Configuration Guide **PUBLIC**

Document Version: 13 – 2018-02-22

SAP Identity Management for SAP System Landscapes: Configuration Guide

Content

1 SAP NetWeaver Identity Management for SAP System Landscapes: Configuration Guide

History of Changes

Version	Change
7.2 Rev 11	Minor changes.
7.2 Rev 10.1	Added note on permissions for the service user used for connections to LDAP directories.
7.2 Rev 9	Added *Setting up an SAP Java Connector (SAP Co) and Related Traces* and *Restricting the CPIC or JRFC Trace to a Specific Pass*.
7.2 Rev 8	Added DB2 connection parameters for VDS connection. Added *Provisioning Productive Instead of Initial Passwords* and *Single Sign-On for AS ABAP Systems* sections
7.2 Rev 7	Added description for setting-up an update job. Updated constants appendix including password provisioning. Updated attributes appendix. Minor updates.
7.2 Rev 6	Added prerequisite for HCM data export to LDAP. Added Oracle connection parameters for VDS connection.
7.2 Rev 5	Added SSL repository constant for ADS. Added notifications set-up for role assignments.
7.2 Rev 4	Added information on the Business Suite connector. Several smaller updates.

Version	Change
7.2 Rev 3	Added information on group handling. Added information on SAP HANA™ database. Added information on provisioning of company addresses. Updated copyright. Added *SAP Note 1618734*.
7.2 Rev 2	Updated *Appendix A: Repository Constants*
7.2 Rev 1	Added *Limitations and Considerations When Connecting an AS Java to an LDAP Directory* section. Added *General Remarks on Repository Constants* section. Added a remark on lower amount of configuration steps. Added a reference to the LDAP wizard (transaction HRIDMWIZARD_START) in the SAP HCM system for configuring the SAP HCM system and exporting the data.
7.2	Original version.

Related Information

SAP Note 1618734 - Upgrading SAP Provisioning Framework
Limitations and Considerations When Connecting an AS Java to an LDAP Directory [page 14]
General Remarks on Repository Constants [page 121]
Password Provisioning [page 98]
Single Sign-On for AS ABAP Systems [page 99]
Setting up an SAP Java Connector (SAP JCo) and Related Traces [page 116]
Restricting the CPIC or JRFC Trace to a Specific Pass [page 119]

2 Introduction

> **Note**
>
> Check that you have the latest version of this document available at help.sap.com/nwidm72.

You can use SAP Identity Management for processing identity information in a variety of ways, depending on your system landscape. You can use it in homogeneous or heterogeneous landscapes, either with or without SAP systems.

In *SAP Identity Management Provisioning Framework for SAP Systems: Architectural Overview*, we described a number of use cases where you can use SAP SAP NetWeaver Identity Management for identity provisioning with SAP systems. These use cases are:

- SAP Human Capital Management (HCM) Integration
  This use case shows how to manage identities when the leading identity source is an SAP HCM system and the identities are provisioned to an LDAP directory server by the Identity Center.
- SAP Enterprise Portal Environment
  This use case shows how to manage identities in an SAP NetWeaver Portal environment. In this case, the leading identity source is a corporate directory, and the identities are provisioned to the portal's AS Java and the various back-end systems. In this example, we show how to provision to an AS ABAP back-end system.
- Identity Lifecycle Management
  This use case shows how to integrate the first two cases, whereby the identities from the SAP HCM use case that have been provisioned to the LDAP directory server are also used for the portal environment and the corresponding back-end system(s).
- Enhanced SAP Business Suite Integration
  Another example of a complete system landscape includes the SAP Business Suite integration. In this case, additional SAP systems, which may also have special requirements, are connected to SAP NetWeaver Identity Management for identity provisioning. The SAP HCM system is typically the leading system for this use case.
- Central User Administration (CUA) Integration
  In this case, you connect the CUA central system to the Identity Center as a target system. The Identity Center provisions the identity data to the CUA central system, which in turn provisions the data to its child systems.

