefix>_PROV_ROLE`	This role can be used by other systems giving input to the provisioning module of the Identity Center.	`<prefix>_PROV`
`<prefix>_TRANSPORT_ROLE`	This role is used to provide access to performing an export or import of a configuration in the Administration User Interface.	`<prefix>_PROV`

5.2.5 Preparing the Installation

The file `include.sql` contains values for global variables used in the installation scripts.

Open the file in a text editor and specify values for the following parameters:

Table 9:

Parameter	Description	Default value
PREFIX	Database prefix If you want to install more than one Identity Center in the same database, you must change this prefix before running the scripts. It can be any legal Oracle identifier and will be prepended to the user and role names. > ℹ Note > The prefix must not start with a numeric value, and must not contain the characters u, 0, 9 or \.	MXMC
NET_SERVICE	Net Service In an Oracle client, this must be set to the net service, e.g. ORADB.	' '
DATA_TS	Data tablespace for the Identity Center database.	USERS
INDEX_TS	Index tablespace for the Identity Center database.	USERS

5.2.5.1 Creating Additional Users

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

Make sure you assign correct roles to the users.

If you want to add users after the Identity Center database is installed, this can be done using the database's administrative tools.
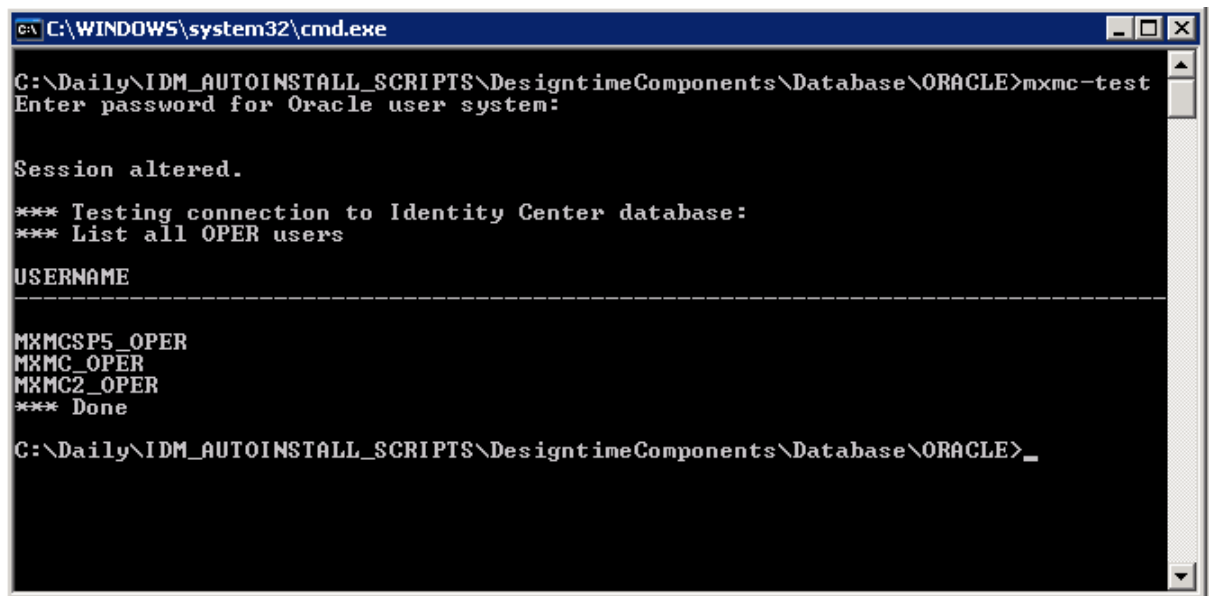
5.2.6 Testing the Database Connection

Context

You can verify that you are able to connect to the database where you want to install the Identity Center database.

Procedure

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

2. Run the command file `mxmc-test.cmd/mxmc-test.sh`. You are prompted for the system password:

```
C:\WINDOWS\system32\cmd.exe                                          _ □ ×

C:\Daily\IDM_AUTOINSTALL_SCRIPTS\DesigntimeComponents\Database\ORACLE>mxmc-test
Enter password for Oracle user system:


Session altered.

*** Testing connection to Identity Center database:
*** List all OPER users

USERNAME
-------------------------------------------------------------------------------

MXMCSP5_OPER
MXMC_OPER
MXMC2_OPER
*** Done

C:\Daily\IDM_AUTOINSTALL_SCRIPTS\DesigntimeComponents\Database\ORACLE>_
```

3. The result of the command file is a list of OPER users for each database or an error message. If you receive an error message, there is a problem with your database installation or configuration, and the Identity Center database installation scripts will not be able to access the database. You need to correct the problem before you continue. Please see the Oracle documentation for details.

5.2.7 Installing the Identity Center Database

Context

The Identity Center database is installed by running script `mxmc-install.cmd/mxmc-install.sh`. The screen captures are taken on Microsoft Windows, but the procedure is identical on Unix.

Procedure
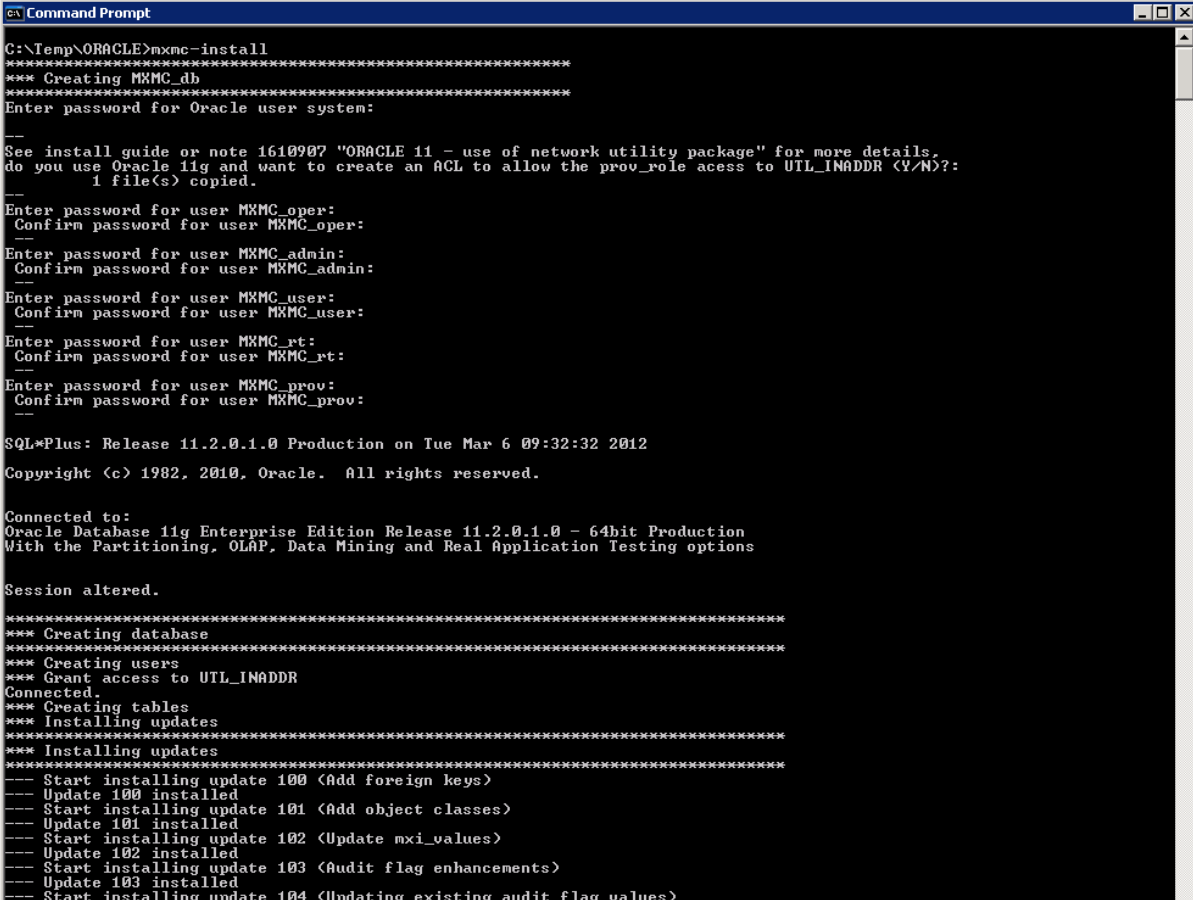
1. If necessary, copy the script files to an empty file system directory.
2. Update the `include.sql` file if necessary.
3. Open a command prompt and navigate to this directory.

> **i Note**
>
> Do not run the scripts directly from Microsoft Windows Explorer.

4. Run the command file `mxmc-install.cmd/mxmc-install.sh`. You are prompted for the system password and the passwords for the Identity Center users.

   You are also prompted if you want to create an Access Control List for UTL_INADDR for Oracle 11. See *Creating an Access Control List for the network utility package UTL_INADDR (Oracle 11)*.

```
Command Prompt                                                    _ □ ✕

C:\Temp\ORACLE>mxmc-install
********************************************************
*** Creating MXMC_db
********************************************************
Enter password for Oracle user system:

--
See install guide or note 1610907 "ORACLE 11 - use of network utility package" for more details,
do you use Oracle 11g and want to create an ACL to allow the prov_role acess to UTL_INADDR (Y/N)?:
        1 file(s) copied.
--
Enter password for user MXMC_oper:
 Confirm password for user MXMC_oper:
--
Enter password for user MXMC_admin:
 Confirm password for user MXMC_admin:
--
Enter password for user MXMC_user:
 Confirm password for user MXMC_user:
--
Enter password for user MXMC_rt:
 Confirm password for user MXMC_rt:
--
Enter password for user MXMC_prov:
 Confirm password for user MXMC_prov:
--
SQL*Plus: Release 11.2.0.1.0 Production on Tue Mar 6 09:32:32 2012

Copyright (c) 1982, 2010, Oracle.  All rights reserved.

Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

Session altered.
********************************************************************************
*** Creating database
********************************************************************************
*** Creating users
*** Grant access to UTL_INADDR
Connected.
*** Creating tables
*** Installing updates
********************************************************************************
*** Installing updates
********************************************************************************
--- Start installing update 100 (Add foreign keys)
--- Update 100 installed
--- Start installing update 101 (Add object classes)
--- Update 101 installed
--- Start installing update 102 (Update mxi_values)
--- Update 102 installed
--- Start installing update 103 (Audit flag enhancements)
--- Update 103 installed
--- Start installing update 104 (Updating existing audit flag values)
```

   When the file completes without error messages, the database is installed correctly.

   You can check the log file mxmc-install.log for any warnings or errors.

5. Close the command prompt window.

Results

The database is now installed and ready for use by the Identity Center. See *Installing the Management Console* and *Identity Center Installation Overview* for more information.

Related Information

5.2.8 Updating an Identity Center Database

Context

> **i Note**
>
> Before updating the Identity Center database, make sure there is a backup of the database.

> **i Note**
>
> If you upgrade from Identity Center 7.1 to 7.2, note that the database structure has changed and you need to run the Migration tool in addition to the database update. Please see the document *SAP NetWeaver Identity Management Migration guide – Identity Management 7.1 to 7.2* for details.

To update an Identity Center database, proceed as follows:

Procedure

1. Open a command prompt and navigate to the directory containing the Identity Center script files.

   Make sure you have the same `include.sql` file as you used during install.
2. Run the command file `mxmc-update.cmd/mxmc-update.sh`. You are prompted for the password for `mxmc_oper`.

You can check the log file mxmc-update.log for any warnings or errors.

3. Close the command prompt window.

5.2.9 Removing an Identity Center Database

Context

To remove an Identity Center database:

Procedure

1. Open a command prompt and navigate to the directory containing the Identity Center script files.
2. Run the command file mxmc-remove.cmd/mxmc-remove.sh. You are prompted for the system password.

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

You can check the log file mxmc-update.log for any warnings or errors.

3. Close the command prompt window.

5.2.10 Creating an Access Control List for the Network Utility Package UTL_INADDR (Oracle 11)

From Oracle version 11 the use of the utility package UTL_INADDR is by default restricted to `sysdba` user. As of SAP NetWeaver Identity Management 7.2 SP4, 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 SAP Note 1610907 .

5.2.11 Enabling and Disabling the 7.2 Approval Mechanism

As of SAP NetWeaver Identity Management 7.2 SP4, you can choose to use an improved approval mechanism, which provides better performance and more functionality.

For new installations, this mechanism is enabled by default, but when upgrading it has to be enabled manually. It is also possible to disable the 7.2 approval mechanism.

The 7.2 approval mechanism provides the following:

- 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 the Identity Center Management Console.

> ℹ **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 do no updates.

Related Information

5.2.11.1 Enabling the 7.2 Approval Mechanism on an Identity Center Database

Context

To enable the 7.2 approval mechanism, proceed as follows:

Procedure

1. Stop any running dispatchers.
2. Open a command prompt and navigate to the directory containing the Identity Center script files.

   Make sure you have the same include.sql file as you used during install.
3. Run the script `mxmc-enable-72-approvals.cmd`/ `mxmc-enable-72-approvals.sh`. You are prompted for the password for `mxmc_oper`.

4. Start the dispatchers.

5.2.11.2 Disabling the 7.2 approval Mechanism on an Identity Center Database

Context

To disable the 7.2 approval mechanism, proceed as follows:

Procedure

1. Stop any running dispatchers.
2. Open a command prompt and navigate to the directory containing the Identity Center script files.

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

5.3   Installing the Identity Center Database on IBM DB2

This section describes how you install, upgrade and remove an Identity Center database on IBM DB2.

The installation of the Identity Center database consists of running an SQL script that uses values from a configuration file called `include.sql`. See *Preparing the Installation*. The values in this file should be modified for each installation.

The following description uses the variable `<prefix>` to indicate that the database name can be modified for each installation. If you for some reason want several Identity Center databases within the same IBM DB2 installation, each Identity Center database must have a different `<prefix>`. This is done by modifying the PREFIX parameter in the `include.sql` file. The default `<prefix>` is `IC`.

> ➡ 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) or 'ic' (on UNIX operating systems).

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

Related Information

5.3.1 Database Script Files

Context

The script files are included in the installation kit for `Identity Center Designtime`.

To locate the script files, proceed as follows:

Procedure

1. Navigate to the download area of SAP NetWeaver Identity Management 7.2 on SAP Support Portal and download the installation kit for `Identity Center Designtime`.
2. Unpack the installation kit.
3. The script files are located in the `/Database/DB2` folder.

   > ℹ **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.

   The following scripts are used to install or upgrade the Identity Center database:

Table 10:

Script	Description	Account (run as)
`mxmc-install.cmd` (Microsoft Windows) `mxmc-install.sh` (Unix)	Creates an Identity Center database.	`<prefix>_oper`
`mxmc-update.cmd` (Microsoft Windows) `mxmc-update.sh` (Unix)	Upgrades an Identity Center database	`<prefix>_oper`
`mxmc-remove.cmd` (Microsoft Windows) `mxmc-remove.sh` (Unix)	Removes an Identity Center database.	`<prefix>_oper`

5.3.2 Database Roles and Users

The Identity Center database uses a number of roles, which are assigned to users:

Table 11:

Role	Description	Default user
`db_owner`	This 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 the database administration without distributing the password to the SYSTEM user.	`<prefix>_OPER`
`<prefix>_ADMIN_ROLE`	This role is assigned to the administrator of the Identity Center. This role is allowed to change all information within the Identity Center, and execute the necessary procedures for creating jobs and groups, and maintaining these.	`<prefix>_ADMIN`
`<prefix>_USER_ROLE`	This role can view jobs and groups within the Identity Center, but is not allowed to change any information, except scheduling information.	`<prefix>_USER`

Role	Description	Default user
`<prefix>_RT_ROLE`	This role is used by the runtime engine, and functionality is limited to table and procedure access necessary for the runtime engine.	`<prefix>_RT`
`<prefix>_PROV_ROLE`	This role can be used by other systems giving input to the provisioning module of the Identity Center.	`<prefix>_PROV`
`<prefix>_TRANSPORT_ROLE`	This role is used to provide access to performing an export or import of a configuration in the Administration User Interface.	`<prefix>_PROV`

5.3.3 Preparing the Installation

The file `include.sql` contains values for global variables used in the installation scripts. Open the file in a text editor and specify values for the following parameters:

Table 12:

Parameter	Description	Default value
`PREFIX`	Database prefix If you want to install more than one Identity Center in the same database, you must change this prefix before running the scripts. It will be prepended to the user and role names. > **i Note** > For Microsoft Windows the prefix can be maximum 5 characters long, for Unix maximum 2 characters. > The prefix must not contain the characters @, #, § or \.	`IC`
`STORAGEPATH`	The path to the folder where the database will be installed.	`C:\usr\DB2\IC`

Parameter	Description	Default value
DB2PORT	The port number for the database, as specified when installing the database system. See *Identity Center Installation Overview* for details.	52222
TEMPORARYTABLESPACE	The temporary tablespace used by IBM DB2.	USERTEMP
CREATEOSUSERS	ⓘ **Note** Only for Unix/Linux systems. On Microsoft Windows the operating system users will always be created. Flag to decide whether or not the necessary operating system users are created automatically or not (Y/N). If you choose not to create the users automatically, you have to create the following operating system users that will be used when authenticating to the database: • <prefix>_oper • <prefix>_admin • <prefix>_prov • <prefix>_rt • <prefix>_user	Y

5.3.3.1 Creating Additional Users

You may want to create other users or even 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`

On Unix/Linux, create the users manually. Make sure you assign correct roles to the users. For information how to do that, see the script file:

• `2-create-roles.sql`

5.3.3.2 Prerequisites and Recommendations

For Microsoft Windows

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

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

For Unix/Linux

To install the database on Unix/Linux, the following software is required:

- IBM DB2 CLPPlus
- Bash
- sudo

> **i Note**
>
> On UNIX operating systems, the names of database objects, user names, passwords, groups, files, and paths are case sensitive. You must use lower case letters.

Installing sudo on IBM AIX

On IBM AIX, sudo is normally not a part of the default installation, and must be added separately. The installation is available as part of the IBM AIX Toolbox, which can be downloaded from: IBM AIX Toolbox download information ⬀

The whole package: AIX Toolbox for Linux Applications ⬀

For information about how to install sudo, see the IBM documentation.

5.3.4 Installing the Identity Center Database

Context

The Identity Center database can either be installed on Microsoft Windows or a Unix platform.

> **i Note**
>
> All installation scripts must be run on the database server.

- **Microsoft Windows**:
  Run the script files from the IBM DB2 command window.
- **Unix/Linux**:
  The installation script must be executed as the IBM DB2 instance/installation user, default: db2inst1.
  The `mxmc-install.sh` script requires the user to be allowed to execute the sudoer command.
  Run the script files from the Unix shell, logged in as the IBM DB2 instance/installation user.

Procedure

1. If necessary, copy the script files to an empty file system directory.
2. Update the `include.sql` file if necessary.
3. For
   - **Microsoft Windows**: Open the IBM DB2 command window. In the *Start* menu, choose *IBM DB2/ <Database>/Command window - Administrator*
   - **Unix/Linux**: Open a command prompt.
4. Navigate to the directory where the database installation scripts are located.
5. Run the command file `mxmc-install.cmd/mxmc-install.sh`. You are prompted for the system password and the passwords for the Identity Center users.

```
Administrator: DB2 CLP - DB2COPY1 - mxmc-install                              _ □ ×

C:\Daily\IDM_AUTOINSTALL_SCRIPTS\DesigntimeComponents\Database\DB2>mxmc-install

Enter password for user IC_OPER:
 Confirm password for user IC_OPER:

Enter password for user IC_ADMIN:
 Confirm password for user IC_ADMIN:

Enter password for user IC_USER
 Confirm password for user IC_USER:

Enter password for user IC_RT:
 Confirm password for user IC_RT:

Enter password for user IC_PROV:
 Confirm password for user IC_PROV:
 PREFIX:                IC
STORAGEPATH:           C:\usr\DB2\IC
TEMPORARYTABLESPACE: USERTEMP
DBPORT                 52222

***************************************************************
*** Creating users for IC_db
***************************************************************
*** Creating IC_OPER
Creating user IC_OPER
Setting password for IC_OPER
Setting description for IC_OPER
Adding user IC_OPER to group DB2USERS
Adding user IC_OPER to group DB2ADMNS
*** Creating IC_ADMIN
Creating user IC_ADMIN
Setting password for IC_ADMIN
Setting description for IC_ADMIN
Adding user IC_ADMIN to group DB2USERS
Adding user IC_ADMIN to group DB2ADMNS
*** Creating IC_USER
Creating user IC_USER
Setting password for IC_USER
Setting description for IC_USER
```

When the file completes without error messages, the database is installed correctly.

You can check the log file `mxmc-install.log` for any warnings or errors.

6. Close the command prompt window.

Results

The database is now installed and ready for use by the Identity Center. See *Installing the Management Console* and *Identity Center Installation Overview* sections for more information.

For a better performance of the IBM DB2, you can schedule a REBIND command for the IBM DB2 packages that contain static SQL statements to be executed on a regular basis. For more information about the use of the REBIND command, see SAP Note 2235911 .

Related Information

Installing the Management Console [page 31]
Identity Center Installation Overview [page 7]

5.3.5 Updating the Identity Center Database
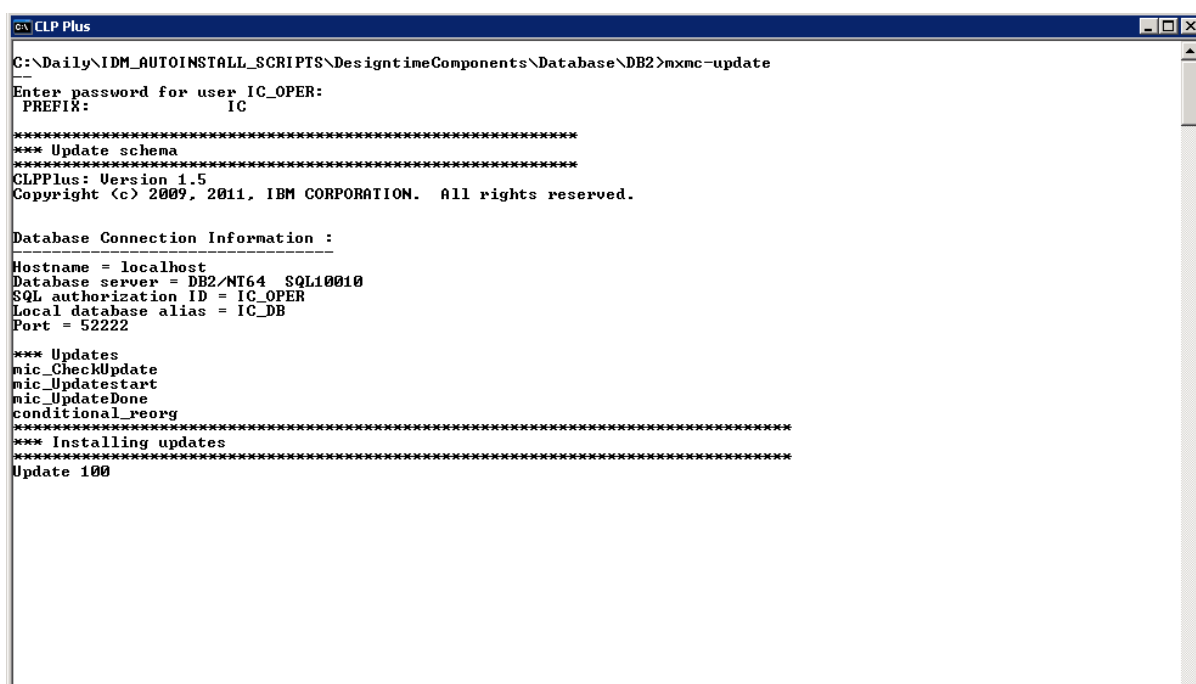
Context

> **i Note**
>
> Before updating the Identity Center database, make sure there is a backup of the database.

