SAP NetWeaver® Identity Management
Identity Services

Configuration Guide

Version 7.2 Rev 7
Preface

The product

The SAP NetWeaver Identity Management Identity Services provides web services access to identity information stored in an identity store in the Identity Center or some other application that can be accessed from the Virtual Directory Server. The Identity Services accepts SPML (Service Provisioning Markup Language) requests.

It acts as an abstraction layer between identity services clients and the identity information. This reduces the complexity of access as much of the connection details (location, protocols, repository types and so on) are hidden from the clients.

The reader

This manual is intended for people who are to implement an Identity Services solution.

Prerequisites

To get the most benefit from this manual, you should have the following knowledge:

- Knowledge of the Identity Center.
- Knowledge of the Virtual Directory Server.
- Knowledge of deploying web services on SAP NetWeaver.

The following software is required:

- SAP NetWeaver Identity Management Virtual Directory Server 7.2 SP9 or newer, correctly installed and licensed.
- SAP NetWeaver Identity Management Identity Center 7.2 SP9 or newer, correctly installed and licensed.
- One of the following SAP NetWeaver versions:
  - SAP NetWeaver AS Java as of Release 7.0 SP14 or higher (SAP NetWeaver 7.0).
  - SAP NetWeaver Composition Environment 7.1 Including Enhancement Package 1 (SAP NetWeaver CE 7.1 EHP 1).
  - SAP NetWeaver Composition Environment 7.2 (SAP NetWeaver CE 7.2).
  - SAP NetWeaver 7.3.
  - SAP NetWeaver 7.3 Including Enhancement Package 1 (SAP NetWeaver 7.3 EHP 1).
  - SAP NetWeaver 7.4.

The manual

This document describes how you create and configure an Identity Services solution.
Related documents

You can find useful information in the following documents:

- The tutorials for the Identity Center
- The tutorials for the Virtual Directory Server
- For documentation about the Software Deployment Manager (SDM), see [http://help.sap.com/saphelp_nw70/helpdata/EN/22/a7663bb3808c1fe10000000a114084/frameset.htm](http://help.sap.com/saphelp_nw70/helpdata/EN/22/a7663bb3808c1fe10000000a114084/frameset.htm).
- For Software Update Manager (SUM), see:
  - You can find its documentation on SAP Service Marketplace at [http://service.sap.com/sltoolset](http://service.sap.com/sltoolset) → Software Logistics Toolset 1.0 → Software Update Manager (SUM), under "Documentation" on the bottom of the page.
- SAP NetWeaver Identity Management Compliant provisioning using SAP Access Control – Architectural overview.
- SAP NetWeaver Identity Management Compliant provisioning using SAP Access Control - Configuration guide.
- For more documentation for SAP NetWeaver, see Help Portal ([http://help.sap.com](http://help.sap.com)).
# Table of contents

**Introduction** .................................................................................................................................. 1

**Adding the configuration in the Virtual Directory Server** .......................................................... 2

**Testing the configuration with LDAP clients** ............................................................................... 6
  - Starting the server ................................................................................................................................. 6
  - Configuring the internal LDAP browser and testing the configuration .............................................. 7
  - Performing the searches ........................................................................................................................ 8
  - Testing the configuration with LDP .................................................................................................... 11

**Deploying the configuration on SAP NetWeaver** ....................................................................... 14
  - Including the JDBC drivers and additional JAR files ........................................................................... 14
  - Configuring the deployment ................................................................................................................ 15
  - Deploying the configuration ................................................................................................................ 16
  - Updating the deployed configuration ................................................................................................... 19

**Post-deployment** .......................................................................................................................... 20
  - Define Keys.ini file for application ..................................................................................................... 20

**Testing the configuration using SPML** ....................................................................................... 21
Introduction

This document describes the necessary steps needed to add the Identity Services configuration to the Virtual Directory, adapt this configuration and add a framework in the Identity Center that can be used to enable a provisioning solution implemented in the Identity Center for Identity Services. For overview information and available operations, see the document SAP NetWeaver Identity Management Identity Services: Architectural overview.