To implement these use cases, we provide the SAP provisioning framework. This framework provides templates for connecting SAP systems to SAP Identity Management and for setting up the corresponding provisioning jobs.

Related Information

SAP Identity Management Provisioning Framework for SAP Systems: Architectural Overview

2.1 Prerequisites

- Role Model
  As mentioned in the Architectural Overview document, a primary prerequisite for the implementation of identity management is a role model. The role model provides a mapping between the user's business role (for example, `EMPLOYEE`) to the technical roles or privileges in the back-end system (for example, the ABAP role `Z_HCM_EMPLOYEE_ROLE`). Before proceeding, you must set up this role model for all of the systems involved in the system landscape that you want to manage using the SAP provisioning framework.
- You are familiar with the SAP Identity Management components. These comprise of the Identity Center and the Virtual Directory Server (VDS).
- You have installed the Identity Center, and have deployed the Web Dynpro user interfaces for workflow and administration.
- For the SAP HCM or the SAP Business Suite use cases, you have also installed the VDS component.
- When working with the SAP provisioning framework, the systems must meet the following system requirements:
  - SAP Identity Management: Release 7.2
    If you are using the provisioning framework for SAP systems that was provided with SAP SAP NetWeaver Identity Management Release 7.1, see also the documentation provided with that release. This document is for the SAP provisioning framework for Release 7.2.
  - AS ABAP: Release 4.6C or higher
  - AS Java/Portal: Release 6.40, 7.0, 7.1 SPS 5, 7.2, or 7.3.
    In addition, for Releases <= 7.0, SPML patches must be deployed on the AS Java as described in *SAP Note 1064236*.
  - SAP ERP HCM: Release 6.0 SP 32
    This support package stack is required for provisioning only delta information from the SAP HCM system to SAP Identity Management.
  - SAP Business Suite 7.0
    This release is required for the enhanced SAP Business Suite integration use case.
- You have credentials to use for the connections to the target systems. The corresponding authorizations allow for creating and updating entries.

Related Information

Identity Management for SAP System Landscapes: Architectural Overview
Note 1064236 - SAP Identity Management for UME using SPML

2.2 Limitations and Considerations

2.2.1 Limitations and Considerations that Apply to Specific Use Cases

2.2.1.1 Limitations and Considerations When Using the SAP HCM Use Case

The following limitations apply when using the SAP HCM use case:

- The delta mechanism is not preconfigured when importing the data from the SAP HCM system into the staging area in the Identity Center. A full load is always performed.
- When using the SAP HCM use case, the following options are delivered with the SAP provisioning framework for determining the user account name:
  - The SAP HCM system can determine the user account name using the *P0105-SYHR_A_P0105_AF_SYSUNAME* field. If this field does not contain any data, but other employee data is maintained, then the employee data is first only written to the staging area. Only after this field is filled in the SAP HCM system is the complete data written to the productive identity store. Data consistency is ensured (for example, if you delete the user name from this field) by making sure that a unique personnel number is also specified in the *P0000-PERNR* field.
  - The Identity Center can determine the user account name. In this case, it uses the SAP HCM *P0000-PERNR* field as input to determine a unique system-wide user ID. The *P0105-SYHR_A_P0105_AF_SYSUNAME* field is ignored.

  If you have other needs for determining the system-wide user account name, then you must adjust the tasks and jobs accordingly.
- For changes to attributes that should occur in the future, a pending object is created and then processed at the time of the change. By default, multiple changes to the same attribute produce multiple pending change request, with an exception for the MX_FS_EMPLOYMENT_STATUS_ID. For this attribute, an existing pending value is overwritten. If you want to change the behavior for this or other attributes, you must change the script that is used in the SAP HCM staging area identity store framework. For more information, see *SAP Note 1524813*.
- If you have difficulties transferring Unicode characters from the SAP HCM system, then start the system's LDAP connector using the code page that corresponds to the SAP HCM system. For more information, see *SAP Note 539198*.