To update an Identity Center database, proceed as follows:

Procedure

1. Make sure you use the same values in the `include.sql` file as you used during install.
2. For
   - **Microsoft Windows**: Open the IBM DB2 command window. In the *Start* menu, choose *IBM DB2/ <Database>/Command window - Administrator*.
   - **Unix/Linux**: Open a command prompt.
3. Navigate to the directory containing the Identity Center script files.
4. Run the command file `mxmc-update.cmd/mxmc-update.sh`. You are prompted for the password for `<prefix>_oper`.

```
CLP Plus

C:\Daily\IDM_AUTOINSTALL_SCRIPTS\DesigntimeComponents\Database\DB2>mxmc-update
--
Enter password for user IC_OPER:
 PREFIX:            IC

**********************************************************
*** Update schema
**********************************************************
CLPPlus: Version 1.5
Copyright (c) 2009, 2011, IBM CORPORATION.  All rights reserved.


Database Connection Information :
---------------------------------
Hostname = localhost
Database server = DB2/NT64  SQL10010
SQL authorization ID = IC_OPER
Local database alias = IC_DB
Port = 52222

*** Updates
mic_CheckUpdate
mic_Updatestart
mic_UpdateDone
conditional_reorg
***********************************************************************************
*** Installing updates
***********************************************************************************
Update 100
```

You can check the log file `mxmc-update.log` for any warnings or errors.

5. Close the command prompt window.

5.3.6 Removing an Identity Center Database

Context

> ℹ **Note**
>
> In Unix, the `mxmc-remove.sh` script requires the user to be allowed to execute the sudoer command.

To remove an Identity Center database, proceed as follows:

Procedure

1. For
   - **Microsoft Windows**: Open the IBM DB2 command window. In the *Start* menu, choose *IBM DB2/ <Database>/Command window - Administrator*.
   - **Unix/Linux**: Open a command prompt.
2. Navigate to the directory containing the Identity Center script files.
3. Run the command file `mxmc-remove.cmd/mxmc-remove.sh`. You are prompted for the system password.

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

```
DB2 CLP - DB2COPY1                                                      _ □ ×

C:\Daily\IDM_AUTOINSTALL_SCRIPTS\DesigntimeComponents\Database\DB2>mxmc-remove

******* Remove schema **********************************
Are you sure you want to delete the IC schema?
Press CTRL-C to abort now.
Press any key to continue . . .

******* IC_OPER password ************************
Enter password for user IC_OPER:

   Database Connection Information

 Database server        = DB2/NT64 10.1.0
 SQL authorization ID   = IC_OPER
 Local database alias   = IC_DB


******* Remove schema **********************************
*** WARNING!!! ***
All Identity Center information will be removed!!!!!!
Press CTRL-C to abort now.
Press any key to continue . . .

************************************************************
*** Drop IC_db
************************************************************
DB20000I  The SQL DISCONNECT command completed successfully.
11/14/2012 14:41:52    0   0   SQL1064N  DB2STOP processing was successful.
SQL1064N  DB2STOP processing was successful.
11/14/2012 14:41:58    0   0   SQL1063N  DB2START processing was successful.
SQL1063N  DB2START processing was successful.
DB20000I  The DROP DATABASE command completed successfully.

************************************************************
*** Delete IC_db users
************************************************************
*** Delete IC_OPER
*** Delete IC_ADMIN
*** Delete IC_USER
*** Delete IC_RT
*** Delete IC_PROV

IC_db database and IC users removed!
C:\Daily\IDM_AUTOINSTALL_SCRIPTS\DesigntimeComponents\Database\DB2>_
```

You can check the log file `mxmc-update.log` for any warnings or errors.

4. Close the command prompt window.

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

6 Installing and Configuring the Identity Management User Interface

This section describes how you install the Identity Management User Interface and perform the initial configuration.

You configure Identity Management User Interface using the Identity Center Management Console.

Overview

While the administrator (manager) manages the Identity Center configuration through the Management Console, the Web Dynpro Java application Identity Management User Interface is used for all end-user registration/self service, password resets and approval of tasks. It also contains monitoring information for administrators (managers) of the Identity Center. When installing and configuring the User Interface you need to complete the following steps:

- Define the JDBC connection for the JMX layer
- Deploy the Identity Management User Interface
- Configure the JMX layer
- Perform the initial configuration
- (Optionally) Integrate the User Interface in the SAP NetWeaver Portal

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.

The procedures may also be different depending on your version of SAP NetWeaver. See the supported versions in the *Prerequisites* below.

There is a section describing the procedures for SAP NetWeaver AS Java as of Release 7.0. Much of the procedures for other supported SAP NetWeaver versions on the list (SAP NetWeaver CE 7.1 EHP 1, SAP NetWeaver CE 7.2, SAP NetWeaver 7.3, SAP NetWeaver 7.3 EHP 1 and SAP NetWeaver 7.4) are the same. The procedures for these versions are therefore described in a shared section *Other SAP NetWeaver releases* throughout the document.

Prerequisites

Before you can install the Identity Management User Interface, make sure that the following prerequisites are present:

- One of the following SAP NetWeaver versions must be correctly installed and licensed:
  - SAP NetWeaver AS Java as of Release 7.0 (SAP NetWeaver 7.0)
  - SAP NetWeaver Composition Environment 7.1 Including Enhancement Package 1 (SAP NetWeaver CE 7.1 EHP 1)

84   PUBLIC

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring the Identity Management User Interface

- o SAP NetWeaver Composition Environment 7.2 (SAP NetWeaver CE 7.2)
        - o SAP NetWeaver 7.3
        - o SAP NetWeaver 7.3 Including Enhancement Package 1 (SAP NetWeaver 7.3 EHP 1)
        - o SAP NetWeaver 7.4
- SAP NetWeaver Identity Management Identity Center version 7.2 SP9 or higher, must be correctly installed and licensed.
- Basic knowledge about the SAP NetWeaver AS Java and its tools.
- When giving certain accesses to the Identity Management User Interface, basic knowledge about the Identity Center is required.

Related Information

Visual Administrator
SAP NetWeaver Administrator for SAP NetWeaver CE 7.1 EHP 1
SAP NetWeaver Administrator for SAP NetWeaver CE 7.2
SAP NetWeaver Administrator for SAP NetWeaver 7.3
SAP NetWeaver Administrator for SAP NetWeaver 7.3 EHP 1
SAP NetWeaver Administrator for SAP NetWeaver 7.4
Software Deployment Manager
Software Logistics Toolset 1.0

6.1 Defining the JDBC Connection for the JMX Layer

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 Center database.

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

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

Related Information

6.1.1 SAP NetWeaver AS Java as of Release 7.0

To set up the connection for SAP NetWeaver AS Java 7.0, use Visual Administrator (the J2EE Engine administration tool). Start and login to the Visual Administrator.

Related Information

6.1.1.1   Deploying the JDBC Driver

To deploy the driver on SAP NetWeaver 7.0, follow the process described in *Deploying and Removing JDBC Drivers*.

> **i Note**
>
> The JDBC driver must be installed on the server as described in *Installing the JDBC Drivers* in the *Identity Center Installation Overview* section.

> **i Note**
>
> SAP NetWeaver AS Java 7.0 is not supported when using IBM DB2 as the database system.

> **i 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` or `ORACLE`.

> **i Note**
>
> On the server, verify that the file exists in the location `\usr\sap\<System ID>\<INSTANCE_NAME>\j2ee\cluster\server0\bin\ext\<name of the driver>` (for example: `C:\usr\sap\F21\JC30\j2ee\cluster\server0\bin\ext\SQL2005` or `C:\usr\sap\F21\JC30\j2ee\cluster\server0\bin\ext\ORACLE`). Sometimes an empty file is created. If this is the case, copy the file manually into the location then restart the server.

Related Information

6.1.1.2 Adding the Identity Center Database as a Data Source

The driver is uploaded and we can now create the data source. To do so, follow the process of creating a data source with JDBC version 1.x, as described in *Creating a DataSource with JDBC 1.x Driver*.

> **i 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.

> **i Note**
>
> SAP NetWeaver AS Java 7.0 is not supported when using IBM DB2 as the database system.

Following the above mentioned process for adding the Identity Center database as a data source, pay special attention to the following fields (and apply the values listed):

Table 13:

Tab	Name of the field	
Main tab	*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_DataSource` for the data source. Read more about creating and managing data source aliases in Managing Aliases.
Main tab	*JDBC Version*	Make sure that the 1.x JDBC version is selected.

Tab	Name of the field	
Main tab	*Driver Class*	Fill in the driver class: • `com.microsoft.sqlserver.` `jdbc.SQLServerDriver` for MS SQL Server • `oracle.jdbc.driver.Oracl` `eDriver` for Oracle

Main tab	*Database URL*	Provide the correct database URL:
		• **For MS SQL Server**: `jdbc:sqlserver://`
		`<host>;database=<databas`
		`e 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=<`
		`database prefix>_db`.
		• **For Oracle**: `jdbc:oracle:thin:@<host>`
		`:<port>:<database SID>` (for example, `jdbc:oracle:thin:@10.55.`
		`165.63:1521:orcl`)

Main tab	*User*	Enter the user name that you use to log in to the database server, the provisioning user. For example, **`<database`** **`prefix>_prov`** (for example, **`mxmc_prov`**).
Main tab	*Password*	Provide the password of the provisioning user defined in the *User* field.
Additional tab	*Default Connection Isolation*	Select *TRANSACTION_READ_COMMITTED*.
Additional tab	*SQL Engine*	• Choose *Native SQL* for MS SQL Server. • Choose *Vendor SQL* for Oracle.

Related Information

6.1.1.3 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 Visual Administrator, select *Server\Services\JDBC Connector* on the *Cluster* tab.
2. Select *DataSources* on the *Runtime* tab, and navigate to the data source you need to update.
3. Update the data and choose ![save icon] to save the changes in the data source. The following warning will appear:
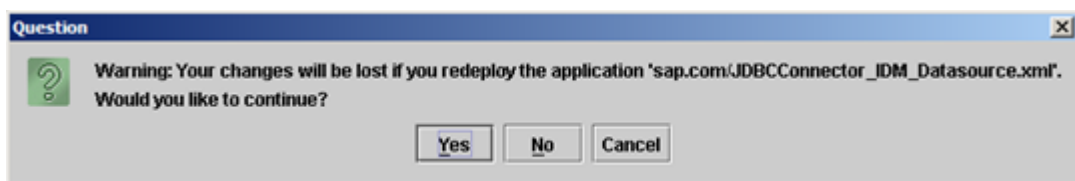
4. Choose *Yes* to confirm and save the changes.

    After updating, the server needs to be restarted – the application must be stopped and started again. Follow the steps described in *How to Restart an Application* to restart the application `sap.com/tc~idm~jmx~app`.

    The server is now restarted and ready to use.

Related Information

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring the Identity Management User Interface

PUBLIC **89**

6.1.2 Other SAP NetWeaver Releases

Context

To set up the connection for SAP NetWeaver CE 7.1 EHP 1, SAP NetWeaver CE 7.2, SAP NetWeaver 7.3, SAP NetWeaver 7.3 EHP 1 and SAP NetWeaver 7.4, use the SAP NetWeaver Administrator (NWA).

To access the NWA, proceed as follows:

Procedure

1. In your browser, enter `http(s)://<host>:<port>`, which will take you to your index page.
2. Select SAP NetWeaver Administrator or enter `http(s)://<host>:<port>/nwa` in your browser. Both procedures will display the login page for the NWA.
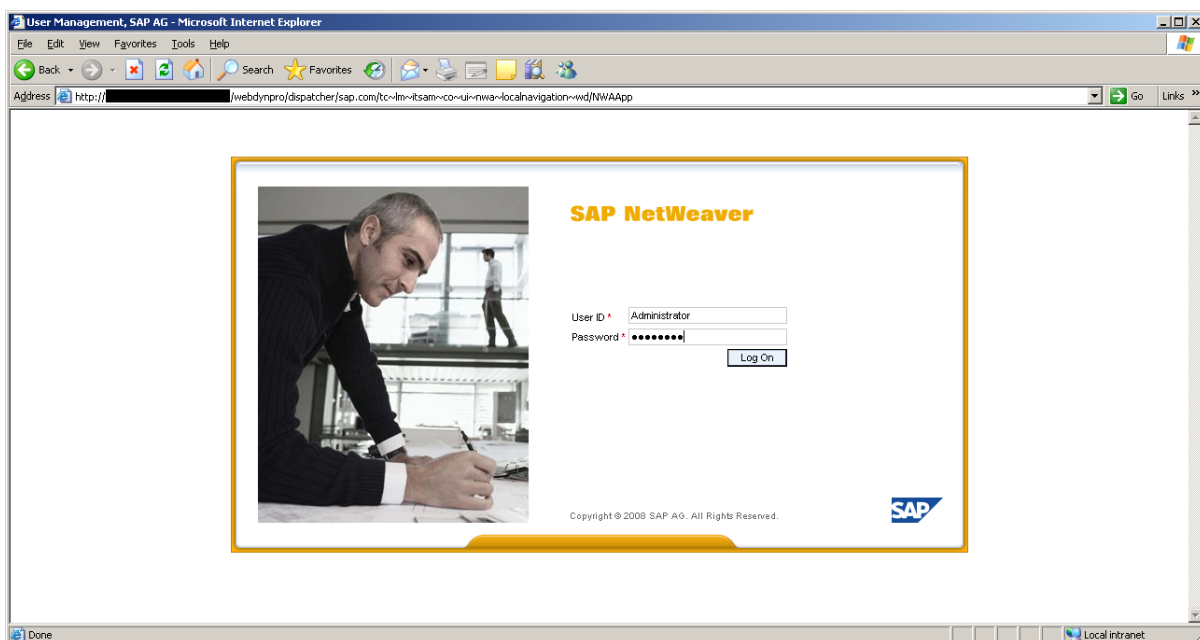
Enter the credentials, the correct user ID and the password.

6.1.2.1   Deploying the JDBC Driver

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

90   PUBLIC

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring the Identity Management User Interface

> ℹ **Note**
>
> The JDBC driver must be installed on the server as described in *Installing the JDBC Drivers* in *Identity Center Installation Overview*.

> ℹ **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` or `DB2`.

Related Information

Installing the JDBC Drivers [page 20]
Managing JDBC Drivers for SAP NetWeaver CE 7.1 EHP 1
Managing JDBC Drivers for SAP NetWeaver CE 7.2
Managing JDBC Drivers for SAP NetWeaver 7.3
Managing JDBC Drivers for SAP NetWeaver 7.3 EHP 1
Managing JDBC Drivers for SAP NetWeaver 7.4

6.1.2.2 Adding the Identity Center Database as a Data Source

To create the data source, follow the descriptions listed for each SAP NetWeaver version. See the Related Information for details.

> ℹ **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.

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

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring the Identity Management User Interface

PUBLIC **91**

Table 14:

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_DataSource** for the data source. Read more about creating and managing aliases here: • For SAP NetWeaver CE 7.1 EHP 1: Managing JDBC Data-Source Aliases • For SAP NetWeaver CE 7.2: Managing JDBC DataSource Aliases • For SAP NetWeaver 7.3: Managing JDBC DataSource Aliases • For SAP NetWeaver 7.3 EHP 1: Managing JDBC Data-Source Aliases • For SAP NetWeaver 7.4: Managing JDBC DataSource Aliases
Driver Name	Select the JDBC driver.
SQL Engine	• Choose *Native SQL* for MS SQL Server. • Choose *Vendor SQL* for Oracle and IBM DB2.
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

Name of the field	Value

Database URL	Provide the correct database URL:
	
	• **For MS SQL Server**:
	`jdbc:sqlserver://`
	`<host>;database=<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=<database`
	`prefix>_db`.
	
	• **For Oracle**:
	`jdbc:oracle:thin:@<host>:<port>:<datab`
	`ase SID>` (for example,
	`jdbc:oracle:thin:@10.55.165.63:1521:or`
	`cl`)
	
	• **For IBM DB2**:
	`jdbc:db2://<server>:<port>/`
	`<prefix>_DB:currentSchema=<PREFIX>_OPE`
	`R;currentFunctionPath=<PREFIX>_OPER;ma`
	`xStatements=100;retrieveMes`
	`sagesFromServerOnGetMessage=true;`
	For example:
	`jdbc:db2://MyServer:52222/`
	`IC_DB:currentSchema=IC_OPER;currentFun`
	`ctionPath=IC_OPER;maxStatements=100;re`
	`trieveMessagesFromServerO`
	`nGetMessage=true;`
	
	> ℹ Note
	> For IBM DB2 the <PREFIX>_OPER user must be in all caps.

User Name	Enter the user name that you use to log in to the database server, the provisioning user. For example, **`<database prefix>_prov`** (for example **`mxmc_prov`** or **`IC_prov`**).
Password	Provide the password of the provisioning user defined in the *User Name* field.

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring the Identity Management User Interface

PUBLIC **93**

Related Information

6.1.2.3   Updating the Data Source

Context

If you need to update the data source information (for example, changes in server, database, password etc), proceed as follows:

Procedure

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

94   P U B L I C

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring the Identity Management User Interface

SAP NetWeaver Administrator - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http:// /webdynpro/dispatcher/sap.com/tc~lm~itsam~ui~mainframe~wd/FloorPlanApp?applicationID=com.sap.itsam.cfg.java.app.resources&isLocal=true

Application Resources: Overview

Home   History   Back Forward   Help Log Off

Related Links

Show JDBC Custom DataSources

Resource List

Create New Resource   Delete Selected Resource   Refresh

State	Resource Name	Resource Type	Owner Name	Owner Type
●	IDM	JDBC Custom Data Source	sap.com/sap.com~IDM	J2EE Application
■	IDM_DataSource	JDBC Custom Data Source	sap.com/JDBCConnector_IDM_DataSource.xml	J2EE Application

Possible States: ■ Fully available △ Partly available ● Not available ◇ Unknown

Resource Details

IDM_DataSource

JDBC Custom Data Source

Save

Settings | Connection Pooling | Additional Properties | Antecedent JDBC Driver | Dependent Data Source Aliases

Driver Name: * SQL2005
SQL Engine: * Native SQL
Isolation Level: * Transaction Read Commited
JDBC Version: 1x (without XA support)

Driver Class Name: * com.microsoft.sqlserver.jdbc.SQLServerDriver
Database URL: * jdbc:sqlserver://trd90500010.example.com;database=mxmc_db
User Name: * mxmc_prov
Password: * ••••••••

Description:

Local intranet

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.

6.2 Deploying the Identity Management User Interface

Context

Start by downloading the `.SCA` file (the Identity Management User Interface) which is to be deployed:

Procedure

1. Navigate to the download area of SAP NetWeaver Identity Management 7.2 on SAP Support Portal and download the `.SCA` file (Identity Management User Interface).

   > **i Note**
   >
   > For deploying of the User Interface on AS Java 7.0, download the `.SCA` file stored under NW IDM IC UIS 7.00\OSINDEP. For deploying of the User Interface on the EHP 1 for SAP NW CE 7.1, SAP NW CE 7.2 and SAP NW 7.3, download the `.SCA` file stored under NW IDM IC UIS 7.10\OSINDEP.

2. If necessary unpack the file.

Results

The `.SCA` file is now ready to be deployed.

Related Information

6.2.1 SAP NetWeaver AS Java as of Release 7.0

Context

You deploy the Identity Management User Interface from Software Deployment Manager(SDM):

Procedure

1. Start SDM.
2. Deploy the Identity Management User Interface.

   The Identity Management User Interface is now deployed. The next step is configuring the JMX layer, which is described in section *Configuring the JMX layer*.

Related Information

[Software Deployment Manager](#)

6.2.2 Other SAP NetWeaver Releases

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. You can use the SUM to deploy the Identity Management User Interface.

Prerequisites

- Make sure that the Software Update Manager is downloaded and available on your SAP NetWeaver AS Java. The SUM is part of the Software Logistics Toolset delivery and available for download from SAP Software Download Center *Support Packages and Patches* > *A - Z* > *Index* > *S* > *SL TOOLSET* > *SL TOOLSET 1.0* > *Entry by Component* > *SOFTWARE UPDATE MANAGER (SUM)* .
- You can find the documentation for SUM on the SL Toolset page on SAP Service Marketplace. For SAP NetWeaver AS for Java, there are specific guides for the combinations of operating systems and databases.

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring the Identity Management User Interface

PUBLIC **97**

> **i** Note
>
> To find the documentation describing the SUM, from the Software Logistics Toolset📚 page on SAP Service Marketplace, navigate to ▌▶ *Software Logistics Toolset 1.0* ❯ *System Maintenance* ❯ under *Documentation* at the bottom of the page.

- Before running and using the SUM, you have to complete all required preparation and planning actions in the SUM 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

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

Procedure

1. Run the Software Update Manager on the application server of the primary application server instance.
2. Start the SL Common GUI of the Software Update Manager.
3. Logon to the Software Update Manager and deploy the SCA file.

Related Information

Running the Software Update Manager [page 99]
Starting the SL Common GUI of the Software Update Manager [page 100]
Deploying using the Software Update Manager [page 101]

6.2.2.1 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>.
   - for UNIX:

     ```
     SAPCAR -xf <download directory>/<path>/<Archive>.SAR -R /usr/sap/<sid>
     ```

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

   > i 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
     ```
   - for UNIX:

     ```
     cd /usr/sap/<SID>/SUM
     ./STARTUP confighostagent <SID>
     ```

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring the Identity Management User Interface

PUBLIC   **99**

> **i Note**
>
> Always call the script with the root user.

6.2.2.2 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.

   > **i 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.

6.2.2.3 Deploying using the Software Update Manager

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.

Context

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.

> i 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 process.

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

Procedure

1. Enter the user name and the password for the AS Java Administrator user with which you log on 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. Confirm the selected target system version by choosing *Next*.

   > i Note
   >
   > You can find the Central Software Update Manager Note in the Software Update Manager guide or by searching on SAP Support Portal.

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.

   When the SAP NetWeaver Identity Management User Interface is deployed on your SAP NetWeaver, proceed to configuring the JMX layer, which is described in section *Configuring the JMX layer*.

6.3 Updating the Identity Management User Interface

To update an already deployed Identity Management User Interface, download the updated SCA file and proceed as follows:

- For SAP NetWeaver AS Java as of Release 7.0: Deploy the Identity Management User Interface as described for this SAP NetWeaver version in *Deploying the Identity Management User Interface*.
- For other supported SAP NetWeaver releases: use Software Update Manager (SUM) as described for these versions in *Deploying the Identity Management User Interface*.

Related Information

Deploying the Identity Management User Interface [page 96]

6.4 Deploying on an Existing SAP NetWeaver AS Java Installation

If you wish to run the Identity Management User Interface on a previously installed and already in use SAP NetWeaver AS Java, you need to make sure that the required environment is in place.

Context

Deploying on an existing SAP NetWeaver AS Java is done using the same procedures as when installing the Identity Management User Interface.

Procedure

1. Verify that the JDBC driver for your database system is present. If necessary, add the JDBC driver as described in *Defining the JDBC connection for the JMX layer*.
2. Add the Identity Center database as a data source as described in *Defining the JDBC connection for the JMX layer*.

102   PUBLIC

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring the Identity Management User Interface

3. Download the `.SCA` file from the download area of SAP NetWeaver Identity Management 7.2 on SAP Service Marketplace (for AS Java 7.0 download the `.SCA` file stored under NW IDM IC UIS 7.00\OSINDEP, while for EHP 1 for SAP NW CE 7.1, SAP NW CE 7.2 or SAP NW 7.3 download the `.SCA` file stored under NW IDM IC UIS 7.10\OSINDEP) and unpack if necessary.
4. Deploy the Identity Management User Interface as described in *Deploying the Identity Management User Interface*.

Related Information

6.5   Configuring the JMX Layer (Java System Properties)

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.

The procedure is different depending on your version of SAP NetWeaver.