Both the configuration in the Virtual Directory Server and the framework in the Identity Center are based on templates. When implementing a solution, it may be necessary to extend/modify the configuration created based on the template.

In order to successfully implement an Identity Services solution, two components of the Identity Management are involved:

- Virtual Directory Server
  - Accepts the identity service client's requests.
  - Pre-process them before handing them over to configured back-ends.
  - Accepts and post-process results before returning them to the client.

- Identity Center
  - Performs the provisioning operations from the client's requests in the applications connected to the provisioning solution.

The configuration process described in this document consists of:

- Adding the configuration in the Virtual Directory Server.
- Testing the configuration using LDAP clients.
- Deploying the configuration on SAP NetWeaver.
- Performing the post-deployment operations.
- Testing the configuration using SPML.
- Adding the provisioning framework to the Identity Center.
Adding the configuration in the Virtual Directory Server

The first step is to add the configuration to the Virtual Directory Server. Here you specify how you connect to the Identity Center database you will use for the provisioning system.

There are two possibilities:

- You can connect the Virtual Directory Server configuration to an Identity Center database with an existing provisioning system that you want to enable for Identity Services. You must add the Identity Services provisioning framework to be able to access the provisioning system via Identity Services.

- You can connect to an empty Identity Center database where you will later install the Identity Services provisioning framework and build a provisioning solution that you connect to the Identity Services provisioning framework.

Do the following:

1. In the Virtual Directory Server console, choose File/New….

![Image of the Virtual Directory Server console](image.png)

Select "SAP NetWeaver 7.2" in the "Group" list and "Identity Service 72.xml" in the "Template" list.

2. Choose "OK".
The template dialog box is displayed:

![Template Dialog Box](image)

Fill in the fields with the following information:

**Port**
Enter the port number that will be used when deploying the configuration as an LDAP server. Make sure that this port is not in use by another application on your system. It is recommended to test and verify the configuration (especially if additional tailoring of the template is done) using an LDAP client, before deploying configuration on NetWeaver.

**Identity Center URL**
Start the JDBC URL wizard by choosing "..." to the right of the field. Enter the connection parameters to the Identity Center database you want to connect to. Use the `<prefix>_rt` user to access the database.

**Identity Store ID**
Enter the ID of the identity store that will be exposed through Identity Services. The template supports only one identity store, but this can be extended in the configuration.

**Path to Keys.ini**
Enter the path to the `Keys.ini` file, located in `<Identity Center install directory>\Key` by default.

**GRC Repository**
Enter the correct ID of the GRC repository definition. Observe the ID in the "General" tab of the repository definition's details pane in the Identity Center Management Console (field "ID/Name").

**Role Assignment**
Enter the correct task ID of the role assignment task (**AC Callback Service**). Observe the ID in the "Options" tab of the task's details pane in the Identity Center Management Console (field "Task ID/Name").
Role Definition
The parameter holds the task ID of the role definition task. For future use, i.e. leave the default value (no need to change).

Authenticated user (Login/Password)
The template is designed so that users with anonymous login have access to all search functionality of the configuration, while only a single authenticated user is able to execute update operations. Enter a user name and password for the user that should be allowed full access (superuser/superuser by default).

See the help file for the Virtual Directory Server for more information about user groups and users and how you can extend the template and to change the access privileges.

3. Choose "OK".

The "Save" dialog box is displayed:

![Save dialog box]

Enter the name of the new configuration (for instance, IdServ72.xml).

4. Choose "Save".
The resulting configuration is displayed in the Virtual Directory Server:
Before you proceed with deploying the configuration on SAP NetWeaver, it is recommended to test its basic operations and connectivity using an LDAP client. For that purpose you can use any LDAP client (for instance LDP, Softera, JExplore).