Related Information

Note 1524813 - HCM Staging Area - Script 'sap_importTimeValuesOverWrite'

Note 539198 - LDAP Connector (Version 2.6)

2.2.1.2 Considerations When Using the SAP Enterprise Portal

SAP Identity Management does not support remote roles used by a Federated Portal Network (FPN) to share content. If you are integrating a FPN with SAP Identity Management, use the Remote Delta Link mode to share content instead. For more information, see the Related Links section.

Related Information

'Remote Delta Link' Mode
FPN Part III - Sharing Content between SAP NetWeaver Portals

2.2.1.3 Considerations When Using the Identity Lifecycle Management Use Case

When using this use case you must ensure that users exist and are assigned to the appropriate groups on the LDAP directory server before running jobs or initiating provisioning steps that will assign portal roles to the users. Otherwise, if a user exists in SAP HCM and is assigned to a portal role, and the portal role assignment is provisioned without the user existing in the LDAP directory server that is used as a user store for the portal, then you will receive errors.

2.2.1.4 Considerations When Using the Enhanced SAP Business Suite Integration Use Case

For this case, note the following:

- There is no support for central user administration with this use case.
- When integrating SAP Identity Management with the SAP Business Suite, application-specific identity data is also provisioned. To ensure that the correct data is provisioned based on the systems that are integrated, there are application-specific Business Add-Ins (BAdIs) to use for preprocessing and postprocessing. These BAdIs are handled as privileges in the Identity Center as type FUNCTION_SET. You need to include them in the business roles that apply to the corresponding SAP Business Suite applications.
- By default, the Identity Center also maintains user account data when provisioning. For certain applications, you may want to have certain identity data provisioned without having a user account created for the identity, for example, when provisioning business partner data. For this case, create a dedicated repository for the AS ABAP where the user account should not be created. For this repository, specify the NO_USER_ACCOUNT repository constant .

2.2.2 Limitations and Considerations that Apply to Specific Connectors

2.2.2.1 Limitations that Apply to All Connectors

The following limitations apply when using the SAP provisioning framework:

- The users used for the connections should be technical users that do not have to change their passwords, for example, service users in AS ABAP or technical users in AS Java.

  > **Caution**
  >
  > Since the connections are system-to-system connections that do not have a user interface, if the user is a dialog user and is required to change his or her password, for example, if the password is initial, then errors will occur.

  > **Note**
  >
  > The administrator of the LDAP directory must create a user that SAP Identity Management can use to connect to the LDAP server. This user should have read and search permissions as well as create and change authorizations for all branches of the LDAP directory.

- Whenever a user attribute is changed (except for role and privilege assignments), all user attributes are provisioned to the selected back-end systems (not only the changed attributes). If you want to remove attributes from the set of attributes to provision, modify the *Update System Privilege trigger attributes* pass in the initial load job for the appropriate connected system. This pass contains a negative list of attributes that are not to be provisioned to the target systems.
- To deactivate (or completely delete) a user in the SAP Identity Management identity store and in all target systems, first remove all privileges from the user assignments. This will delete the user in the individual repositories. After that, you can deactivate or delete the user in the identity store. If you deactivate or delete a user without removing the privilege assignments, the user will be deleted in the identity store, but not in the individual repositories.
  By default, the web-enabled task *Inactivate Identity* is configured to only deactivate a user in the identity store and not delete it. In this way, the history of the user can be retained. If you want to actually delete the identity, adjust the pass accordingly. (Set MX_INACTIVE to FALSE in the *Destination* tab for the *Inactivate Identity* pass.)
- When performing the initial loads, consolidation occurs based on user IDs, meaning that an identity is created in the identity store for each unique user ID that is read.
- Company addresses are read from the system that is specified as the leading system for company addresses and provisioned to the rest of the connected systems. This means you cannot maintain system-dependent company addresses throughout your landscape.

2.2.2.2 Limitations and Considerations for AS ABAP/SAP Business Suite System Connectors

- Time dependencies for privilege assignments are read into the Identity Center with the initial load. The privilege assignments are then provisioned to the target systems when they become active.

  > **Caution**
  >
  > After the initial load, the time dependencies are stored in the Identity Center and no longer in the AS ABAP. Previous time-dependent assignments are lost in this step, therefore, you no longer have a history of such assignments. You also no longer see future assignments in the AS ABAP.