Related Information

6.5.1 SAP NetWeaver AS Java as of Release 7.0

Context

To alter the configuration, proceed as follows:

Procedure

1. Start the Visual Administrator.
2. Select the *Cluster* tab.
3. Go to ▶ *Server* ❭ *Services* ❭ *Configuration Adapter* ❭.
4. In the right pane, go to *apps\sap.com\tc~idm~jmx~app\appcfg* and open *Propertysheet application.global.properties*. Use the [icon] icon, or just double-click, to open and view.

name ▲	value	custom
com.sap.idm.jmx.ac_check_level	0	☐
com.sap.idm.jmx.cache.ttl	60	☐
com.sap.idm.jmx.crypt.keyfile		☐
com.sap.idm.jmx.idstore.reqidprefix	MXIDMUI	☐
com.sap.idm.jmx.idstoreid	1	☐
com.sap.idm.jmx.show_selfservice	true	☐

Display configuration

OK

104   P U B L I C

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring the Identity Management User Interface

The following properties are available:

Table 15:

Property	Value

`com.sap.idm.jmx.ac_check_level`	This property is used to specify how to display 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.

Property	Value
`com.sap.idm.jmx.cache.ttl`	This is time-to-live for the elements in the cache. Set to 60 minutes by default. **i 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.
`com.sap.idm.jmx.crypt.keyfile`	A file holding the 3DES keys, that is, the `Keys.ini` file. See the *SAP NetWeaver Identity Management Security Guide* for details. **i Note** If SAP NetWeaver AS Java is not installed on the same host as the Runtime Components, the `Keys.ini` file that is located in the folder `<Identity Center installation directory> /Key` (normally `C:/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.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. **i 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.

Property	Value
`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 (that is, the *Self Services* tab is visible by default).

Close *Propertysheet application.global.properties* by choosing *OK*.

5. To make changes to the configuration you need to enter the edit mode. To switch between view and edit

   mode choose ✎ icon. A dialog box will appear warning you that you are about to switch to edit mode:
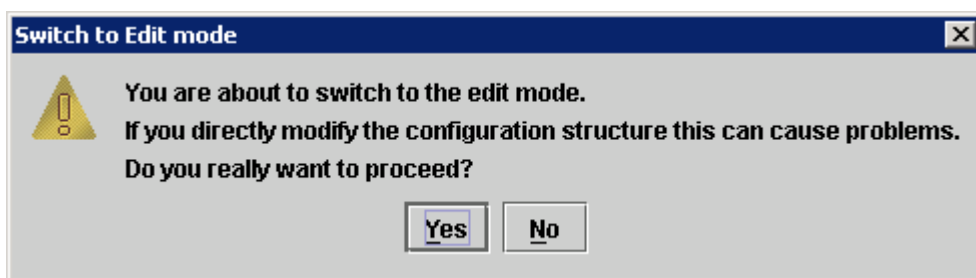
Choose *Yes*.

6. When in edit mode, open *Propertysheet application.global.properties* either by choosing ✎ icon or by double-clicking.

7. Select and open the property you wish to edit and change, for example, `com.sap.idm.jmx.idstoreid`. A *Change property entry* dialog box opens:

Enter the correct value into the *Custom* field.

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring the Identity Management User Interface

PUBLIC **107**

> ℹ **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.

8. Choose *Apply custom*.
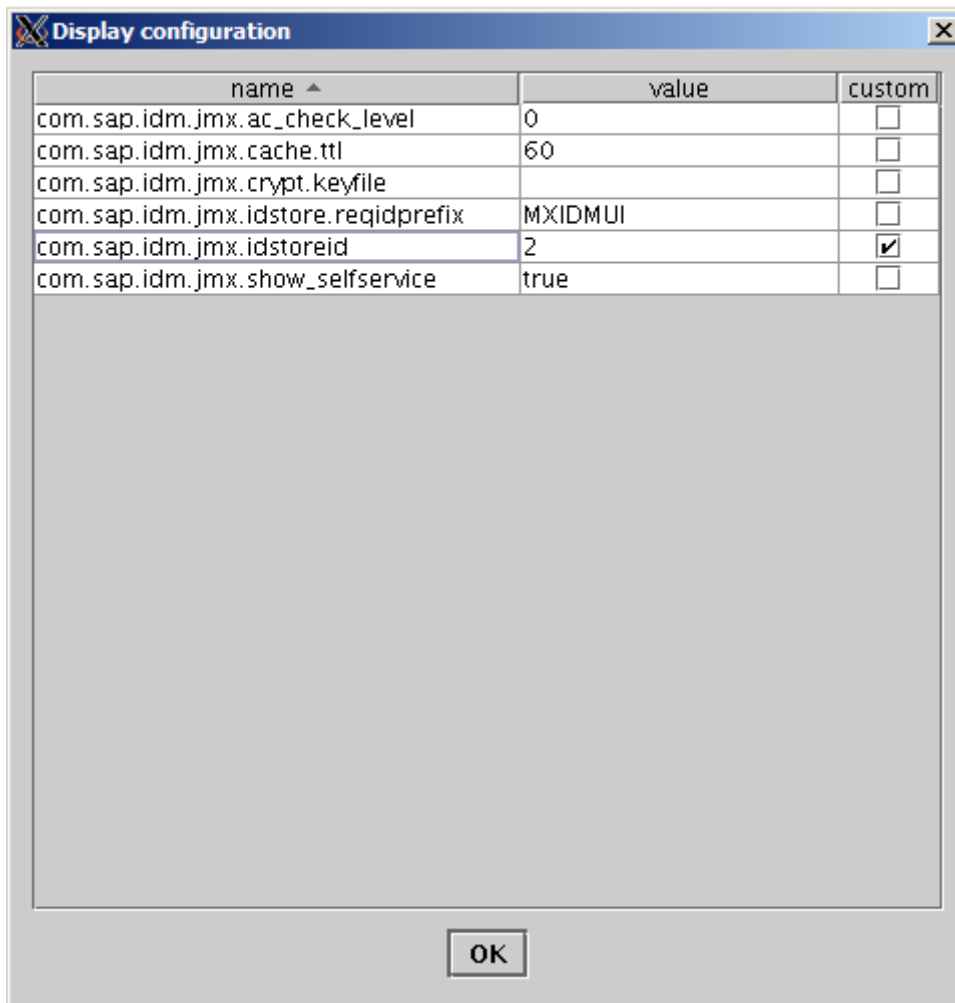
The new value is now inserted into the configuration.

9. Choose *OK* to apply changes.

108   PUBLIC

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring the Identity Management User Interface

6.5.2 Other SAP NetWeaver Releases

Context

To alter the configuration, do the following:

Procedure

1. In the NWA, go to ▮▶ *Configuration Management* ▶ *Infrastructure* ▮ .

2. Select *Java System Properties*.

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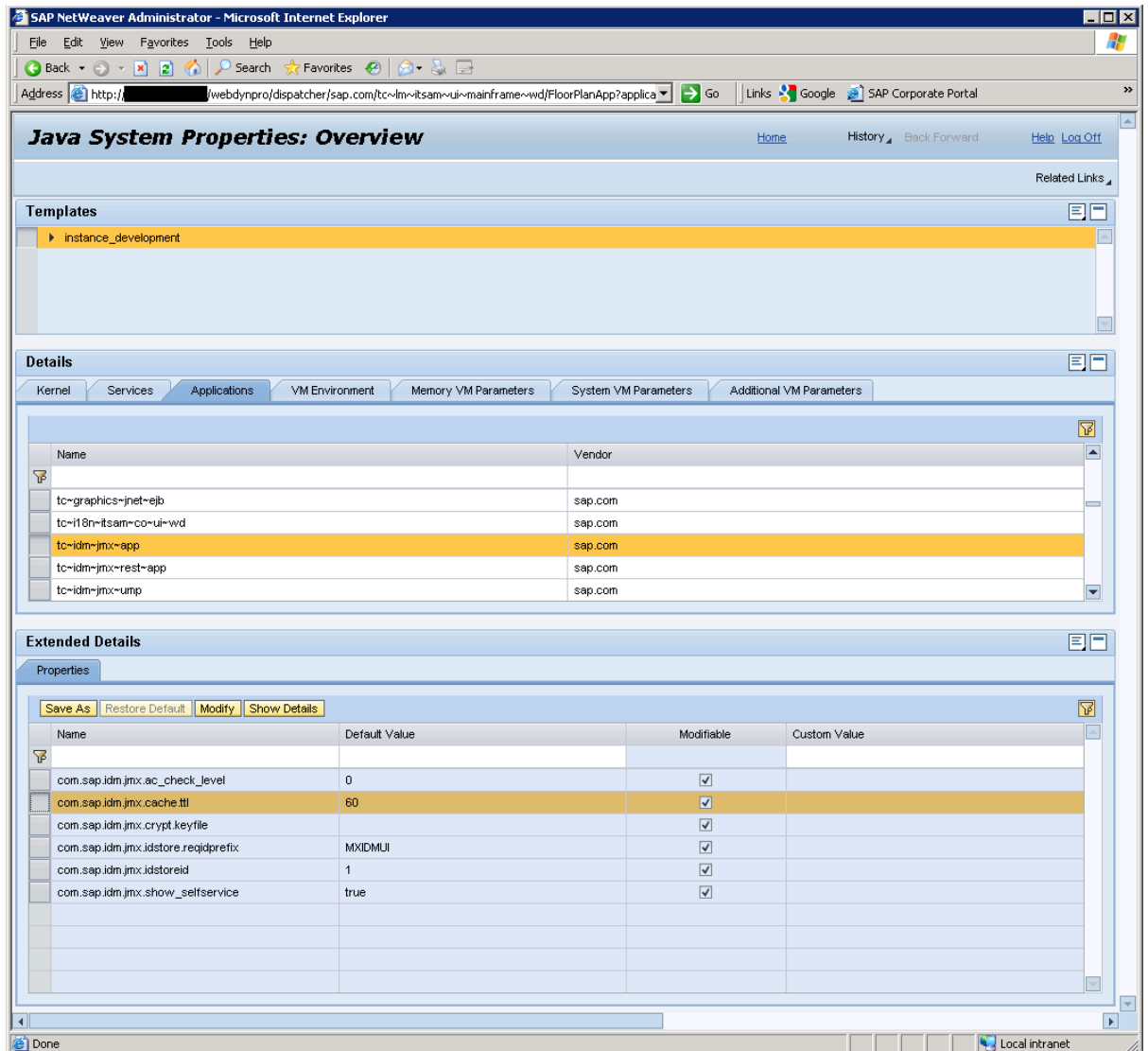
4. Find and select the *tc~idm~jmx~app*. In the *Extended Details* section, you can see the following properties:

Table 16:

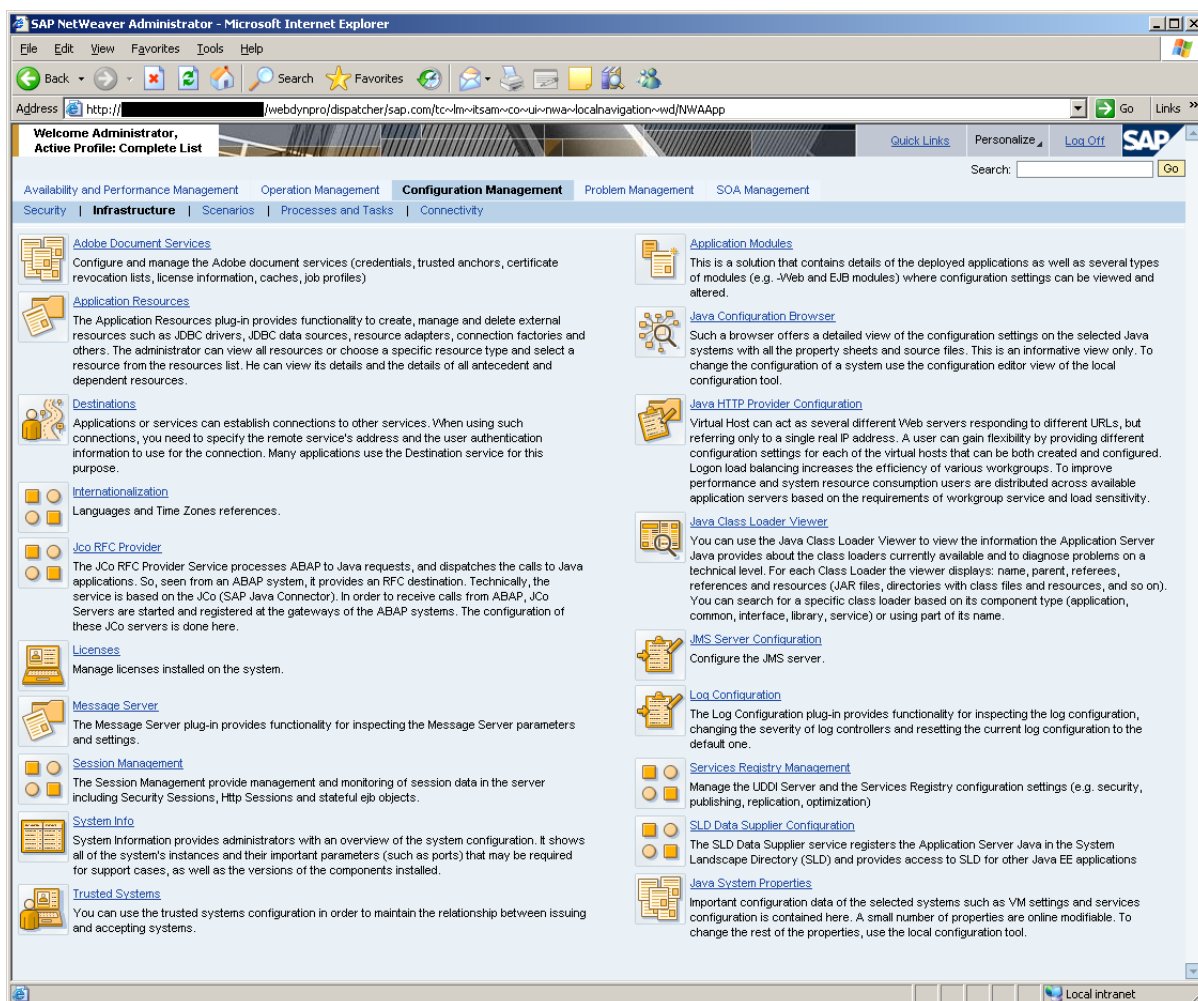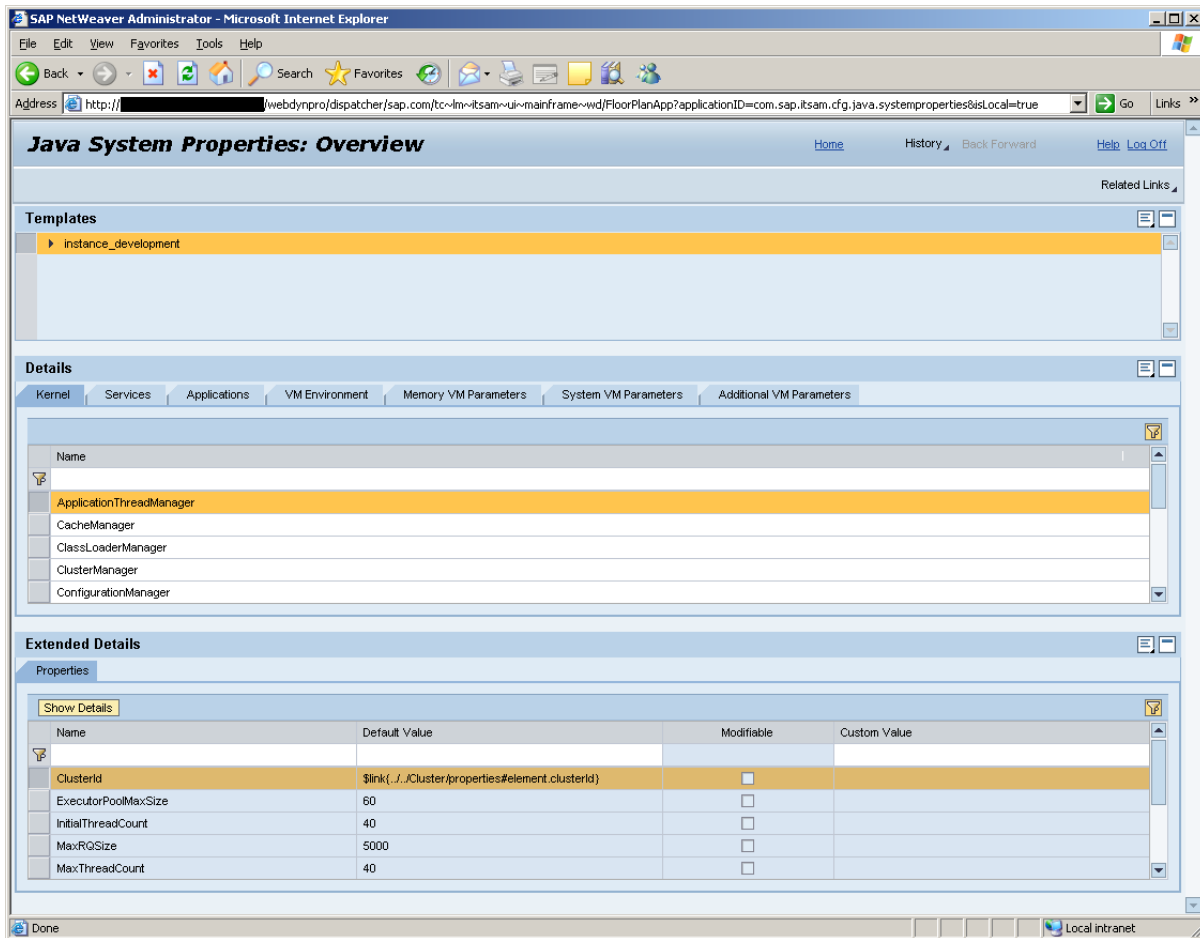| Property	Value

`com.sap.idm.jmx.ac_check_level`	This property is used to specify how to display 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	Value
`com.sap.idm.jmx.crypt.keyfile`	A file holding the 3DES keys, that is, the `Keys.ini` file. See the *SAP NetWeaver Identity Management Security Guide* for details.
	ℹ **Note** If SAP NetWeaver AS Java is not installed on the same host as the Runtime Components, the `Keys.ini` file that is located in the folder `<Identity Center installation directory> /Key` (normally `C:/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. For more information about SAP system directories, see SAP System Directories on UNIX (for SAP NetWeaver versions CE 7.2 EHP1, 7.3, 7.3 EHP1 and 7.4) or Setting Access Privileges for SAP System Directories Under UNIX/LINUX for SAP NetWeaver CE 7.1 EHP1.
`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. ℹ **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.

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring the Identity Management User Interface

PUBLIC   **113**

Property	Value
`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 (that is, the *Self Services* tab is visible by default).

5. To make changes to the configuration, select the property you wish to edit and change (for example, `com.sap.idm.jmx.idstoreid`), and choose *Modify*.
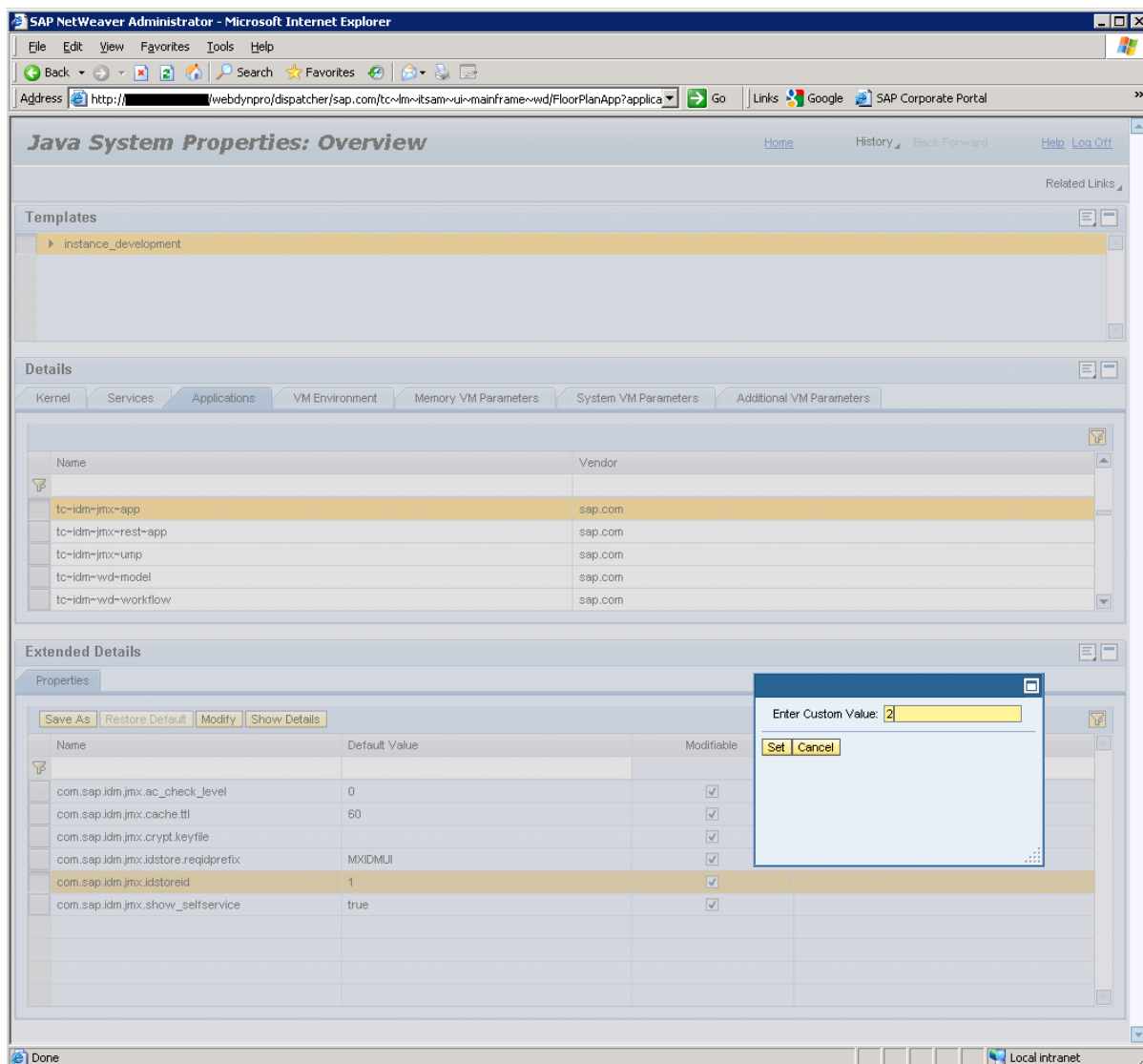
6. Enter the custom value and choose *Set* to change it.