### Starting the server

Start the server as an LDAP deployment in the following way:

1. Choose the "Operation" button to display the operation log.
2. Choose the "Start" button to start the server.

**Note:**

Depending on your settings, you may have to compile the extension class "attrClass" explicitly before starting the server, e.g. choose Server/Compile and start from the main menu.

If the run-time environment is correct, the server will start listening on configured port. Verify that the log shows no error messages.

If the log contains error messages, some typical error messages may be:

- The JDBC driver for the Identity Center database system (Microsoft SQL Server or Oracle) is not in the classpath for the Virtual Directory Server. If necessary, see the help file for details about how you add a JDBC driver to classpath.

- The selected port number is occupied. The port number can be changed by viewing the properties of the "main_listener" LDAP deployment.

- The extension class (attrClass) is not compiled.
Configuring the internal LDAP browser and testing the configuration

First, we use the built-in LDAP client to test the configuration.

1. Choose **Tools/Browse LDAP**… to open built-in LDAP browser.

2. To test the configuration (and to perform a basic search operation), choose the "Wizard…” button to open the "LDAP URL” dialog box:

   - Enter the host name and port number you specified for the server.
   - Enter `operation=info` as starting point.
   - Leave the "Return attributes” field empty (meaning – you will request all attributes).
   - Search type: Not applicable
   - Filter: Not applicable

3. Choose "OK".
4. Choose "Search". If the configuration is correct, the following search result is displayed in the LDAP browser:

![LDAP browser screenshot]

**Performing the searches**

You can now perform a set of search operations toward this server. There are several operations you can perform by entering different URLs.

For all operations you can leave "Return attributes" field empty (meaning – you will request all attributes).

**Performing a basic operation**

Specify the following URL:

![LDAP URL screenshot]

Starting point: operation=info
Search type: Not applicable
Filter: Not applicable
The result should be as follows:

**Listing available systems**

Specify the following URL:

Starting point: operation=listsystems

Search type: Not applicable

Filter: (objectclass=*)
Testing the configuration with LDAP clients

The result should be as follows:
Testing the configuration with LDP

The Microsoft LDAP utility (LDP) is quite simple and easy to use. You can use it both for browsing as well as updating of the entries in the LDAP server.

1. Start LDP.
2. Choose **Connection/Connect**.

![Connection/Connect](image)

Enter host name and port number you specified for the server.

3. Choose "OK".

The following is displayed:

![Connection/Bind](image)

4. Choose **Connection/Bind**.

Enter the user name and password for the user you specified when you created the configuration (*superuser*/superuser by default).

Although we could have connected anonymously, we now use the credentials of the user with full access rights.

5. Choose "OK".

---

© Copyright 2014 SAP AG. All rights reserved.
Performing a basic operation

To perform a basic operation from LDP:

1. Choose Browse/Search.

   ![Search dialog box]

   Enter operation=info as "Base Dn".

2. Choose "Options".

   ![Search options dialog box]

   Remove any value in the "Attributes" field. Empty value here means that LDP always requests all attributes in all subsequent searches.

3. Choose "OK" to return to the "Search" dialog box.

4. Choose "Run".

   The result of this operation is exactly the same as the result obtained after successful connection.

Note:
Because of a known issue with LDP, this command may fail. If so, just repeat the procedure.
Listing available systems

To list available systems:

1. Choose **Browse/Search**.

   Fill in `operation=listsystems` in the "Base Dn" field.

2. Choose "Run".

   The expected result is shown below:
Deploying the configuration on SAP NetWeaver

This section describes how you deploy the configuration on the following SAP NetWeaver versions:

- SAP NetWeaver AS Java as of Release 7.0.
- SAP NetWeaver CE 7.1 EHP 1.
- SAP NetWeaver CE 7.2.
- SAP NetWeaver 7.3.
- SAP NetWeaver 7.3 EHP 1.
- SAP NetWeaver 7.4.

Note:
Make sure that all extension classes are compiled before deploying.