  To improve efficiency, you can execute the `PRGN_COMPRESS_TIMES` report with the *Remove Validity Periods That Have Already Expired* option for all users. This removes all outdated role assignments so that the initial load only reads active and future role assignments.
- For dual-stack systems, use the dual-stack repository template when setting up the repository. For jobs, use the AS ABAP job templates. The dual-stack repository type contains the connection information for both the AS ABAP and the AS Java backend systems, and the job templates check whether the system is a dual-stack system at execution time.
- The ABAP connector does not support reference users.
- In AS ABAP systems, a new Customizing switch for local user management defines the user group as mandatory field for specific clients (see *SAP Note 1663177*). Therefore, users can no longer be created without entering a valid user group. If you activate this switch for any AS ABAP repository, you must ensure that for each user a corresponding user group is available, for example, using an entry field in your customized user interface.
- Composite roles and derived roles are read into the identity store, however, there is no information in the Identity Center to indicate these role types. In the Identity Center, you see a flat list containing all roles.
- When you use SAP Identity Management, you should not assign roles and profiles locally in your AS ABAP systems any longer. All local assignments of roles to users are overwritten by any change in the user's central assignments carried out with SAP Identity Management. If you change any assignment there, a list of all assigned roles and privileges for the user is sent to the relevant AS ABAP system overwriting all local data in the AS ABAP system. To synchronize the authorization assignments in SAP Identity Management and the local AS ABAP, we recommend to use reconciliation jobs.
- Whenever a role or group assignment is changed, all role, profile, and group assignments are provisioned (not just the delta). The assignments are provisioned to all systems that are affected by the change.
- The Provisioning framework for SAP Systems does not support indirect role assignments coming from SAP Human Capital Management (HCM). If you want to manage the roles on a per user bases in SAP NetWeaver Identity Management, you need to assign the roles directly to a user. Besides, all the role assignments provisioned from SAP NetWeaver Identity Management will be direct assignments.
- Mobile numbers must not contain a hyphen (-). The ABAP connector interprets the hyphen (-) as an extension, but the AS ABAP ignores extensions for mobile numbers.
- When connecting to an AS ABAP Release 4.6C, the password used for the connection needs to be entered in the repository constants in upper case.
- Not all identity attributes are supported, for example, licensing attributes. See *Appendix B: Mapping Between Identity Center and AS ABAP Attributes* for a list of the supported attributes.

Related Information

Appendix B: Mapping Between Identity Center and AS ABAP Attributes [page 149]
SAP Note 1663177 - SU01: User group as required entry field

2.2.2.3 Additional Prerequisites for AS ABAP/SAP Business Suite System Connectors

- Automatic profile generation must be enabled on the AS ABAP so that changes to role assignments are automatically reflected in a user's profile.
  You can check this using table maintenance (for example, transaction `SM30`). Maintain the `PRGN_CUST` table. Make sure an entry with the name AUTO_USERCOMPARE exists in the table and that it contains the value YES.

  > **Tip**
  >
  > If you do not activate AUTO_USERCOMPARE, then run the `PFCG_TIME_DEPENDENCY` report after executing any provisioning steps.

- The user type for the communication user should be communication user.
- To make sure the communication user used for the ABAP connector only has the necessary authorizations in the back-end system, assign the `SAP_BC_SEC_IDM_COMMUNICATION` role to the user (see *SAP Note 1557803*).
  This role was updated with Release 7.0 SPS 2 with authorizations for using the CUA, and with Release 7.1 for authorizations to retrieve value help values. Therefore, if you are upgrading to SPS2 or Release 7.1 respectively, and want to use these features, then you must also upload the new version of the role, regenerate the corresponding profiles, and update the role assignment for the communication user.
- For enhanced Business Suite integration, the communication user also needs the `SAP_CA_BP_IDM_INTEGRATION` role.