> **i 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:
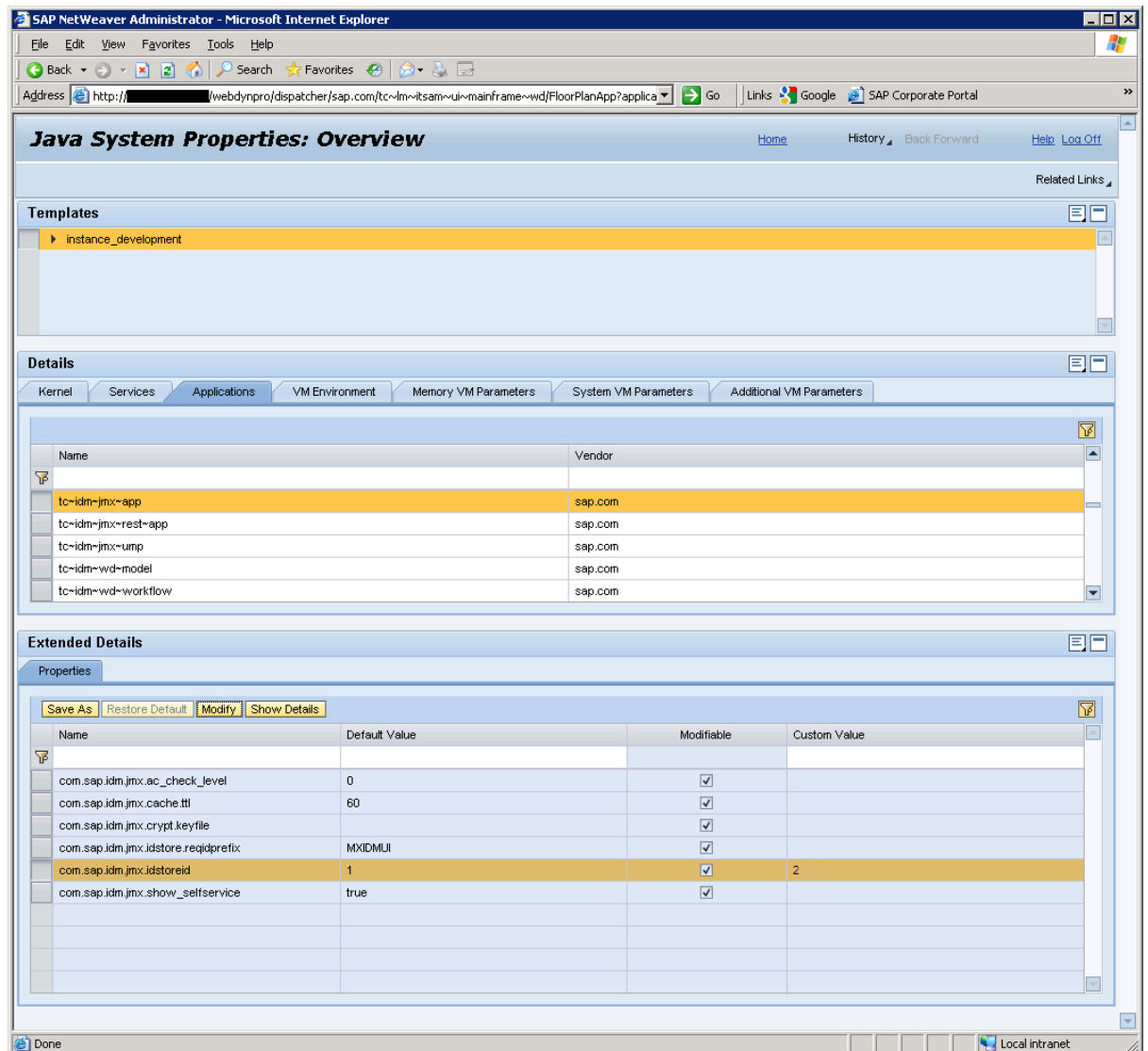
7. Choose *Save As* to confirm the change.

6.6   Initial Configuration

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 *Access to the Identity Management User Interfaces (URLs)* in *SAP NetWeaver Identity Management Security Guide*.

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 *Providing General Access (UME Actions)* and *Providing Specific Access (Identity Management Privileges)* in the *SAP NetWeaver Identity Management Security Guide*.

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

6.6.1 Adding user to the Identity Store

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 Center's identity store. This is not necessary for access to the *Monitoring* tab, that is, it is sufficient that the user exists in UME.

Context

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 Center before or after the role creation is not of importance.

> ℹ️ 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, as described in document *SAP NetWeaver Identity Management Identity Center User management for the Identity Management User Interface*.

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

Procedure

1. In the Identity Center, select the identity store in the console tree and view the identity store properties.
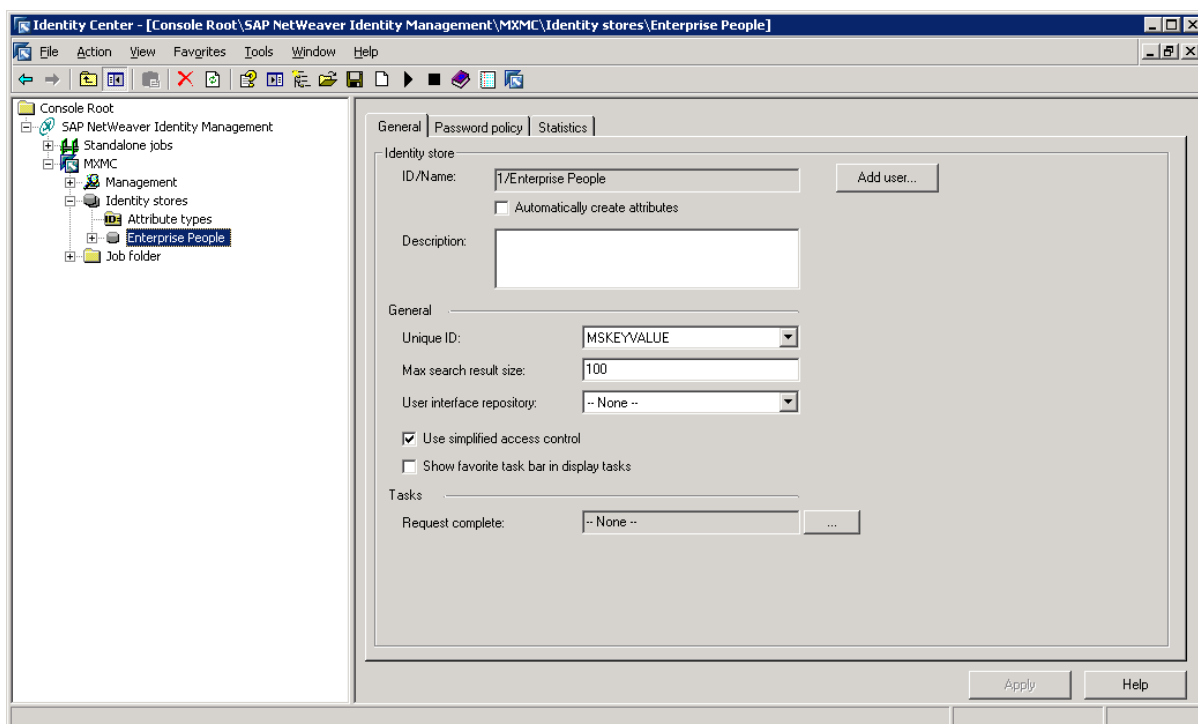
2. Select the *General* tab and choose *Add user…*.
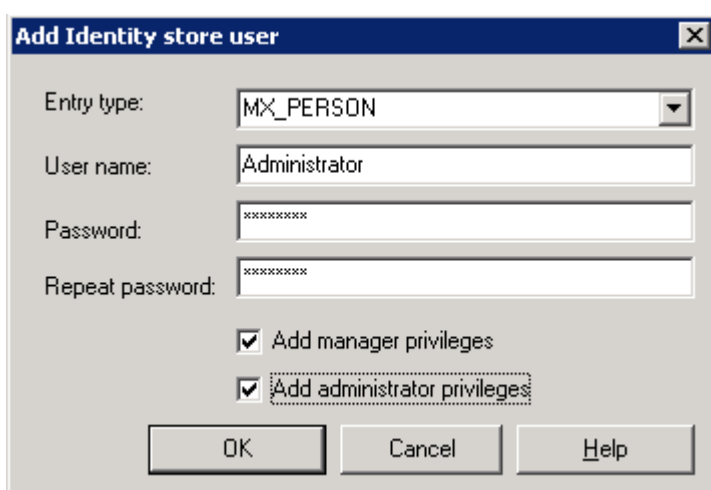
This will open *Add Identity store user* dialog box.

   a. Enter user name and password for the user.

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring the Identity Management User Interface

PUBLIC   **117**

b. Select *Add manager privileges* and/or *Add administrator privileges* to give access to manager/administrator tabs in the 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 create user.

Related Information

6.6.2 General Access (Self Services Tab)

Self service tasks, where users can change its own user data, request the role and so on, 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. In your browser, enter `http(s)://<host>:<port>`. 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).
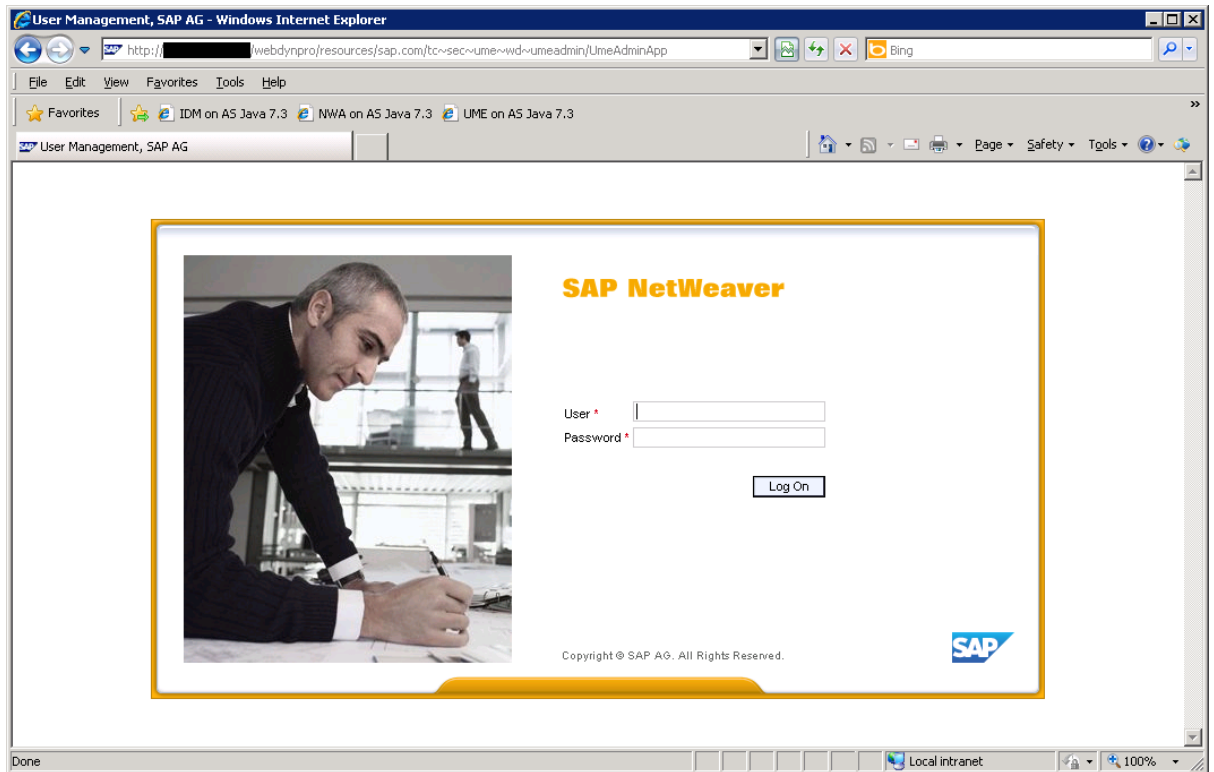
3. Provide your UME credentials and choose *Log on*:
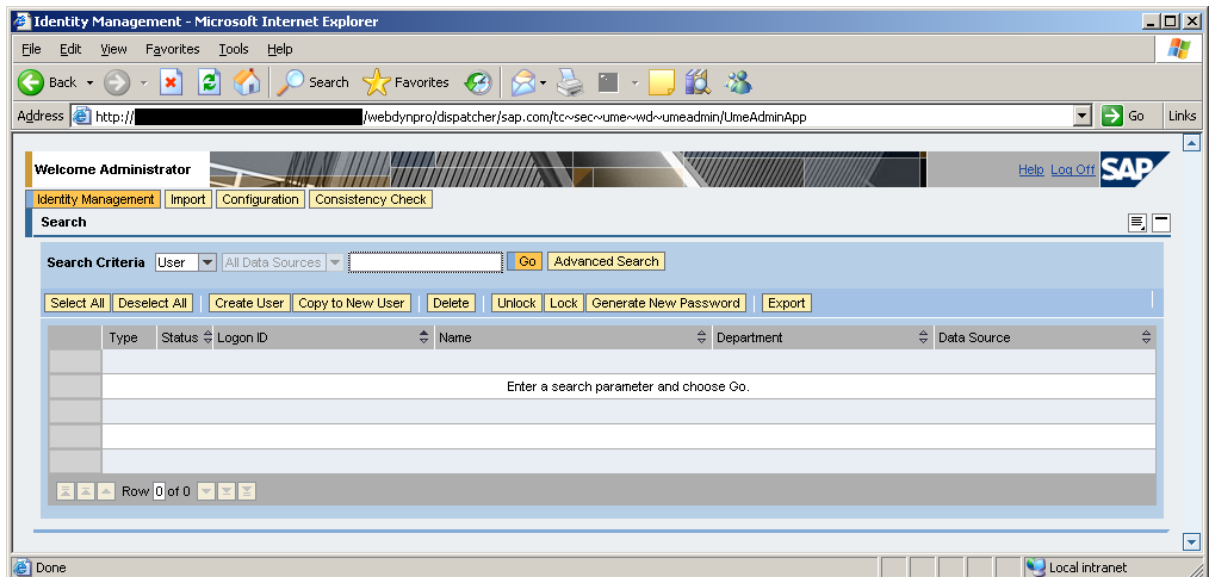
4. Change search criteria to *Role*, and then choose *Create Role*:

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring the Identity Management User Interface

PUBLIC   **119**
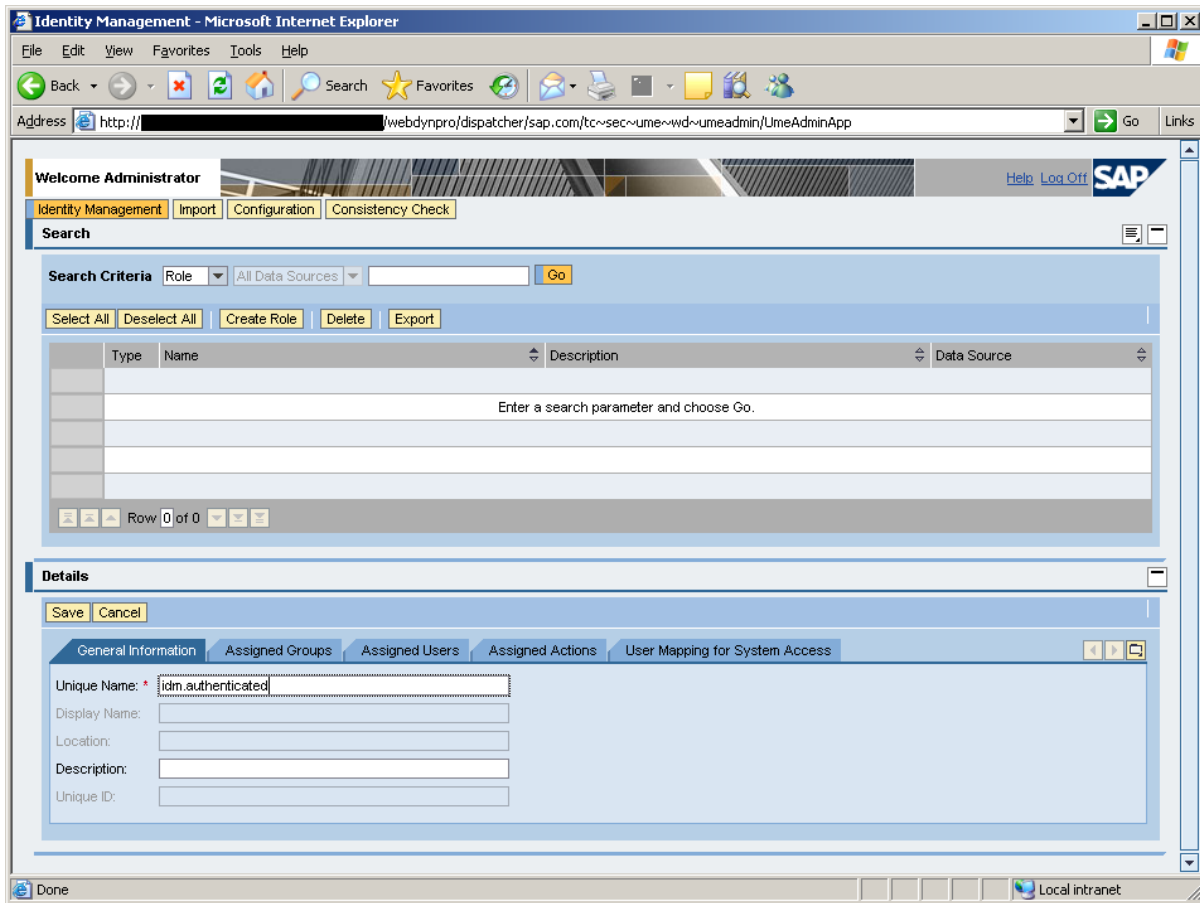
a. On the *General Information* tab fill in the following:

Table 17:

Field	Value
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.

120   P U B L I C

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring the Identity Management User Interface
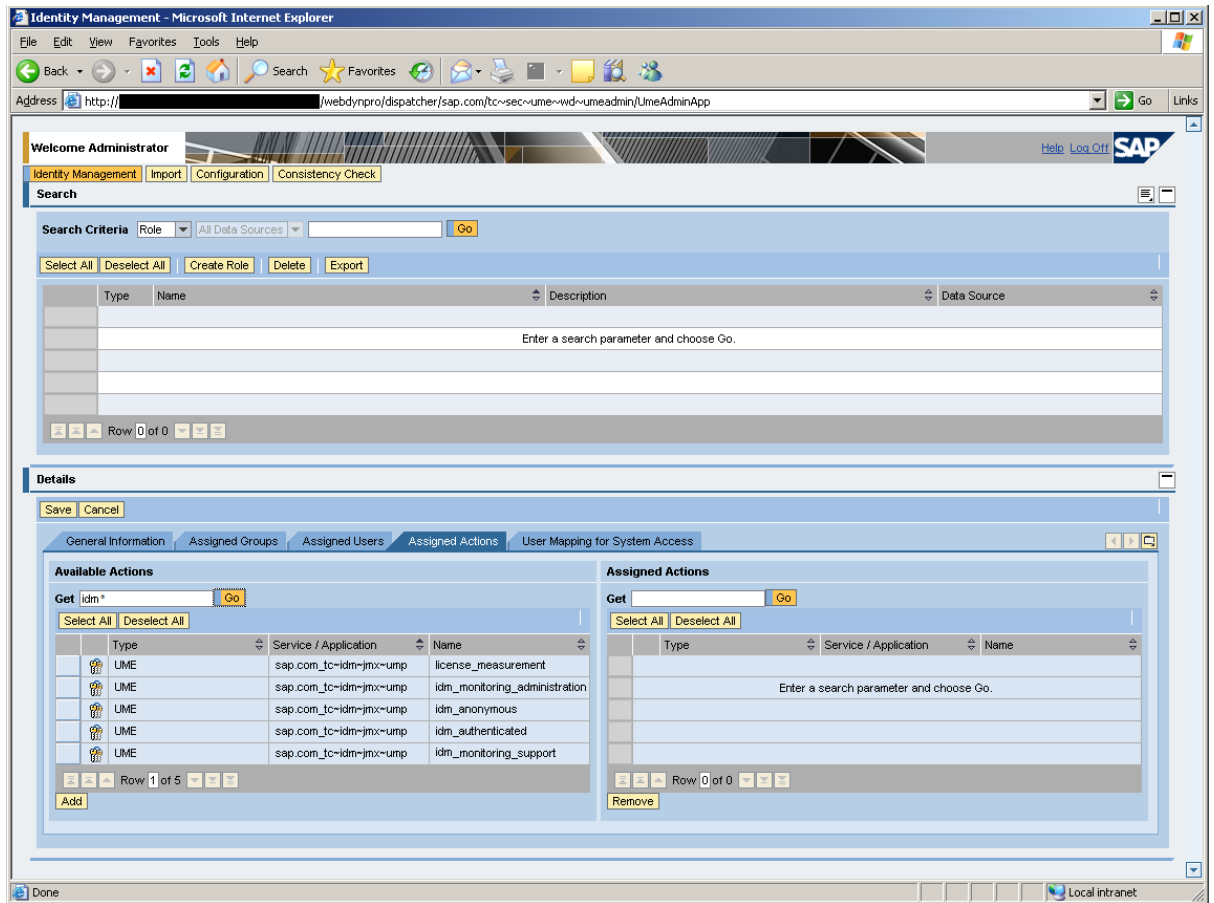
a. In the left pane (*Available Actions*): Type `idm*` in the field *Get* and choose *Go*. This will list the actions/ access rights it is possible to link to the role.

6. Select the `idm_authenticated` action and choose *Add*.
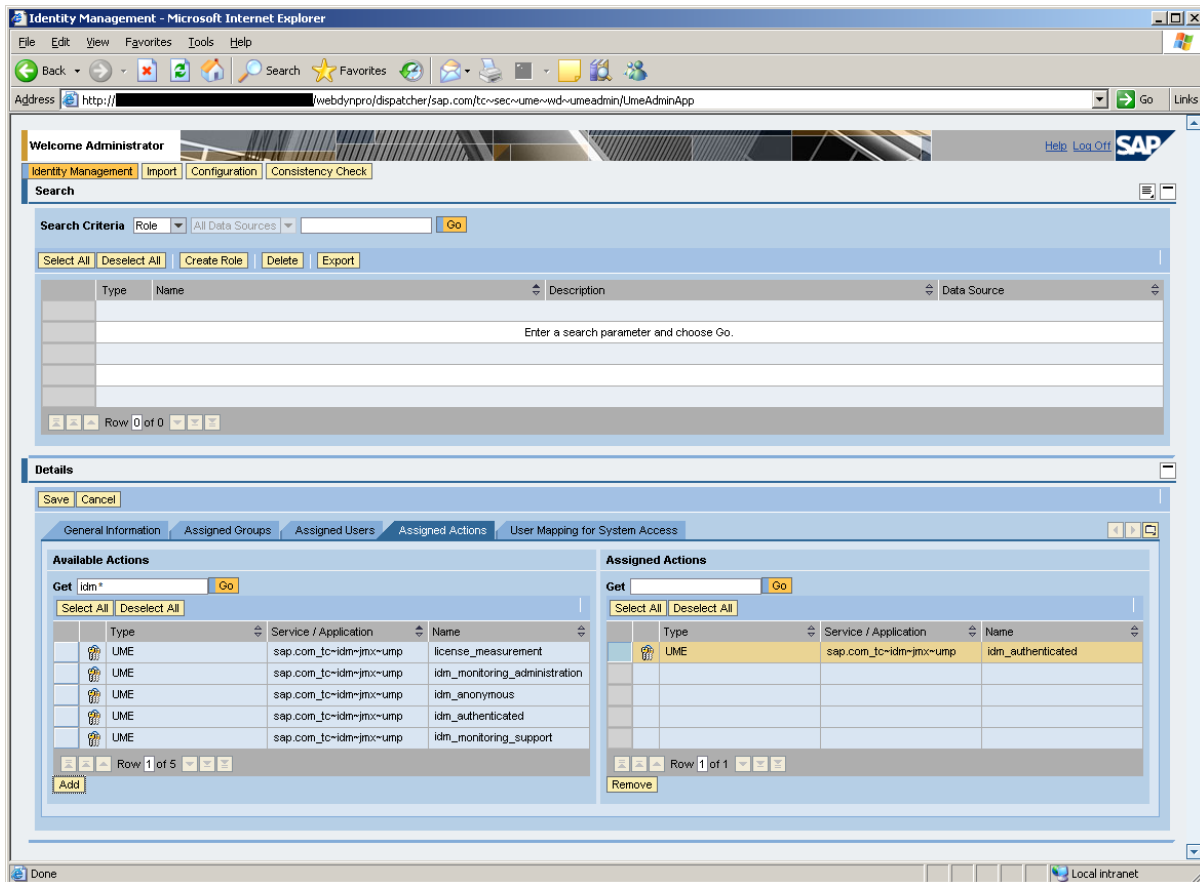
a. The `idm_authenticated` action is now assigned to the role and this will be shown in the right pane (*Assigned Actions*).