The following steps are necessary to deploy a configuration:

- Include the necessary JDBC drivers and additional JAR file(s) (in the Virtual Directory Server)
- Configure the deployment (in the Virtual Directory Server)
- Deploy the configuration

Note:
It is a good practice and recommended to always run and test the Virtual Directory Server configuration locally before deploying it.

Including the JDBC drivers and additional JAR files

When the Virtual Directory Server configuration is deployed on an SAP NetWeaver application server, we have to ensure that the classpath of the deployed configuration contains all necessary JDBC drivers (and any additional JAR file(s)). It is not sufficient that the local configuration has a proper classpath.

The necessary JDBC drivers and the additional JAR file(s) must be added to the EAR file that is created by the Virtual Directory Server, which will ensure that these files will be a part of its classpath when the configuration is deployed (even remotely). The following JAR file needs to be defined in addition to the necessary JDBC drivers:

- idmcommon.jar

The above mentioned JAR file is available in the directory \&lt;Identity Center install directory\>\Java, by default C:\usr\SAP\IdM\Identity Center\Java.

To add the necessary drivers and other JAR file(s), do the following:

1. Create a folder "lib" in the configuration's workspace (here C:\usr\sap\IdM\Virtual Directory Server\configurations\IdServ72).
2. Copy the JAR file(s) from the specified directory (-ies) to the created lib folder in the configuration's workspace.
Deploying the configuration on SAP NetWeaver

SAP NetWeaver Identity Management Identity Services Configuration Guide

© Copyright 2014 SAP AG. All rights reserved.

Note:
After successfully testing the Virtual Directory Server configuration locally before the deployment (as it is recommended), the classpath would typically contain the files as reflected in the image below (JDBC driver files, as well as the previously mentioned JAR file). Make sure that all these files are copied to the lib folder in the configuration's workspace before the EAR file is created.

Configuring the deployment

To configure the deployment:

1. View the properties of the "Identity Service" web service deployment (select Deployments\Web service deployments\Identity Service in the console tree and choose "Properties..." from the context menu).
Deploying the configuration on SAP NetWeaver

SAP NetWeaver Identity Management Identity Services Configuration Guide

© Copyright 2014 SAP AG. All rights reserved.

Server
Make sure that "NetWeaver" is selected.

2. Choose "Deploy". If you already specified a file name for the EAR file, this file name will be used. If not, you are prompted to specify this file name.

The EAR file is created and is ready to be deployed using standard SAP deployment tools.

An information dialog box appears:

Choose "OK" to close the dialog box.

Deploying the configuration

If the Virtual Directory Server is not installed on the same server as your SAP NetWeaver, copy the EAR file so it is accessible from the SAP NetWeaver server.

The deployment process is different, depending on the version of your SAP NetWeaver.

SAP NetWeaver AS Java as of Release 7.0

To deploy the configuration (the EAR file) on SAP NetWeaver AS Java as of Release 7.0, use the Software Deployment Manager (SDM):

1. Start the Software Deployment Manager (SDM).

2. Connect to the SDM server – choose or SDM Gui/Login to open a connection dialog box and enter the SDM server password, hostname and port before choosing "Login".

Note:
The following convention applies for the port: 5<J2EEinstance_number>18. For example, if your J2EE instance number is 15, the port is 51518. The SDM Server accepts only one user at a time. If somebody has already connected to it, you will receive an error message.
3. Choose "Login".

4. Select the "Deployment" tab and choose "Add" button.

Browse to locate the EAR file you want to deploy.
5. Choose "Next" twice.

6. Choose "Start Deployment".

7. When installed, choose "Confirm" and close the SDM application (choose to exit).

The configuration is now deployed on your SAP NetWeaver. Proceed to performing the post-deployment operations described in section Post-deployment on page 20.
Other SAP NetWeaver versions

To deploy the configuration (the EAR file) on other supported versions of SAP NetWeaver (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), do the following:

1. Convert the new EAR file to SDA/SCA file. See SAP Note 1223957 for conversion description and access to the nwpacktool.zip attachment file (NetWeaver Packaging Tool), which can be used to create an SCA file from an EAR file.