Related Information

SAP Note 1557803 - Correction of role SAP_BC_SEC_IDM_COMMUNICATION
SAP Note 327917 - New user types as of Release 4.6C

2.2.2.4 Limitations and Considerations when Connecting a CUA System

- To support a CUA landscape, connect the CUA central system to the Identity Center using the ABAP connector. The Identity Center provisions identity data to the CUA central system, which in turn provisions the

data to its child systems. This provisioning takes place according to the configuration of the attribute distribution settings on the central system.

- The CUA is not supported with the SAP Business Suite integration use case.
- Although you do not have to change the attribute distribution settings (using transaction `SCUM`), we recommend using the global distribution setting for attributes so that they can be maintained in the Identity Center.
- Only connect the CUA central system to the Identity Center. Do not connect any of the CUA child systems. If you want to connect a child system directly to the Identity Center, disconnect it from CUA first.
- If a corresponding LDAP directory is also connected to the Identity Center, then the LDAP synchronization for the CUA central system is obsolete.
- You no longer need to assign users to systems in the CUA landscape as the Identity Center makes this correlation when a user is assigned a privilege in the corresponding system.

2.2.2.5 Limitations and Considerations When Connecting an AS Java to an LDAP Directory

- Only the privilege assignments are provisioned to the AS Java repository. All other attributes are handled by the LDAP back-end repository. The user must exist in the LDAP repository before you assign any privileges to him or her in the Java repository. Assigning the Java account privilege or another Java role privilege to the user does not automatically create the user in the LDAP repository. You can still enable or disable users, because the hook for the back-end repository (LDAP) is defined.

2.2.2.6 Additional Prerequisites for AS Java System Connectors

- The communication user used for the AS Java connector should be a technical user and should only have the necessary authorizations in the back-end system. As of AS Java Release 6.40, the appropriate authorizations are provided with the UME action `UME.Spml_Write_Action`. (There is also an action called `UME.Spml_Read_Action` for read-only access.) Prior to Release 6.40, the action to use is `MANAGE_ALL_COMPANIES`.
- Whenever a role or group assignment is changed, all role, profile, and group assignments are provisioned (not just the delta). The assignments are provisioned to all systems that are affected by the change.
- For AS Java with an LDAP directory as the UME user store, note that the UME group assignments are not provisioned to UME users who are stored in the LDAP directory server. UME group assignments are provisioned to those users that are stored in the database (for example, Administrator). LDAP group assignments are provisioned directly to the users that are stored in the directory server.

2.2.2.7 Limitations and Considerations for LDAP Directory Connectors

Templates for the Sun Microsystems Sun One LDAP server and Microsoft Active Directory Server (ADS) are provided. You can adjust the tasks and jobs for other directory servers to meet your needs on a project base. Privilege grouping is not supported for LDAP directories.

2.2.2.8 Restrictions for SAP HANA Connectors

Validity

For the `MX_VALID_FROM` user attribute, take into account that, if the valid from date for the user is earlier than the current date, the user is provisioned to the SAP HANA system with a validity from the current date. This limitation comes from the SAP HANA system, in which you cannot create a user with a validity starting in the past.

Password Provisioning

If an administrator sets a productive password in the Identity Management system, the user also has to configure it in the SAP HANA system. For more information, see the SAP HANA Platform documentation.

Privilege Grouping

Since no multiple assignments are possible in the SAP HANA system, the SAP HANA Connector in the Identity Management system does not support assignment grouping. For this reason, privileges are provisioned to the SAP HANA system separately, but not as a group.

Setting Emails for Different Users

When you create a user and set its e-mail address with the `MX_MAIL_PRIMARY` attribute, you must use a unique e-mail. If you define an e-mail that already exists for another user, you will get an error message. That is a requirement of the SAP HANA system.