7. Select the *Assigned Groups* tab:
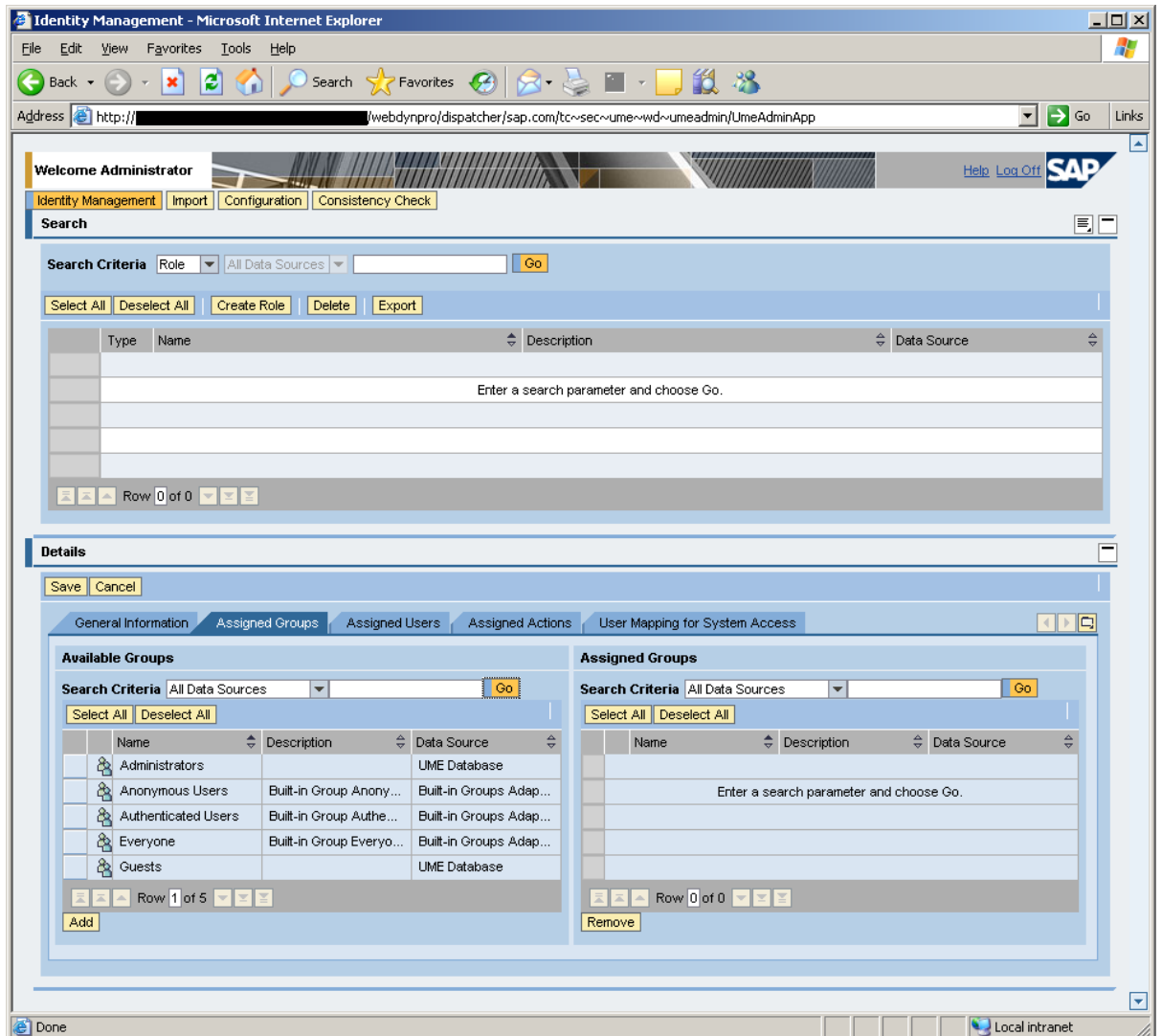
    a. In the *Available Groups* pane, choose *Go* to list all available groups.

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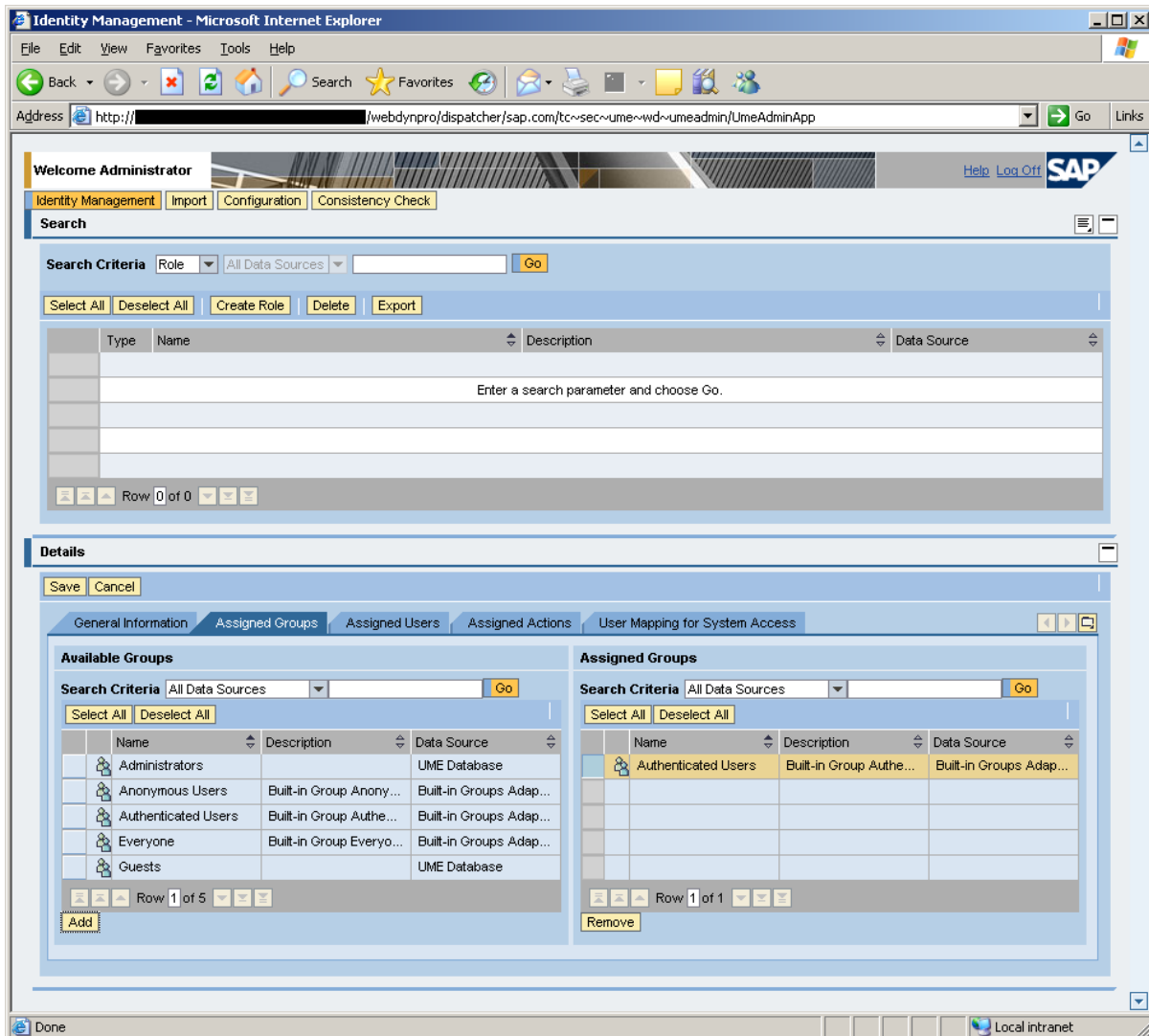
The *Authenticated Users* group is now given the role and this will be shown in the right pane (*Assigned Groups*).

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:
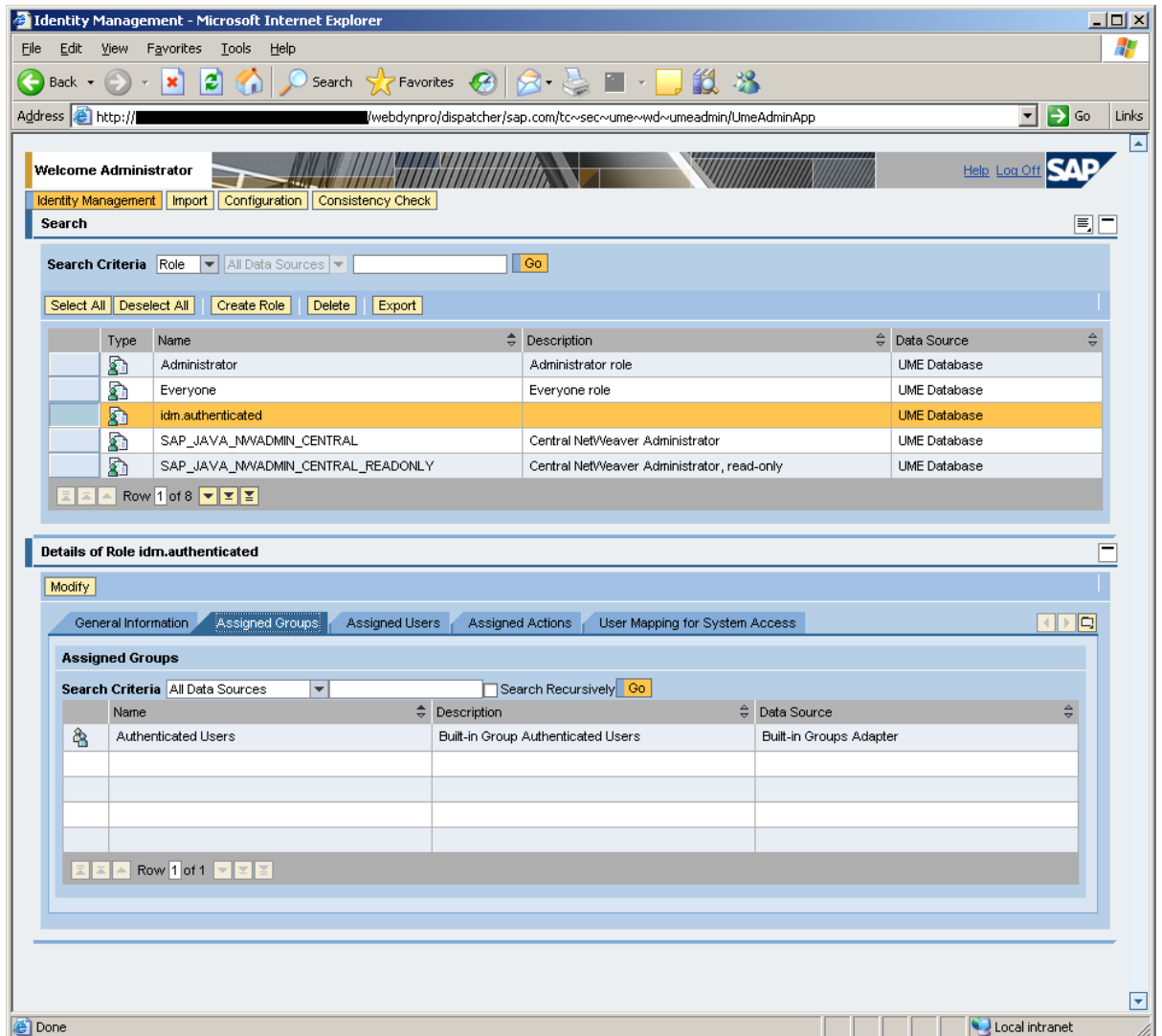
Results

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

6.6.3 Access to Monitoring (Monitoring Tab)

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 *General*

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring the Identity Management User Interface

PUBLIC   **125**

Access (Self Services Tab). Assign the created monitoring role to *Administrators* group or a specific user who needs access to *Monitoring* tab in the 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 *Monitoring of Identity Management* section in *SAP NetWeaver Identity Management Solution Operation Guide*.

Related Information

6.6.4 Configuring the Language Settings for the Identity Management User Interface

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

Context

Follow the steps below:

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. Select 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.

   > ℹ **Note**
   >
   > If you have configured customized favorite buttons in the 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.

6.6.5 General Access to Identity Management User Interface

Context

To access the User Interface do the following:

Procedure

1. In your browser, enter `http(s)://<host>:<port>/idm`.
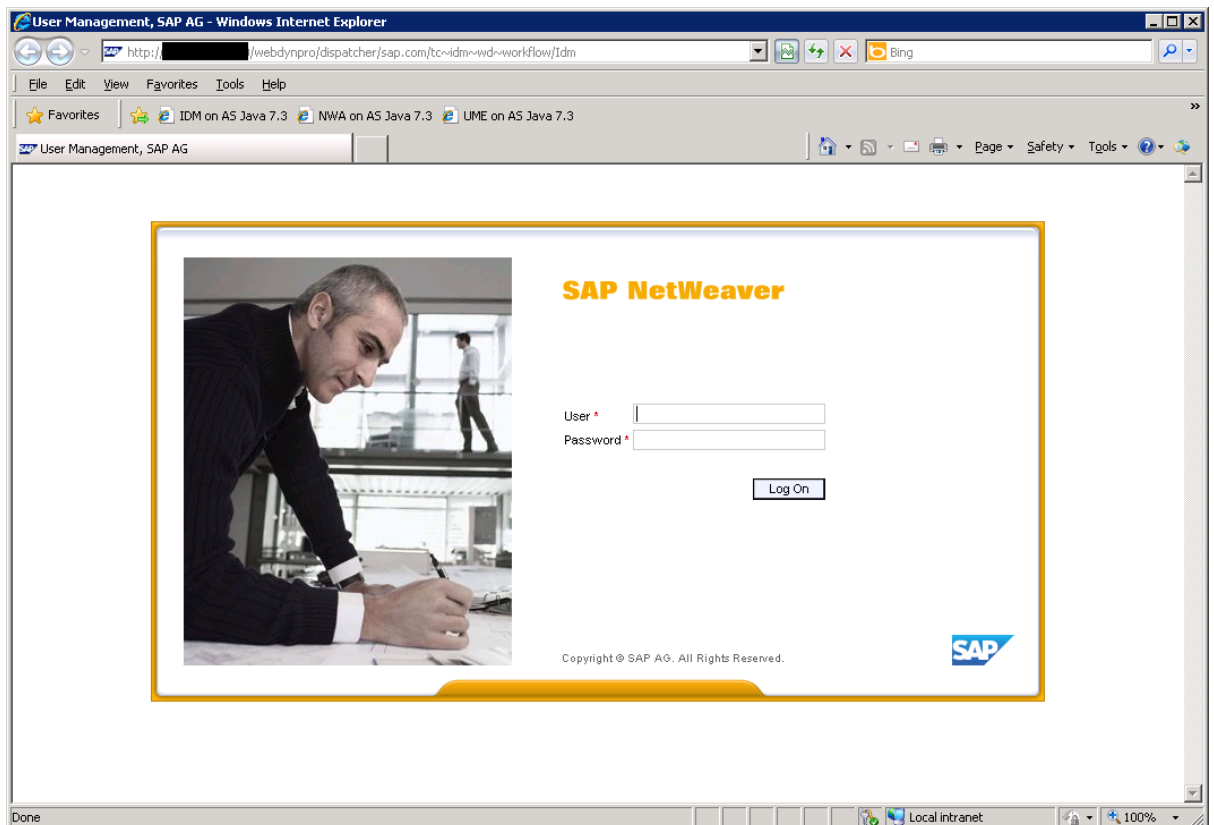
   a. Provide the credentials in the log-in window.
2. Choose *Log on*.
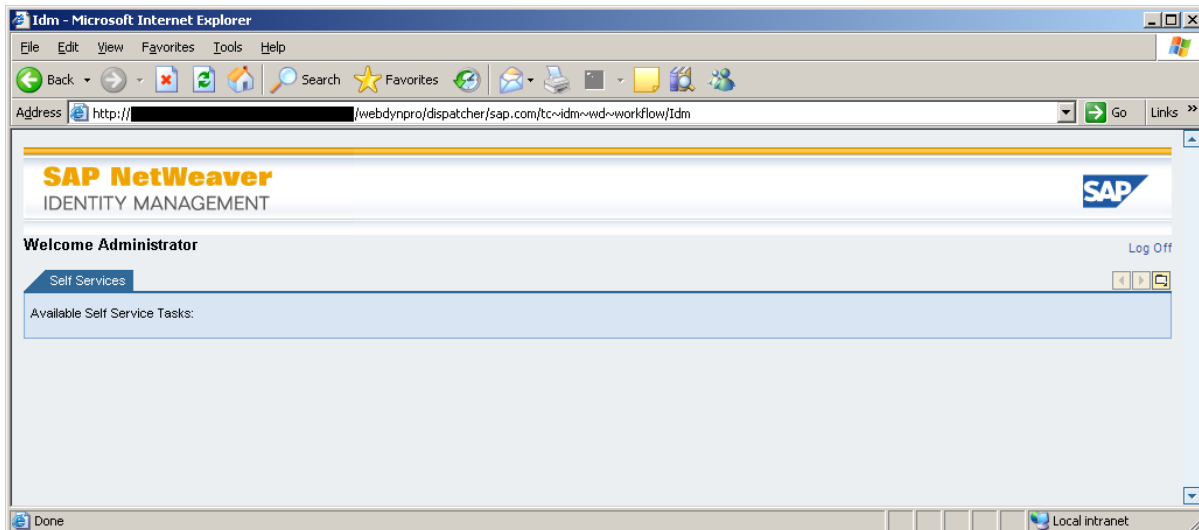
Results

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

6.6.6 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 in the Identity Center's identity store to the person entries.

Context

> **i Note**
>
> For more details about each privilege, see *Providing Specific Access (Identity Management Privileges)* section in the *SAP NetWeaver Identity Management Security Guide*.

In *Adding User to the Identity Store*, the manager and administrator privileges (all) are given the admin user automatically by selecting *Add manager privileges* and *Add administrator privileges* when adding the user to the

identity store. But these privileges can be also be assigned to users manually and on the need-to basis, for instance by creating a self service task for privilege assignment. You can do it following the steps below:

Procedure

1. In the Identity Center, select the identity store and choose ▶ *New* ❯ *Folder* ❯ from the context menu to create a new folder.
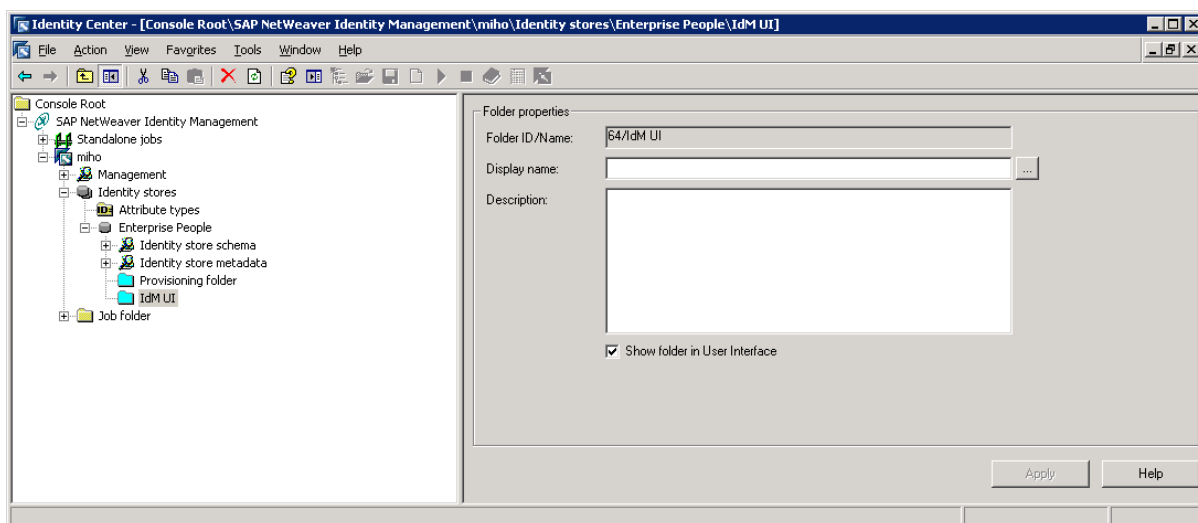
   a. Rename the folder to `IdM UI`.

2. Select the folder and choose ▶ *New* ❯ *Ordered task group* ❯ from the context menu.
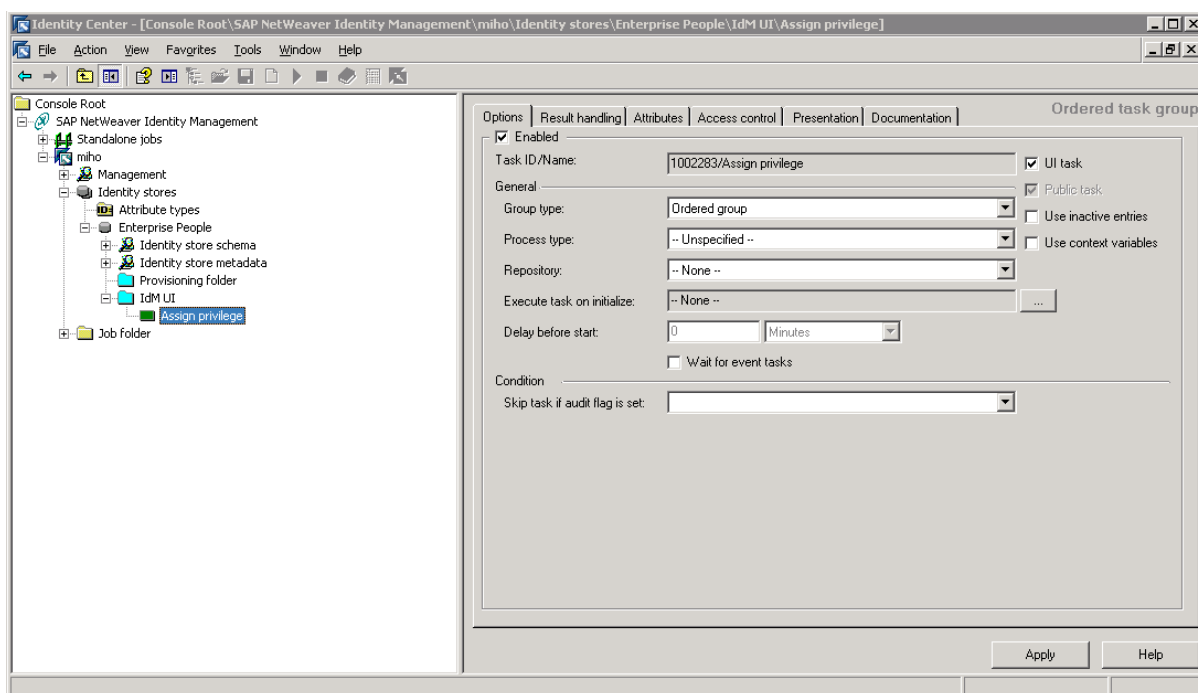
a. Rename the task to `Assign privilege`.

b. Select the *UI task* option.