2. Use the Software Update Manager (SUM) to deploy the generated SCA file on SAP NetWeaver:
   - You can find its documentation on SAP Service Marketplace at [http://service.sap.com/sltoolset](http://service.sap.com/sltoolset) → Software Logistics Toolset 1.0 → Software Update Manager (SUM), under "Documentation" on the bottom of the page.

You may also see the document *SAP NetWeaver Identity Management Identity Center Installing and configuring the Identity Management User Interface* for more details about deployment with Software Update Manager (section *Deploying the Identity Management User Interface*).

When the configuration is deployed on your SAP NetWeaver, proceed to performing the post-deployment operations described in section *Post-deployment* on page 20.

Updating the deployed configuration

If the Virtual Directory Server is not installed on the same server as your SAP NetWeaver, copy the EAR file so it is accessible from the SAP NetWeaver server.

The process of updating a deployed configuration is different, depending on the version of your SAP NetWeaver.

SAP NetWeaver AS Java as of Release 7.0

Deploy the configuration as described for this SAP NetWeaver version in section *Deploying the configuration* on page 16.

Other SAP NetWeaver versions

For SAP NetWeaver versions CE 7.1 EHP 1, CE 7.2, 7.3, 7.3 EHP 1 and 7.4, deploy the configuration as described for these SAP NetWeaver versions in section *Deploying the configuration* on page 16.
Post-deployment

After the configuration is deployed on your AS Java, the following post-deployment operations should be performed:

- Define the correct path to Keys.ini file for your deployed application.

Define Keys.ini file for application

If handling encrypted data, as it usually is the case, it is important to define the correct Keys.ini file for your deployed application on the AS Java. Make sure that the correct and full path to the Keys.ini file is defined in the Propertiesheet application.global.properties of application vds-<application_name> (here vds-ids72). Restart your application to apply the changes.
Testing the configuration using SPML

The Virtual Directory Server installation includes a simple SPML client that can be used to perform this test, but any SPML client can be used.

1. Choose All Programs/SAP NetWeaver Identity Management/Virtual Directory Server/Test Web Services Client to start the web service client. Select the “Connection” tab:

![Generic WS Client Interface](image)

Enter the URL on the format

http://<IP of the NetWeaver server>:<Port>/<application name>/router

For instance:

http://10.55.160.92:53000/ids72/router

The server name and port number depends on the configuration of the SAP NetWeaver server where you have deployed the configuration.

The application name used in the template for Identity Service was "ids72", but this can be configured to something else. This makes it possible to deploy multiple Identity Services, each with its own configuration and different application name. Add the application name defined when configuring the deployment (see page 15).

Select "Basic" authentication with the correct credentials (superuser/superuser by default) for full access rights. Or select "Anonymous" authentication for read-only access rights.
2. Select the "SPML Request" tab:

Enter the "Request ID" (optional).
Enter `operation=info` as "Starting point".
Select "No filter".
3. Choose "Send SPML request". The expected result is shown below (select the "Result" tab if necessary):

```
---
DN:operation=info
default:defaultkey=[ca]
default:namingcontext=[ou= newbie,o=ids]
default:system-id=[101]
namingcontext=[ou=nwldm,o=ids]
operationset=[operation=info, operation=schema, operation=list, operation=request@clds, operation=listSystems, operation=listApplications, operation=listPrivileges, operation=listUsers, operation=listRoles, operation=roleassignmentresult, operation=roleDefinitionresult, operation=auditlog]
supportedspmlversion=[SPML01]
top:topfix=[o=ids]
supported syste types=[SAPNWIdm]]
---
```
4. Select the "SPML Request" tab:

Enter `operation=listsystems` as "Starting point".

5. Choose "Send SPML request".
The expected result is shown below:

![Screenshot of a Generic WS Client interface with a request for a list of systems and the corresponding response showing a DN with attributes such as 'systemId', 'systemType', and 'objectClass'.]

Note:
The parentheses are not part of the values.