3. Select the *Attributes* tab:
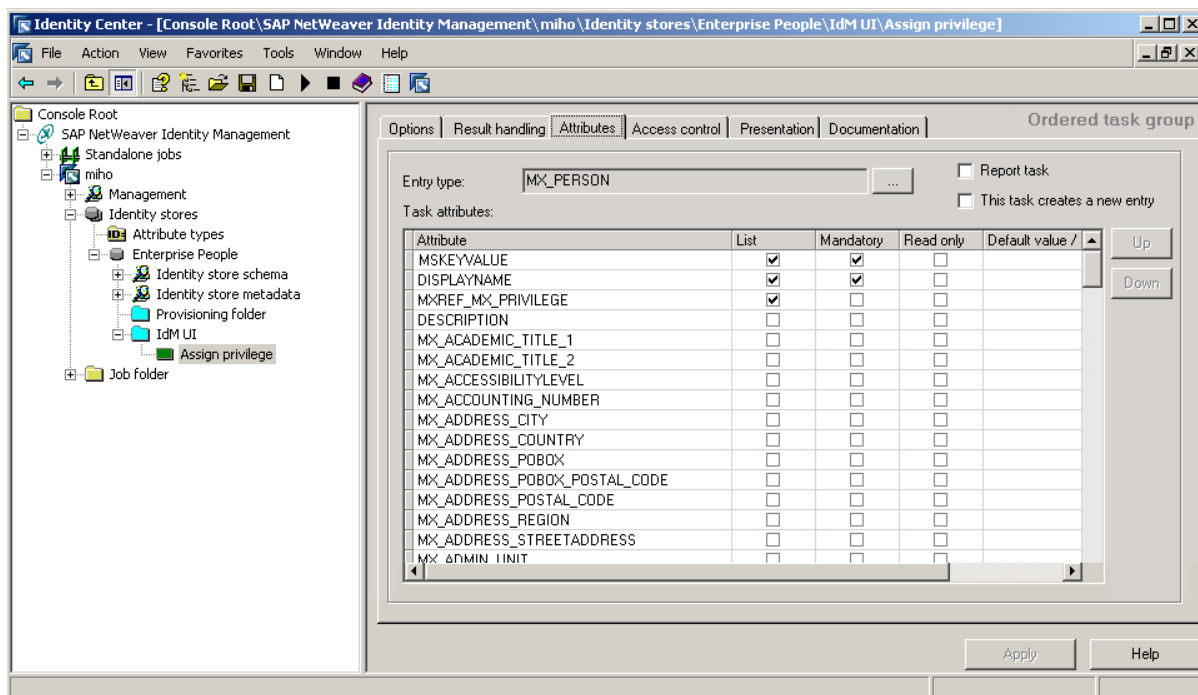
a. Fill in the following:

Table 18:

Field	Value
Entry type	Select MX_PERSON entry type. Choose [...] to open a dialog box from which you select the entry type. ℹ **Note** A dialog box will appear asking you to confirm your choice. Choose *Yes* to confirm and to close the dialog box.
Task attributes	The attributes MSKEYVALUE and DISPLAYNAME are already selected. Select the attribute MXREF_MX_PRIVILEGE. Use *Up* or *Down* to list the selected attributes in the same order as shown above.

4. Choose *Apply*.

5. Select the *Access control* tab.

6. Choose *Add*.

a. Fill in the following:

Table 19:

Field	Value
Allow access for	Select *Logged-in user or identity store entry*.
ID store	Select the correct identity store. In this example *Enterprise People* is used.
Name	Leaving this field empty will make the task accessible to everyone. Name is entered when restricting the access to the task (for example, 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.

7. Choose *OK*.
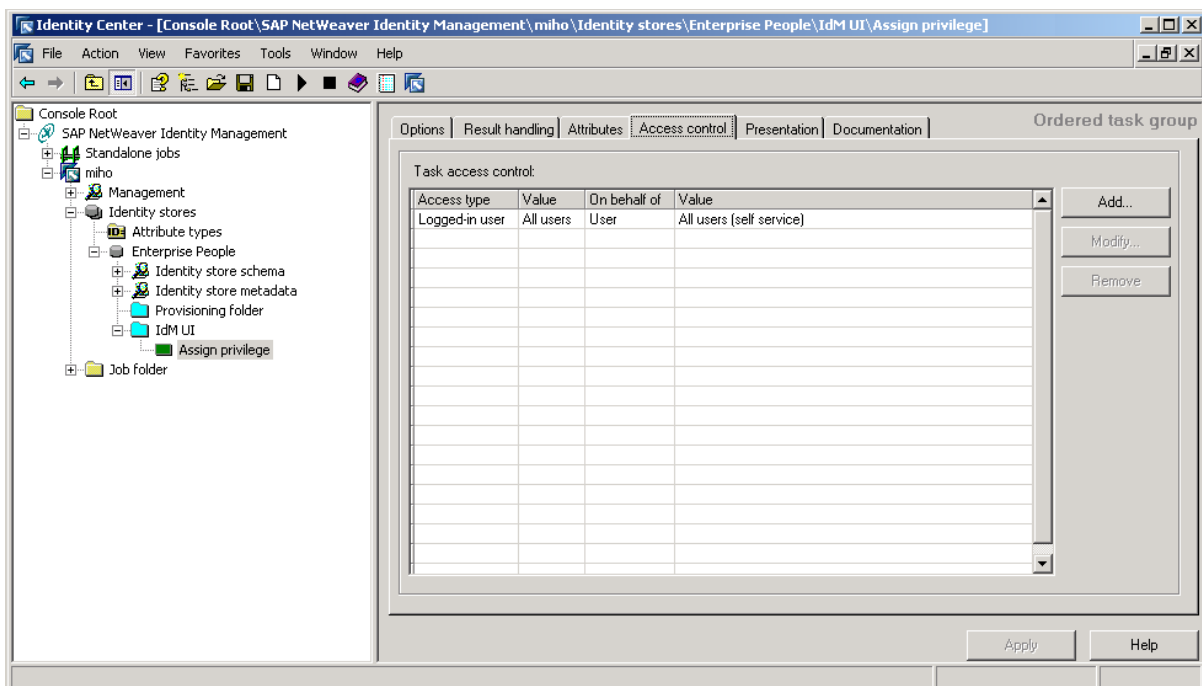
8. Choose *Apply*.

Results

Now the self service task is created and is visible in the *Self Services* tab of the User Interface:
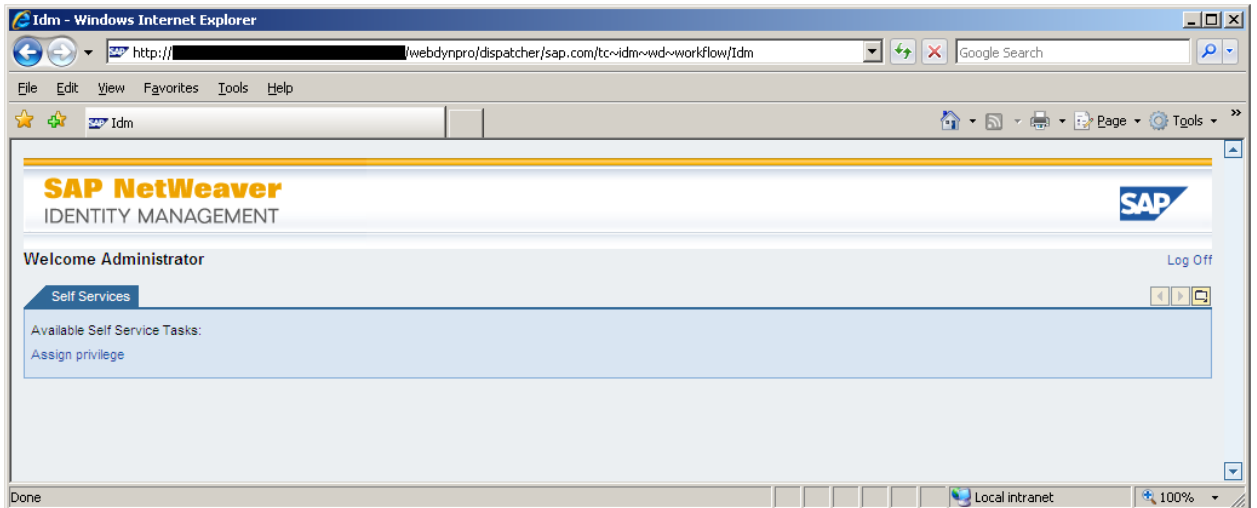
To assign privileges and give access to other tabs than *Self Services*, do the following:

1. Select the task.
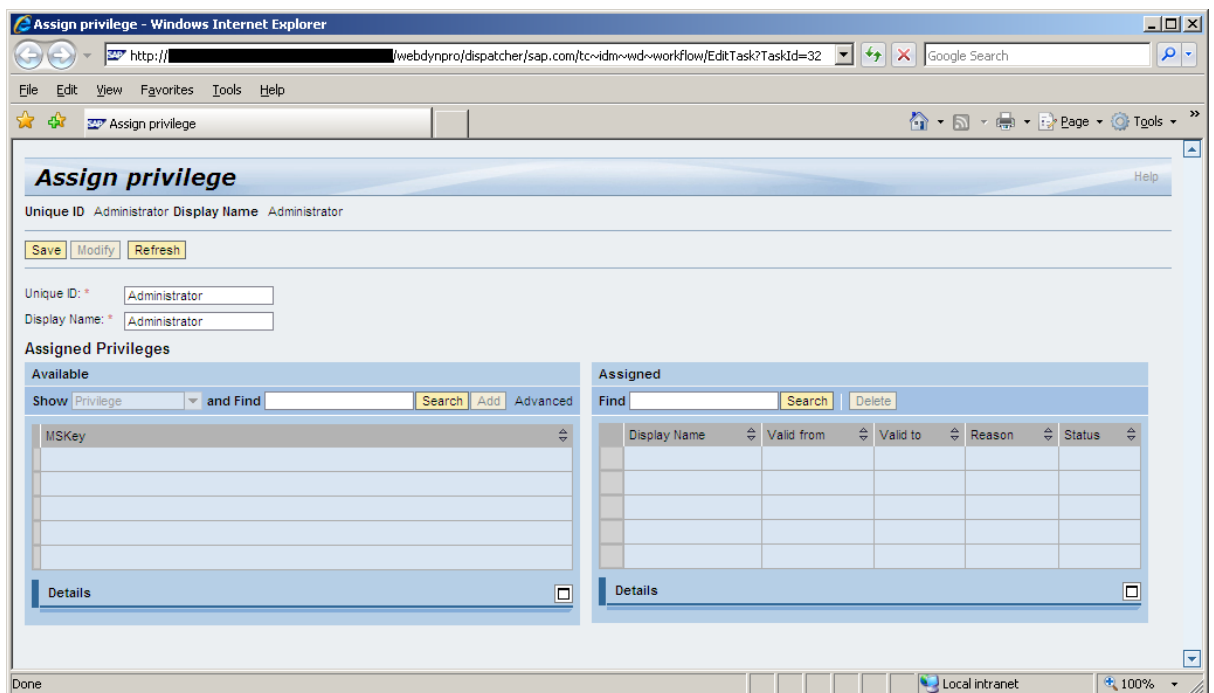
The task will open in a new window.

> **i Note**
>
> If you are using Internet Explorer 7 or later, you can open the task in a new tab instead of the new window. To enable this option in your browser, choose *Tools/Internet Options*, and in the *Tabs* section of the *General* tab, choose *Settings* where you select the option *Always open pop-ups in a new tab* or similar. If you are using Mozilla Firefox, the task will open in a new tab by default.

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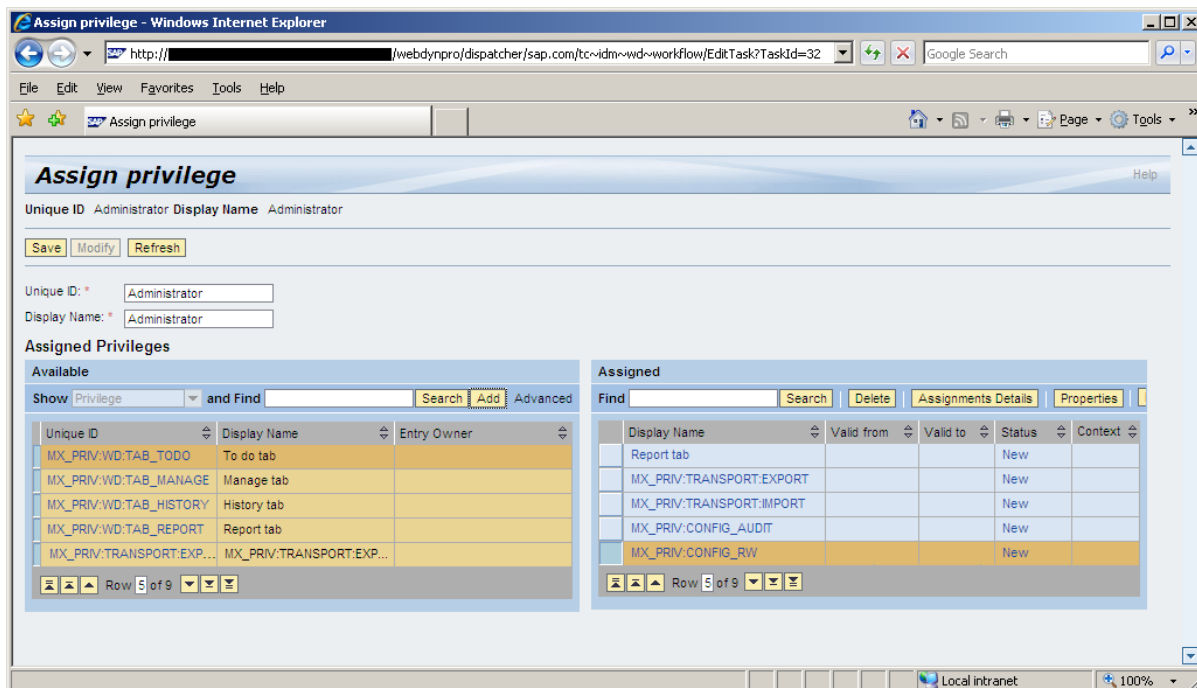
> **i Note**
>
> When searching for any specific entry (persons, roles, privileges and so on) in the Identity Management User Interface, make sure you always provide the language-specific characters of that entry. For example: To search for an entry containing an accented **é**, you should type **é**.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

   1. Select the desired privileges (multi-select is possible).
3. Choose `Add`.
4. Choose `Save` and close the task.
   The privileges are now added and the tabs should be visible in the Identity Management User Interface.

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

* For the URL `http(s)://<host>:<port>/idm`:
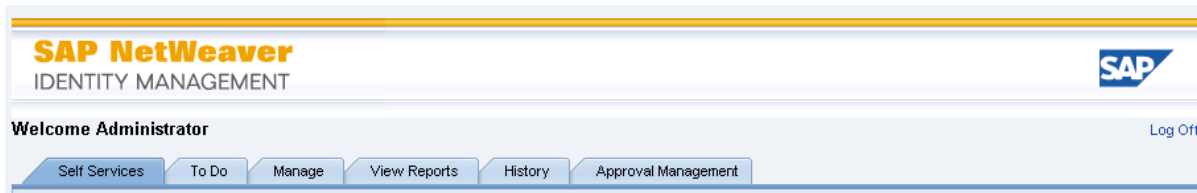
* For the URL `http(s)://<host>:<port>/idm/admin`:
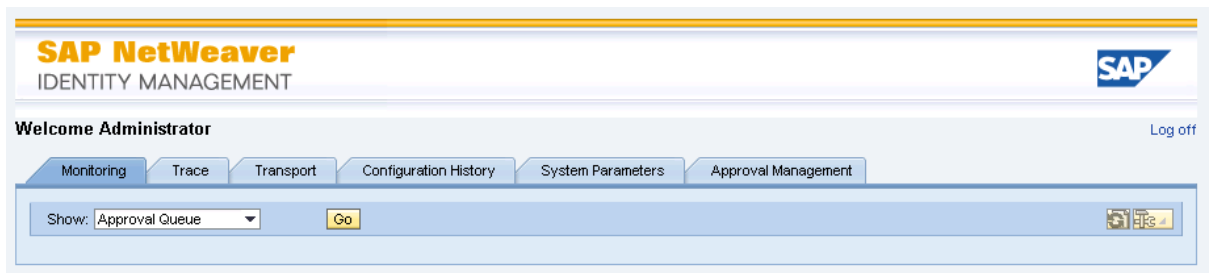
6.7 Customizing the Web Dynpro Java Applications

As a Web Dynpro application, SAP NetWeaver Identity Management User Interface may be adapted. You can define a specific theme (the look and feel) of your User Interface application or create and activate keyboard access for User Interface elements.

Related Information

Defining Customer Specific Themes for Web Dynpro Applications [page 135]
Keyboard Access for User Interface Elements in Web Dynpro [page 136]

6.7.1 Defining Customer Specific Themes for Web Dynpro Applications

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 section.

Related Information

Configuring the Web Dynpro Runtime Environment for SAP NetWever 7.0
Setting the Theme for SAP NetWever 7.0
Configuring the Web Dynpro Runtime Environment for SAP NetWeaver CE 7.1 EHP 1
Setting the Theme for SAP NetWeaver CE 7.1 EHP 1
Configuring the Web Dynpro Runtime Environment for SAP NetWeaver CE 7.2

6.7.2 Keyboard Access for User Interface Elements in Web Dynpro

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 following information (for supported SAP NetWeaver versions) in the Related Information section.

Related Information

Keyboard Access for UI Elements in Web Dynpro for SAP NetWeaver 7.0
Enabling User Interaction for SAP NetWeaver CE 7.1 EHP 1
Enabling User Interaction for SAP NetWeaver CE 7.2
Keyboard Access for Web Dynpro for ABAP / for Java for SAP NetWeaver 7.3
Keyboard Access for Web Dynpro for ABAP / for Java for SAP NetWeaver 7.3 EHP 1
Keyboard Access for UI Elements in Web Dynpro (New Rendering) for SAP NetWeaver 7.4

6.8 Integrating Identity Management User Interface in the SAP NetWeaver Portal

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

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

- Import the predefined content for the SAP NetWeaver Portal.

- Check the Portal integration of the Identity Management User Interface.

Related Information

Importing Predefined Contents for the SAP NetWeaver Portal [page 137]
Verifying the Portal Integration of the Identity Management User Interface [page 138]

6.8.1 Importing Predefined Contents for the SAP NetWeaver Portal

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 section.

Related Information

Import and Deployment for SAP NetWeaver 7.0
Import and Deployment for SAP NetWeaver CE 7.1 EHP 1
Importing and Deploying EPA Archives for SAP NetWeaver CE 7.2
Importing and Deploying EPA Archives for SAP NetWeaver 7.3
Importing and Deploying EPA Archives for SAP NetWeaver 7.3 EHP 1
Importing and Deploying EPA Archives for SAP NetWeaver 7.4

6.8.2 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 NetWeaver 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.

> **i 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.

If everything is done correctly, the contents of the Identity Management User Interface will be presented under the *Identity Management* tab in the SAP NetWeaver Portal. The content will be something similar to the one shown below:
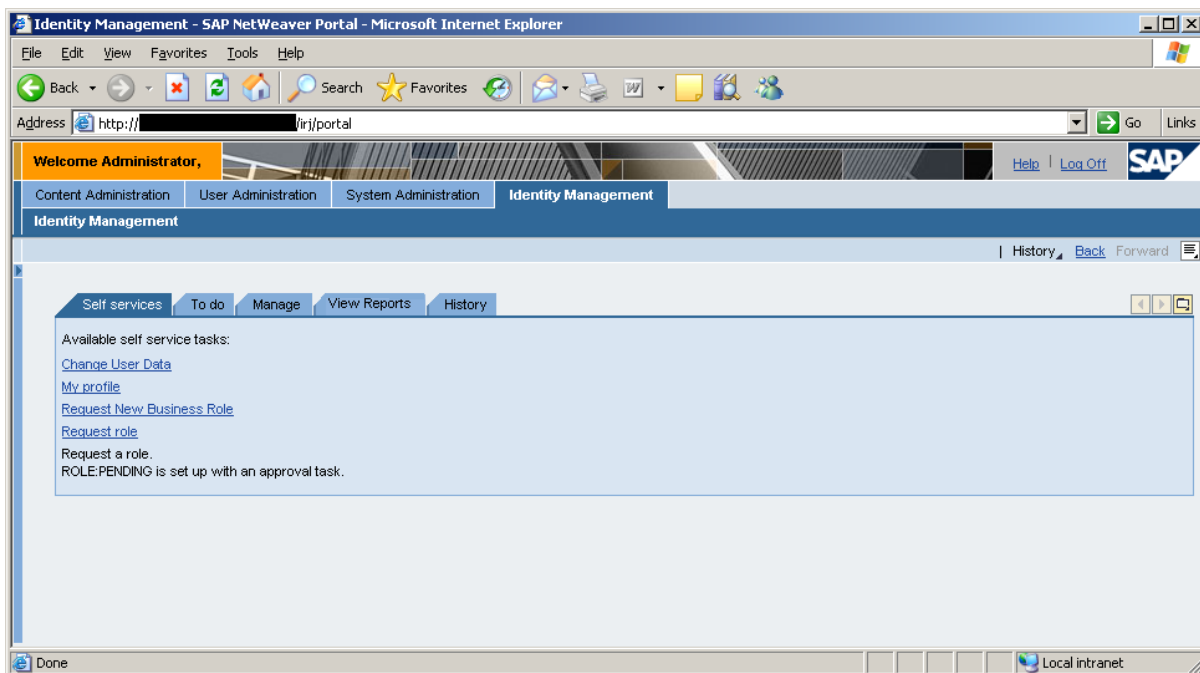
Related Information

7 Installing and Configuring SAP NetWeaver Identity Management User Interface for HTML5

This section describes how to install and configure the SAP NetWeaver Identity Management User Interface for HTML5.

SAP NetWeaver Identity Management User Interface for HTML5 is a user interface based on HTML5 and JavaScript, and developed using the SAP UI Development toolkit for HTML5 (SAPUI5). It also uses SAP Identity Management REST Interface Version 2.

SAP NetWeaver Identity Management User Interface for HTML5 can be used by all users to maintain their own profile information and request new roles (self-service). Authorizations are grouped into business roles, again made available to end-users, who can request assignment of the business roles. SAP NetWeaver Identity Management User Interface for HTML5 only supports assignment requests for business roles, that is, users cannot request privilege assignments.

Managers and administrators can also use SAP NetWeaver Identity Management User Interface for HTML5 for role request approvals. Although privilege assignment requests from the users are not supported, the *My Approvals* page supports approving and declining both business role assignments and privilege assignments for managers and administrators, to support cases in which approval workflows are set up for individual privileges, triggered either by automated processes or other UIs or APIs.

SAP Identity Management User Interface for HTML5 does not support attestations, hence on the *My Approvals* page are shown only approvals. The attestations are available only from the SAP Identity Management REST Interface Version 2.

SAP UI Development Toolkit for HTML5 (SAPUI5)

The SAP UI Development Toolkit for HTML5 (SAPUI5) is SAP's new enterprise-ready HTML5 rendering library for client-side UI rendering and programming. It combines the advantages of being open and flexible as well as being enterprise ready, supporting all SAP Product Standards. While Web Dynpro is best suited to heavyweight transactional applications for expert usage, SAPUI5 is designed for building lightweight consumer-grade UIs for casual usage. It is aimed at developers at SAP and customers with web development skills (HTML, CSS3, JavaScript). SAPUI5 provides extensible controls and powerful theming but is easy to consume, based on open standards, and integrates with third-party JavaScript libraries. SAPUI5 applications run on a wide range of devices (smartphone, tablet, and desktop) and on multiple server platforms.

SAP NetWeaver Identity Management REST Interface Version 2

The SAP NetWeaver Identity Management REST Interface offers a remote interface to SAP NetWeaver Identity Management and its data, that is, it allows you to use custom user interfaces (UIs) that access the SAP NetWeaver Identity Management data.

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring SAP NetWeaver Identity Management User Interface for HTML5

140 PUBLIC

For more information about the Identity Management REST Interface Version 2, see *SAP NetWeaver Identity Management REST Interface Version 2*.

Related Information

SAP Identity Management REST Interface Version 2
UI Development Toolkit for HTML5 Developer Center (SAP Developer Center)
A Vocabulary and Associated APIs for HTML and XHTML (W3C Editor's Draft)
SAP Identity Management REST Interface Version 2
Virus Scan Interface [page 147]
Prerequisites [page 141]
Installation and Configuration Process [page 142]
Restrictions and Considerations [page 151]

7.1 Prerequisites

Before you can install and configure the Identity Management User Interface for HTML5, a set of prerequisites needs to be fulfilled.

The following is the list of prerequisites that need to be fulfilled.

You should have the following knowledge:

- Thorough knowledge about SAP NetWeaver AS for Java and its tools.
- Thorough knowledge about SAP NetWeaver Identity Management, and Identity Center in particular.

The following software is required:

- SAP NetWeaver 7.3 SP9 Patch 1 and higher, or SAP NetWeaver 7.3 including Enhancement Package 1 (EHP1) SP6 Patch 3 and higher (on which SAP NetWeaver Identity Management User Interface and SAP NetWeaver Identity Management User Interface for HTML5 are to be deployed).
- SAP NetWeaver Identity Management Identity Center version 7.2 SP8 or higher, must be correctly installed and licensed.
- An Identity Center where at least one dispatcher is configured and running (see *SAP NetWeaver Identity Management Identity Center: Initial Configuration*).
- SAP NetWeaver Identity Management User Interface is installed and configured in accordance with *Installing and Configuring the Identity Management User Interface* section.
- SAP NetWeaver Identity Management REST Interface Version 2 is deployed on your AS Java (where the SAP NetWeaver Identity Management User Interface is deployed) in accordance with *SAP NetWeaver Identity Management REST Interface Version 2*.
- SAPUI5 library is required. The required library is available as an AS Java Extension for the SAP NetWeaver version you are using (versions 7.3 SP9 Patch 1 and higher, or EHP1 for SAP NetWeaver 7.3 SP6 Patch 3 and higher). 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 (SUM).

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring SAP NetWeaver Identity Management User Interface for HTML5

PUBLIC **141**

> **i Note**
>
> To locate the correct SAPUI5 library, choose the following path 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* ▐.

Related Information

Identity Center Installation Overview [page 7]
Installing and Configuring the Identity Management User Interface [page 84]
SAP NetWeaver Identity Management Identity Center Initial Configuration
SAP Identity Management REST Interface Version 2
SAP Software Download Center🔗
Using the Software Update Manager (SUM)

7.2 Installation and Configuration Process

When all prerequisites are fulfilled, you can start the installation and configuration of the Identity Management User Interface for HTML5.

The process of installing and configuring the Identity Management User Interface for HTML5 involves completing 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 user interface tasks in the Identity Center Management Console and configuring the solution
- Deploying the Identity Management User Interface for HTML5 on your AS Java
- Accessing the Identity Management User Interface for HTML5

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

To access the REST API v2, the user requires the UME actions `idm_authenticated` and `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

142   P U B L I C

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring SAP NetWeaver Identity Management User Interface for HTML5

`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 UI task.

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.

7.3.1 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`, `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 in User Management Engine (UME) for SAP NetWeaver 7.3](#)
[Administration of Users and Roles in User Management Engine (UME) for SAP NetWeaver 7.3 EHP1](#)

7.3.2 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

7.4 Adding the Predefined User Interface Tasks 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 User Interface tasks in the Identity Center Management Console. You need to import predefined User Interface tasks into the Identity Center Management Console. You should not change the User Interface, and therefore should not delete, replace, or modify the imported, predefined User Interface tasks in any way.

Some configuration is required for the solution.

7.4.1 Importing the Task Folder

Context

The file `UI tasks for HTML5.mcc` contains a folder with the predefined User Interface tasks. To import the folder, proceed as follows:

Procedure

1. In the Identity Center Management Console, select the identity store node in the console tree (by default, *Enterprise People*) and choose *Import...* from the context menu.
2. Navigate to the directory `<Identity Center install directory>/Templates/Identity Center/UI for HTML5` and select the file `UI tasks for HTML5.mcc`.
3. Choose *Open*. The *SAP NetWeaver Identity Management Configuration Copy Tool* dialog box appears.
4. Select the option *Link tasks into display- and event properties on entry types and attributes* and make sure that *Import* is selected.
5. Select the *Advanced* tab and make sure that a dispatcher is selected for the imported tasks.
6. Choose *Next >* and then *Import*.
7. When the import is completed, choose *Finish*. Alternatively, to view the details about the completed import, choose *View logfile* before choosing *Finish*.

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring SAP NetWeaver Identity Management User Interface for HTML5

144   PUBLIC

Results

The imported folder with all the User Interface tasks is added to the Identity Center identity store (you may have to refresh the console tree before it is visible):

The imported folder contains the following User Interface tasks:

Name of the UI task	Description
Display Identity	Displays the details of an identity entry. For future use.
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.
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.
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.
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.
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.

Do not delete, replace, or modify the imported, predefined User Interface tasks in any way.

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring SAP NetWeaver Identity Management User Interface for HTML5

PUBLIC   **145**

> ### i Note
>
> The imported tasks cannot be deleted or replaced by any similar tasks in the configuration, because the task GUIDs are referred to directly in the code of the user interface.

> ### i Note
>
> Do not modify the imported tasks to include new attributes.

> ### i Note
>
> Do not modify access control for the predefined tasks.

7.4.2 Configuring the Solution

To use the predefined User Interface tasks 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 task.
- Maintain the values for the attribute `MX_BUSINESS_AREA` for the entry type `MX_ROLE`.
- View the access control defined for the User Interface tasks.
- Activate HTTPS (the use of SSL) on your AS Java.

7.4.2.1 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.

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring SAP NetWeaver Identity Management User Interface for HTML5

146   PUBLIC

Procedure

1. Select and open the entry type *MX_ROLE* in the console tree of the Identity Center Management Console (under the *Entry types* node of the identity store schema) to view the entry type's properties.
2. Select the *Attributes* tab.
3. Find the `DESCRIPTION` attribute and select the *List* option.
4. Choose *OK* to save and close the dialog box.

7.4.2.2 Maintaining the Attributes for the My Data Task

The My Data task 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 User Interface task 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 on 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 *SAP NetWeaver Identity Management for SAP System Landscapes: Configuration Guide*.

Related Information

[SAP Identity Management for SAP System Landscapes: Configuration Guide]

7.4.2.2.1 Virus Scan Interface

Uploading of user pictures into 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

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring SAP NetWeaver Identity Management User Interface for HTML5

PUBLIC **147**

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 NetWeaver Identity Management REST Interface Version 2*.

Related Information

Virus Scan Interface for SAP NetWeaver 7.3 (SAP Help Portal)
Virus Scan Interface for SAP NetWeaver 7.3 EHP1 (SAP Help Portal)
SAP NetWeaver Identity Management REST Interface Version 2

7.4.2.3 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 task, which retrieves and updates the details about the assigned roles and requested new roles for a user. The *My Requests* page of the User Interface allows the filtering of roles by business area.

7.4.2.4 Access Control for the Tasks

Do not modify access control for the predefined tasks.

7.4.2.5 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 User Interface 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.

148   PUBLIC

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring SAP NetWeaver Identity Management User Interface for HTML5

Proceed as follows:

Procedure

1. Follow the steps described in *Configuring the Use of SSL on the AS 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

Configuring the Use of SSL on the AS Java for SAP NetWeaver 7.3
Configuring the Use of SSL on the AS Java for EHP 1 for SAP NetWeaver 7.3

7.5 Deploying the Identity Management User Interface for HTML5

Context

To deploy the Identity Management User Interface for HTML5, do the following:

Procedure

1. Download the SCA file (the Identity Management User Interface for HTML5) to be deployed. Navigate to the download area of SAP NetWeaver Identity Management 7.2 in the SAP Software Download Center (on the SAP Support Portal), and download the SCA file.

   > i Note
   >
   > To locate the correct SCA file for the Identity Management User Interface for HTML5, choose the following path on the SAP Software Download Center: ⦊ *Support Packages and Patches* ❯ *A - Z Index* ❯ *N* ❯ *SAP NW IDENTITY MANAGEMENT* ❯ *SAP NW IDENTITY MANAGEMENT 7.2* ❯ *Comprised Software Component Versions* ❯ *NW IDM 7.2 UI FOR HTML5* ❯ *# OS independent* ❯.

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring SAP NetWeaver Identity Management User Interface for HTML5

PUBLIC   **149**

> **i Note**
>
> Make sure that the SCA file for the Identity Management User Interface for HTML5 has the same SP version as the SAP NetWeaver Identity Management (and its user interface) and the SAP NetWeaver Identity Management REST Interface Version 2. The SCA file name is `IDM_UI_HTML5<IdM SP version>_<IdM Patch version>.sca`. For example, for SAP NetWeaver Identity Management 7.2 SP8 (Patch 0), the file name is `IDM_UI_HTML508_0.sca`.

2. 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
Using the Software Update Manager (SUM)

7.6 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.

150   P U B L I C

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring SAP NetWeaver Identity Management User Interface for
HTML5

7.7 Updating the Identity Management User Interface for HTML5

Context

To perform an update of a deployed Identity Management User Interface for HTML5 component, proceed as follows:

> i Note
>
> The SCA file for the Identity Management User Interface for HTML5 must be on the same SP level as SAP NetWeaver Identity Management (and its User Interface) and SAP NetWeaver Identity Management REST Interface Version 2. Updating the Identity Management User Interface for HTML5 to a new SP version requires the updating of the other components to the same SP version first.

Procedure

1. Update the User Interface task folder and configure the solution as described in *Adding the Predefined User Interface Tasks and Configuring the Solution*. When updating the task folder, make sure that you select the *Update* option instead of *Import*.
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 User Interface Tasks and Configuring the Solution [page 144]
Deploying the Identity Management User Interface for HTML5 [page 149]

7.8 Restrictions and Considerations

Modifications of the Identity Management User Interface

Any modifications of the Identity Management User Interface for HTML5 are not supported.

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring SAP NetWeaver Identity Management User Interface for HTML5

PUBLIC **151**

- The imported tasks should not be deleted or replaced by any similar tasks in the configuration, because the task GUIDs are referred directly in the code of the user interface.
- The imported, predefined User Interface tasks should not be modified in any way (including attributes and the access control defined on the tasks).
- 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.

> ℹ 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

8 Installing and Configuring SAP NetWeaver Identity Management Virtual Directory Server

This section describes how you install and upgrade the Virtual Directory Server. It also contains information about how you configure the environment for the Virtual Directory Server.

The SAP NetWeaver Identity Management Virtual Directory Server can logically represent information from a number of disparate directories, databases, and other data repositories in a virtual directory tree. Different users and applications can, based on their access rights, get different views of the information.

Features like namespace conversion and schema adaptations provide a flexible solution that can continually grow and change to support demands from current and future applications, as well as requirements for security and privacy, without changing the underlying architecture and design of data stores like databases and directories.

8.1 Architecture Overview

The following illustration gives a high-level overview over the architecture of the Virtual Directory Server.

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring SAP NetWeaver Identity Management Virtual Directory Server

PUBLIC **153**

LDAP

SPML

Standalone
Virtual Directory Server

Deployed service

SAP NetWeaver as Java

.XML

VIRTUAL
DIRECTORY
SERVER

User interface

Configuration file
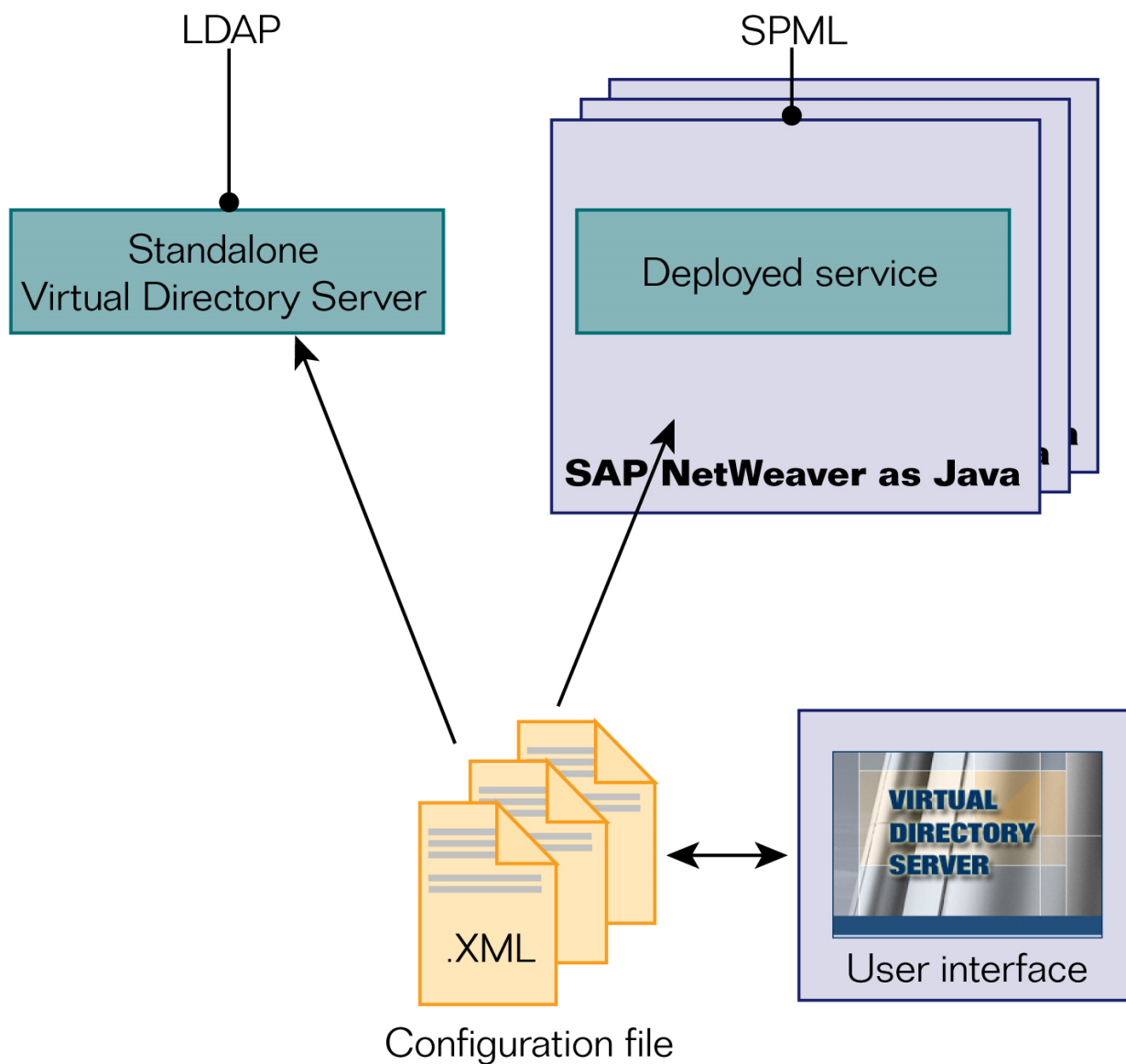
The user interface that is used to maintain the configuration is installed on one server, while the configurations are deployed on one or more servers running SAP NetWeaver AS Java.

8.2 Installation Preparation

Before you install the Virtual Directory Server make sure that the following prerequisite software is installed:

- A Java Virtual Machine (JVM).
- JDBC drivers to any database systems accessed by the Virtual Directory Server.
- A Java compiler for developing Java classes.

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring SAP NetWeaver Identity Management Virtual Directory Server

154   PUBLIC

Related Information

8.2.1 Installing the Java Virtual Machine (JVM)

A Java Virtual Machine (JVM) conforming to the Java 2 specifications, version 1.4, 1.5 or 1.6, must be correctly installed and configured. It is recommended to use the SAP JVM, but you could also use another, for instance the Sun JVM or IBM JVM.

> ℹ **Note**
>
> If using the IBM JVM, remove the file `xerces.jar` from `<ibm inst dir>\jre\lib\ext`) after installation.

The installer needs a Java VM to run. If you have only SAP JVM installed on the system, you must add the `\bin` folder in the installation directory to the PATH environment variable, for instance `c:\usr\sap\sapjvm_5\bin`.

8.2.2 Installing the JDBC Drivers

JDBC drivers for any database systems you intend to access with the Virtual Directory Server. Add these drivers to classpath as described in *Configuring the Virtual Directory Server Environment*.

8.2.3 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 or 1.6). Select *Use specified compiler* and 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. Select *Use embedded compiler* in the *Options* dialog box.

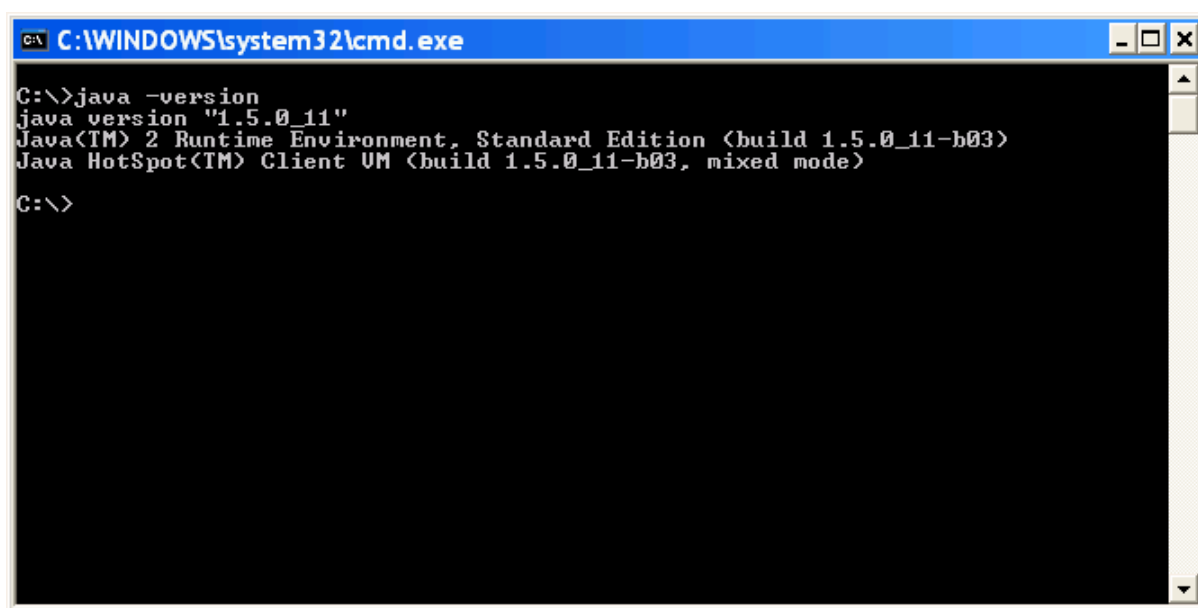## 8.2.4 Verifying the Java Virtual Machine

You can verify the version of your Java Virtual Machine.

Context

Follow the steps below:

Procedure

1. Open a console and choose ▶ *Start* ❯ *Run* ❯.
2. Enter `cmd.exe` in the *Open* field and type: `C:\>java -version`

Version number should be 1.4.x, 1.5.x or 1.6.x.

8.3   Installing the Virtual Directory Server

Context

To install the Virtual Directory Server, proceed as follows:

Procedure

1. Navigate to the download area of SAP NetWeaver Identity Management 7.2 on SAP Support Portal and download the installation kit.
2. Unpack the installation set to a separate directory.
3. Start the installation job corresponding to your platform and supply the necessary information.

   > ⓘ Note
   >
   > If changing to another path than the default installation path, make sure that the path does not contain spaces if you install on a Unix system.

   > ⓘ Note
   >
   > If your operating system is Windows 8 or Windows Server 2012, the `.exe` installation file should run in Compatibility mode for Windows 7. The installation will fail, if this condition is not met.

Related Information

8.3.1 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>`.

8.3.2 Starting the Virtual Directory Server on Microsoft Windows

How you start the Virtual Directory Server depends on the platform.

To start the Virtual Directory Server on Microsoft Windows, do the following:

1. From the *Start* menu, choose ▐ *Programs* ❯ *SAP NetWeaver Identity Management* ❯ *Virtual Directory Server* ▌.

8.3.3 Starting the Virtual Directory Server on Unix

How you start the Virtual Directory Server depends on the platform.

> ⓘ **Note**
>
> A working X-Windows setup is required.

To start the Virtual Directory Server on Unix, do the following:

1. Navigate to the installation directory of the Virtual Directory Server.
   The default is `/usr/sap/idm/Virtual Directory Server`.

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring SAP NetWeaver Identity Management Virtual Directory Server

158   PUBLIC

2. Execute `./Virtual Directory Server`.

8.4 Post-Installation

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.

8.4.1 Configuring the Virtual Directory Server Environment

The Virtual Directory Server needs some initial information in order to operate properly.

Context

To configuring the Virtual Directory Server environment, proceed as follows:

Procedure

1. In the *Options* dialog box, select the *General* tab.

   The dialog box is automatically displayed when you start the Virtual Directory Server first time. You can also open this dialog box by choosing *Tools/Options....*

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring SAP NetWeaver Identity Management Virtual Directory Server

PUBLIC   **159**
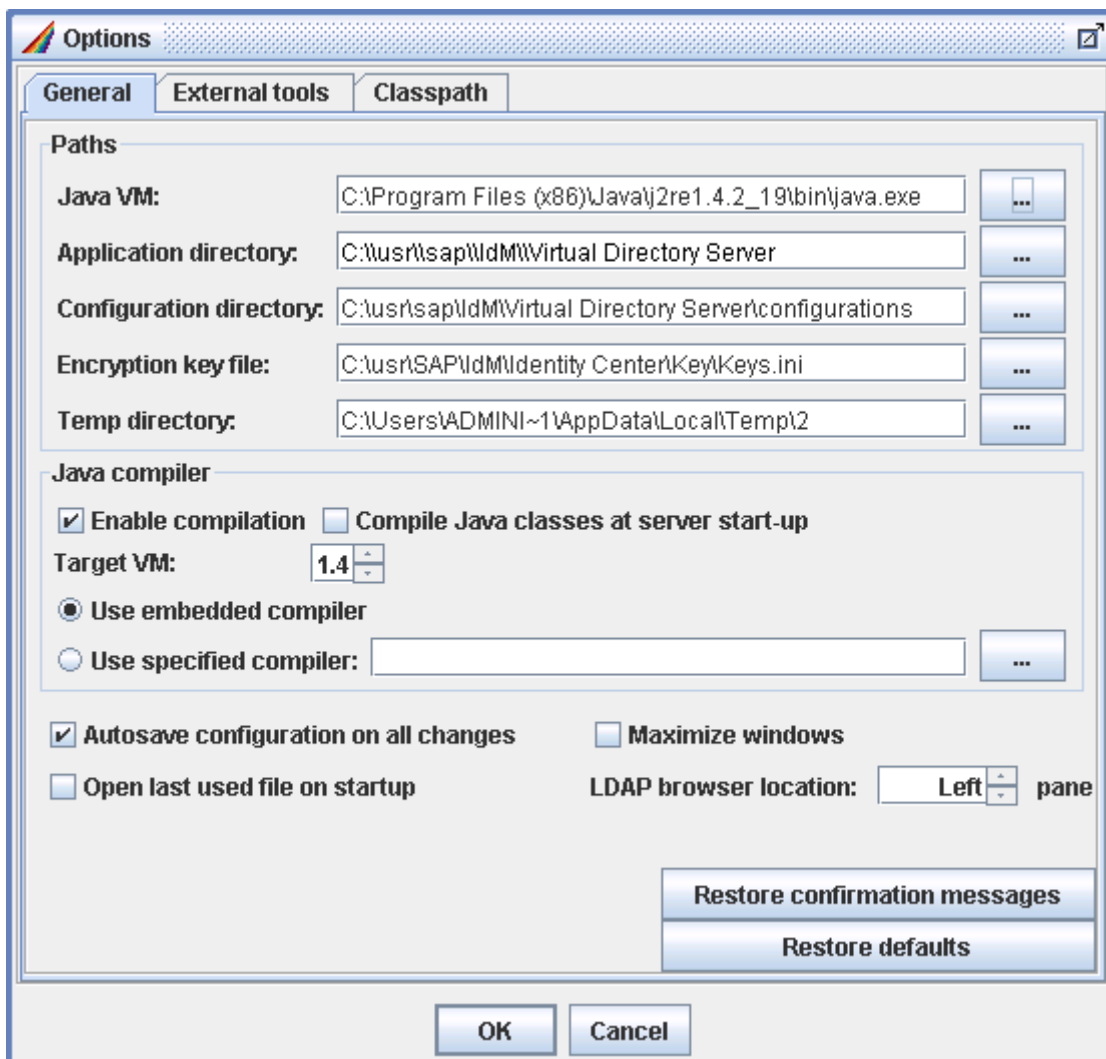
2. Configure the following properties:

Table 20:

Property	Description
Paths	Verify that the paths for to the different directories are correct.
Encryption key file	If the Identity Center is installed on the same server, select the same `keys.ini` file that is used by the Identity Center, normally located in `C:\usr\SAP\IdM\Identity Center\Key\Keys.ini`. If not, distribute the `keys.ini` file as described in *SAP NetWeaver Identity Management Security Guide*.

Property	Description
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.
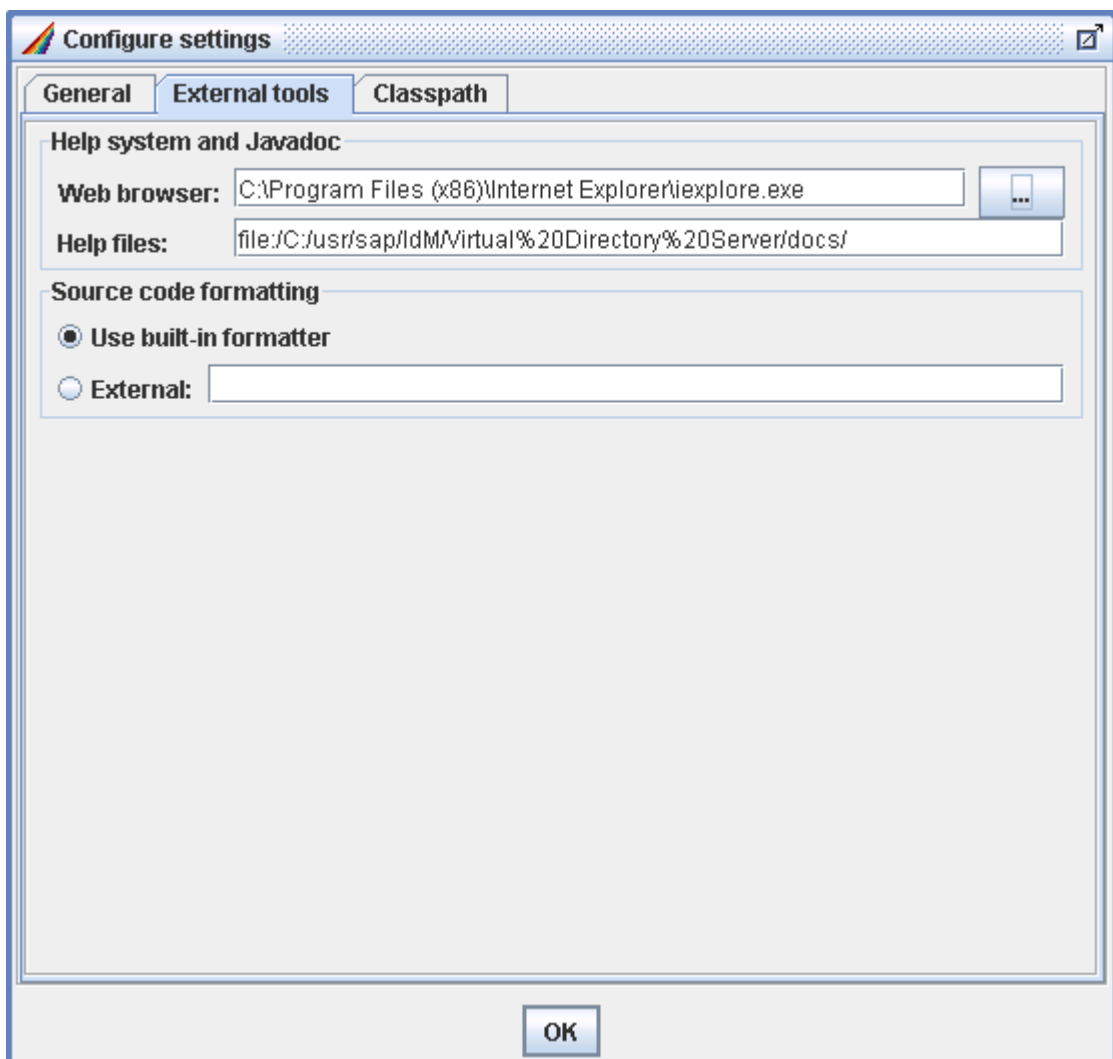
   ○ Select the browser you want to use for viewing the help file and Javadoc. The *Help files* field contains the default start page for the help file.
   ○ Select which tool you want to use for the formatting of the Java source code. You can either use the built-in formatter or an external formatter (for instance Jalopy).
4. Select the *Classpath* tab.

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring SAP NetWeaver Identity Management Virtual Directory Server

PUBLIC   **161**
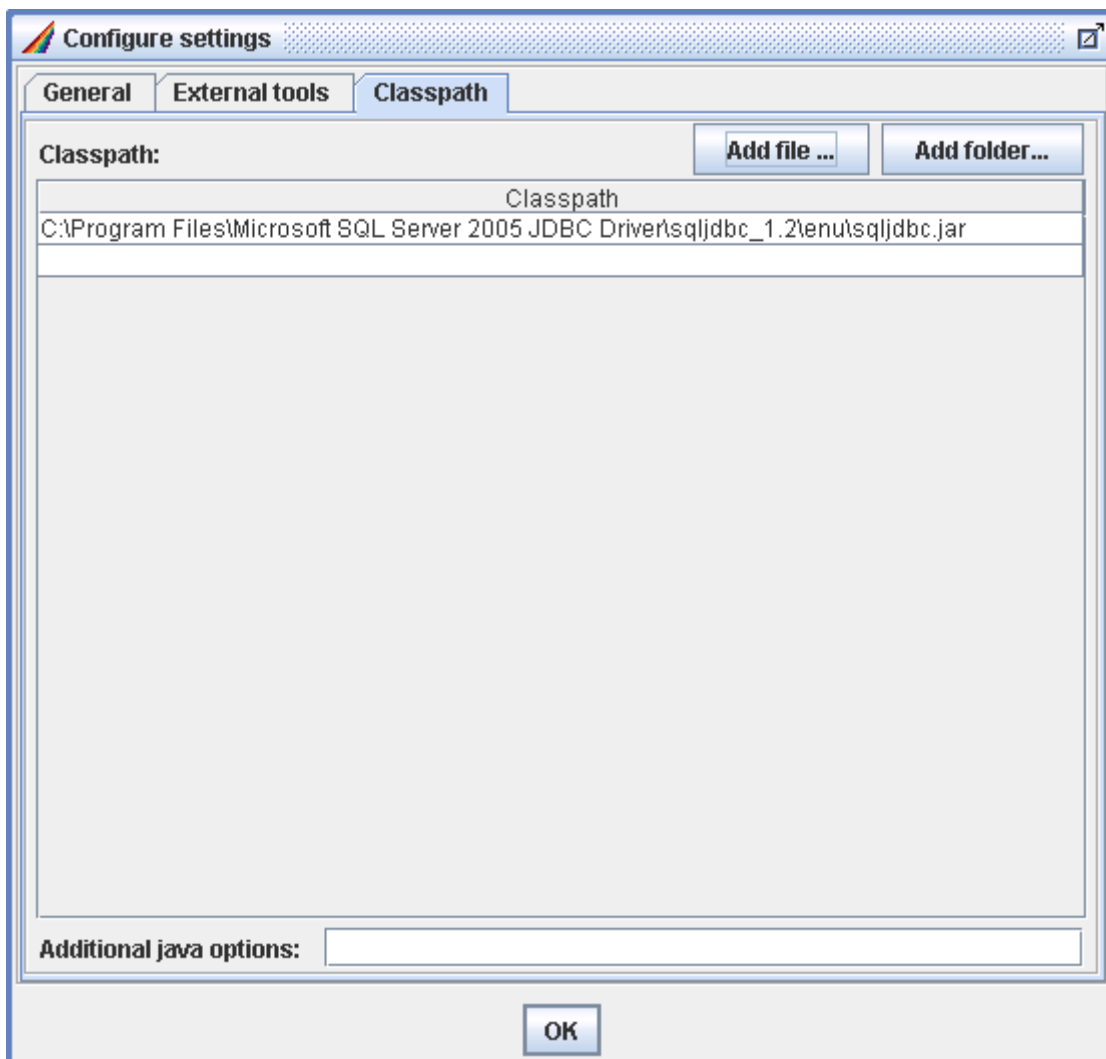
If necessary, add any files or folders to the classpath that are specific to the Virtual Directory Server, for instance if they are needed by the specified JDBC drivers.

5. Choose *OK*.

Related Information

Installing a Java Compiler [page 155]

8.4.2 Using the Paging Mechanism

You can use the paging mechanism when accessing an LDAP directory.

Context

To use the paging mechanism when accessing an LDAP directory, proceed as follows:

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

8.4.3 Using the Alternative LDAP Connector

You can use the alternative (low-memory-consumption) LDAP connector.

Context

To use the alternative LDAP connector, proceed as follows:

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`.

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring SAP NetWeaver Identity Management Virtual Directory Server

PUBLIC   **163**

Related Information

Netscape Directory SDK for Java 🔗

8.4.4 Using the SAML Outbound Connector

You can use the SAML outbound connector.

Context

To use the SAML outbound connector, proceed as follows:

Procedure

1. Download the file `opensaml.jar`.
2. Copy the file to `<inst dir>\lib`.

Related Information

OpenSAML 🔗

SAP NetWeaver Identity Management Installation Guide
**Installing and Configuring SAP NetWeaver Identity Management Virtual Directory
Server**

164   P U B L I C

8.4.5 Using Event Triggers and SendMail Event Actions

You can use event triggers and SendMail event actions.

Context

To use event triggers and SendMail event actions, proceed as follows:

Procedure

1. Download the `mail.jar` from the JavaMail API.
2. Copy the file to `<inst dir>\lib`.

8.4.6 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.

SAP NetWeaver Identity Management Installation Guide
Installing and Configuring SAP NetWeaver Identity Management Virtual Directory Server

PUBLIC   **165**

8.5   Updating the Virtual Directory Server

Context

To update the Virtual Directory Server, follow the steps below:

Procedure

1. Update the software.
   a. Stop any local services.

   > ℹ **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*.

   > ℹ **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 157]

9 Using the Provisioning Monitor Tool

The provisioning monitor helps the administrator to easily troubleshoot problems related to a specific entry in the provisioning queue.

The provisioning monitor can help you to analyze performance issues. Examples are:

- A task, a process, or a flow is not being processed
- Many entries are stuck in the provisioning queue
- The system is too slow, as the execution of tasks or processes is delayed due to a full provisioning queue

The provisioning monitor shows all the workflows related to a specified entry (person, privilege, or role for example) in the provisioning queue. This also includes completed tasks as part of an on-going provisioning process. For workflows started by tasks, you can see which form triggered the flow.

For SAP NetWeaver Identity Management 7.2 and higher versions, the provisioning monitor is available for use from the command prompt. For more information, see Downloading and Running the Provisioning Monitor Tool [page 167].

Related Information

9.1 Downloading and Running the Provisioning Monitor Tool

The provisioning monitor is available as a standalone tool, which can be downloaded separately and run from the command prompt. To save processing time, we recommend you to use the tool on the same machine where the database is located.

Prerequisites

- Java Runtime Environment: 64-bit, version 6 or higher, and have set the *JAVA_HOME* variable to point to it
- You have downloaded the provisioning monitor tool.
- You have the password for the `mxmc_oper` user.

- The following information is required for running the provisioning monitor from the command prompt:

Table 21:

Parameter	Description
JDBC_URL	The JDBC URL to the Identity Management database. The syntax is `<database URL>;user=<prefix>_oper;password=_Password` Example for the JDBC_URL for MS SQL: `jdbc:sqlserver://trd90500010.example.com;databasename=mxmc_db;user=mxmc_oper;password=_Password` For more information about the database URL, see Adding the Database as a Data Source. > i **Note** > If your password contains special characters, place your password instead of `_Password` directly in the JDBC URL, and use the escape symbols for your specific database. > For example, for Microsoft SQL Server, surround your password by curly brackets { }.
JDBC_DRIVER_PATH	The path to the JDBC driver. For more information, see Installing the JDBC Drivers.
MSKEYVALUE	The MSKEYVALUE is the technical name of the unique ID. The unique ID can be found in the Identity Management User Interface.
IDSTORE_ID	The ID of the identity store, where the entry is located
LOG_LEVEL	(Optional) The possible log levels are Trace, Debug, Info, Warn, and Error. If you do not enter this parameter, Info will be taken as the default.

Procedure

1. Download the provisioning monitor ZIP file from the SAP Identity Management Tools page.
2. Unzip the file in a new folder.
3. Open a command prompt from the new folder and use one of the following commands, depending on your operating system:

○ For Microsoft Windows:

```
ProvMonitor.bat <JDBC_URL> <JDBC_DRIVER_PATH> <MSKEYVALUE> <IDSTORE_ID>
<LOG_LEVEL>
```

  ○ For Linux/ Unix:

```
ProvMonitor.sh <JDBC_URL> <JDBC_DRIVER_PATH> <MSKEYVALUE> <IDSTORE_ID>
<LOG_LEVEL>
```

> **i Note**
>
> We recommend using one of the following shells: *Bourne Shell (sh)*, *KornShell (ksh)*, or *Bash Shell (bash)*.

4. When you press `Enter`, you will be prompted to enter the password for the `<prefix>_oper` user.

> **i Note**
>
> Instead of entering the password for `<prefix>_oper` in the prompt, you can enter it directly in plain text in the JDBC URL instead of `_Password`.
>
> If your password contains special characters, we strongly recommend you to enter your password directly in the JDBC URL.

Results

An output folder is created in the directory where the ZIP file was extracted to. This folder contains a sub-folder, named following the convention *Prov_Monitor_MSKEYVALUE_TIMESTAMP*.

To view the result after running the provisioning monitor, see Results from the Provisioning Monitor Tool [page 169].

Related Information

JSON Editor Online

9.2 Results from the Provisioning Monitor Tool

The result of the provisioning monitor is in the folder, named in accordance with the convention: *Prov_Monitor_MSKEYVALUE_TIMESTAMP*. This folder contains the following files:

- **Workflow.json** - contains all the information about the workflow of the specified entry.
- **Problems.json** - contains the results of the analysis of the workflow.

To read the JSON files, you can use any JSON editor, for example the JSON Editor Online ↗ .

The Workflow.json File

The generated *Workflow.json* file can contain the following information about each process and its child tasks:

> ℹ **Note**
>
> A process defines a set of operations executed on a given entry and stored in the identity store. Note that every process is a top-level task that is stored in the database with its TaskID.

- `Task`
  - `TaskId` – ID of the task
  - `TaskName` – Name of the task
  - `ActionType` – The type of action the task is associated to. For example: Ordered task group, Attestation task, Approval task, Switch task, Conditional task, Action task.
  - `UIType` – Type of the task. For example: Not a UI task, UI task, Assignment details task, Assignment request, View assignment request, Password reset.
  - `TaskJob` – This section will be filled if the task is of type Action Task.
    - `JobDispatchers` – The dispatcher which is configured to run this job
      - `DispatcherState` – The state of the configured dispatcher
      - `DispatcherId` – ID of the dispatcher
      - `RunProvisioningJobs` – Shows if the dispatcher is configured to evaluate action tasks
      - `DipsatcherName` – Name of the dispatcher
    - `JobState` – The state of the job
    - `JobId` – ID of the job
    - `JobName` – Name of the job
- `Approvals` – This section will be filled if the task is of type Approval Task and it has not been approved yet. Once the approver has approved or declined the approval request, this attribute will be empty.
  - `UniqueId` – The ID of the approval
  - `State` – The state of the approval. For example: Pending, Declined, Approved
  - `PvoMsKey` –The MSKEY of the pending object awaiting approval
  - `ApprovalType` – The type of approval. For example: Requesting the assignment, Requesting removal of assignment, Requesting validity change, Attestation, Non assignment approval
  - `Actors`
    - `MsKey` – MSKEY of the actor
    - `Role` – The role of the actor. For example: Assigner, Approver, Target user
- `ProvisioningEntry` – This section will be filled if there is still an entry in the provisioning queue related to this task.
  - `State` – State of the task in the provisioning queue
  - `MsKey` – The MSKEY of the entry that this task is triggered for
  - `ParentTaskId` – The ID of the parent task
  - `RepositoryId` – The ID of the repository

- ○ `ExecTime` – Date when the task is started
- ● `AuditLog` – This section will be filled with information about the audit of the task.
  - ○ `RefAudit` – The reference to the parent audit ID
  - ○ `StateText` – The state of the log
  - ○ `ExecTime` – Date when an audit was started
  - ○ `State` – Current state of the auditLog
  - ○ `MsKeyValue` – The MSKEYVALUE of the entry that this task is triggered for
  - ○ `MsKey` – The MSKEY of the entry that this task is triggered for
  - ○ `UserId` – The MSKEY of the user who triggered the task
  - ○ `AuditId` – The ID of the audit
- ● `ExtendedAuditLog` – This property will only be visible if you select the *Enable Trace* checkbox on the *General* tab of Identity Center.
  - ○ `AuditId` – The ID of the audit
  - ○ `MsKey` – The MSKEY of the entry that this task is triggered for
  - ○ `ExecTime` – Date when audit was started
- ● `Children` – Child tasks with the same details as the parent

> ℹ **Note**
>
> The predefined depth of the tree structure is 10. If you use the provisioning monitor from the command prompt, you can set the depth by changing the value of parameter `RECURSION_DEPTH_LEVEL` in the script you use.

Here is an example of the *Workflow.json* file structure (the pending process (task), related to the specified entry, is encircled):

```
[
  {
    "Task": {
      "TaskId": 390,
      "TaskName": "Modify Identity",
      "ActionType": "Ordered task group",
      "UIType": "UI task"
    },
    "Approvals": [],
    "ProvisioningEntry": {},
    "AuditLog": {
      "State": "OK",
      "UserId": "23",
      "AuditId": 275,
      "MsKey": 226,
      "MsKeyValue": "DemoUser",
      "ExecTime": "2015-08-31T11:48:07+0300"
    },
    "ExtendedAuditLog": {
      "AuditId": 275,
      "MsKey": 226,
      "ExecTime": "2015-08-31T11:48:10+0300"
    },
    "Children": [
      {
        "Task": {
          "TaskId": 420,
          "TaskName": "BasicApproval",
          "ActionType": "Ordered task group",
          "UIType": "Not a UI task"
        },
        "Approvals": [],
        "ProvisioningEntry": {},
        "AuditLog": {
          "State": "OK",
          "UserId": "#83:MODIFY;1709670708;3726",
          "AuditId": 276,
          "MsKey": 226,
          "MsKeyValue": "DemoUser",
          "ExecTime": "2015-08-31T11:48:07+0300"
        },
        "ExtendedAuditLog": {
          "AuditId": 276,
          "MsKey": 226,
          "ExecTime": "2015-08-31T11:48:10+0300"
        },
        "Children": [
          {
            "Task": {
              "TaskId": 421,
              "TaskName": "ApprovalTask",
              "ActionType": "Approval task",
              "UIType": "UI task"
```

```
▼ Task {4}
      TaskId : 390
      TaskName  Modify Identity
      ActionType : Ordered task group
      UIType : UI task
  ▶ Approvals [0]
  ▶ ProvisioningEntry {0}
  ▶ AuditLog {6}
  ▶ ExtendedAuditLog {3}
  ▼ Children [3]
      ▶ 0  {6}
      ▶ 1  {6}
      ▼ 2  {6}
          ▶ Task {4}
          ▶ Approvals [0]
          ▶ ProvisioningEntry {5}
          ▶ AuditLog {6}
          ▶ ExtendedAuditLog {3}
          ▼ Children [1]
              ▼ 0  {6}
                  ▼ Task {4}
                      TaskId : 423
                      TaskName  Approval Task
                      ActionType : Approval task
                      UIType : UI task
                  ▼ Approvals [1]
                      ▼ 0  {5}
                          UniqueId : 36
                          State : Pending
                          PvoMsKey : 228
                          ApprovalType : Requesting the assignment
                      ▶ Actors [3]
```

The Problems.json File

The *Problems.json* file can contain additional information about the problem and propose a solution to it if the analysis of the provisioning monitor has detected one or more of these root causes:

SAP NetWeaver Identity Management Installation Guide
Using the Provisioning Monitor Tool

Table 22:

ID of the Problem	Problem Description
1	Tasks are stuck in state *Queued* but there is no task which they are waiting for to finish
2	Tasks are stuck in state *Ready to run* with no execution time
3	An object references itself and can't be completed
4	Tasks are stuck in state *Wait for event tasks* or *Wait for event task status*
5	Approval tasks without assigned approvers are stuck in the provisioning queue
6	There are issues with the dispatcher configuration of the system

If one or more of these root causes is detected, the *Problems.json* file will contain a description of the problem and will propose a solution. If none of these root causes was detected, the *Problems.json* file will be empty.

The generated *Problems.json* file can contain the following information:

- `ProblemID` – The unique ID of the problem
- `ProblemDescription` – Description of the problem
- `RelatedObjects` – Objects related to the problem
  - `ObjectID` – The ID of the object in the SAP Identity Management database
  - `ObjectType` – The type of the object. For example, Process/ Form/ Task, Job, Dispatcher, Package
  - `ObjectDisplayName` – The display name of the object
- `ProposedActions` – Proposed actions to be performed by the user
  - `ActionId` – Consecutive number of the proposed action
  - `Action` – Description of the action to be performed

Here is an example of the *Problems.json* file structure:

```
▼ 2  {4}
      ProblemID : 5
      ProblemDescription : Approval tasks without assigned approvers are stuck in the provisioning queue.
   ▼ RelatedObjects [1]
      ▼ 0  {3}
            ObjectID : 1002243
            ObjectType : Process/Form/Task
            ObjectDisplayName : Basic approval
   ▼ ProposedActions [1]
      ▼ 0  {2}
            ActionID : 1
            Action : The task with ID 1002243 is of type basic approval. Please check if approvers are assigned
                     to the task. If yes, ask your approvers to check their ToDo tabs in the Identity Management
                     User Interface. If no approver is assigned, contact SAP Support.
```

Important Disclaimers and Legal Information

Coding Samples

Any software coding and/or code lines / strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended to better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, unless damages were caused by SAP intentionally or by SAP's gross negligence.

Accessibility

The information contained in the SAP documentation represents SAP's current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAP in particular disclaims any liability in relation to this document. This disclaimer, however, does not apply in cases of willful misconduct or gross negligence of SAP. Furthermore, this document does not result in any direct or indirect contractual obligations of SAP.

Gender-Neutral Language

As far as possible, SAP documentation is gender neutral. Depending on the context, the reader is addressed directly with "you", or a gender-neutral noun (such as "sales person" or "working days") is used. If when referring to members of both sexes, however, the third-person singular cannot be avoided or a gender-neutral noun does not exist, SAP reserves the right to use the masculine form of the noun and pronoun. This is to ensure that the documentation remains comprehensible.

Internet Hyperlinks

The SAP documentation may contain hyperlinks to the Internet. These hyperlinks are intended to serve as a hint about where to find related information. SAP does not warrant the availability and correctness of this related information or the ability of this information to serve a particular purpose. SAP shall not be liable for any damages caused by the use of related information unless damages have been caused by SAP's gross negligence or willful misconduct. All links are categorized for transparency (see: http://help.sap.com/disclaimer).

**go.sap.com/registration/
contact.html**