Related Information

SAP HANA Platform

2.2.2.9 Additional Prerequisites for SAP HANA Connector

To use SAP HANA Connector for SAP Identity Management, you have to fulfill the following requirements:

- You have to create a technical user in SAP HANA with the following roles or privileges:
  - MONITORING role
  - ROLE ADMIN system privilege
  - USER ADMIN system privilege
  - GRANT_ACTIVATED_ROLE object privilege and set it for execution

    Example

    In SAP HANA studio, you just need to create the privilege and select the *EXECUTE* checkbox.
  - REVOKE_ACTIVATED_ROLE object privilege and set it for execution
  - GRANT_APPLICATION_PRIVILEGE object privilege and set it for execution
  - REVOKE_APPLICATION_PRIVILEGE object privilege and set it for execution
  - To grant privileges to other users and roles, a user must have the permission required to grant these privileges.

    Example

    To grant privileges to other users in SAP HANA studio, you can select the *Grantable to other users and roles* checkbox for system privileges and allow *Grantable to others* for object privileges.

Recommendation

To use a permanent password that you do not have to reset, disable the password lifetime.

Example

Creating a technical user JOHN with SQL statements:

```
CREATE USER JOHN PASSWORD Abc123;
ALTER USER JOHN DISABLE PASSWORD LIFETIME;
GRANT MONITORING TO JOHN;
GRANT ROLE ADMIN TO JOHN;
GRANT USER ADMIN TO JOHN;
GRANT EXECUTE ON GRANT_ACTIVATED_ROLE TO JOHN;
GRANT EXECUTE ON REVOKE_ACTIVATED_ROLE TO JOHN;
GRANT EXECUTE ON GRANT_APPLICATION_PRIVILEGE TO JOHN;
GRANT EXECUTE ON REVOKE_APPLICATION_PRIVILEGE TO JOHN;
```

- Follow all other requirements for creating technical users in SAP HANA with SQL statements or via the Developer Studio.

- You have to re-import the provisioning framework.
- If you want the connector to support activated SAP HANA roles, system and application privileges, and the e-mail address, locale, time zone attributes and the custom user attributes, you have to create and run a new load job for your repositories. If the initial load job is already created, you just need to re-run it.
- Make sure that `ngdbc.jar` file used for the JDBC driver is defined as a classpath extension. This file is necessary for the dispatchers.

  Example

  In the Microsoft Management Console (MMC), choose *Tools* > *Options* > *Java* and add the path to the `ngdbc.jar` file in the *Classpath extensions* field.

Related Information

Creating a Technical User with SQL Statements

Creating a Technical User via Developer Studio: *Security Administration* > *Managing SAP HANA Users* > *User Provisioning* > *Creating Users*

SAP HANA Security Guide

Determining the Leading System for Attributes [page 100]

2.2.3 Considerations When Customizing the Provisioning Framework

If you need to modify the provisioning framework to meet your needs, then copy the corresponding templates to a custom folder and only modify the copied tasks. Make sure the links to tasks in repository definitions point to the copied tasks (as applicable). See *Rules and Recommendations*.

Related Information

Rules and Recommendations [page 26]

3 Before You Start

3.1 Overview

The SAP provisioning framework provides a set of templates that you can reference when you set up the system-specific jobs used for your provisioning use case.

Before you start working with the templates and creating the jobs, you should familiarize yourself with the structure and content of the framework. You should be familiar with:

- The template files provided for the different use cases.
- The entry types that you will be working with, for example, the MX_PERSON entry type represents user objects in the system.
- The attributes that describe these entry types.
- How to use tasks and jobs to work with the entry types.
- The syntax of privileges used by the SAP provisioning framework.

These aspects are described in the sections that follow.

> **Tip**
>
> This section provides background information about how the SAP provisioning framework works. For more information about how to import the framework and implement your use case, see *Implementation Process*.

Related Information

Implementation Process [page 30]

3.1.1 Template Files

The table below shows the template files that are provided with the SAP provisioning framework and when they are used. You can find them in the folder `<Install_folder>\Templates\Identity Center\SAP Provisioning framework`.

Template Files

File	Description
`SAP Provisioning Framework.mcc`	Main template file that contains the core tasks, web-enabled tasks, and the connector-specific tasks that apply to the fundamental use case of connecting SAP systems to SAP Identity Management.
`HCM_Staging_Area_Identity store.mcc`	This template file contains a staging area identity store to use when connecting an SAP HCM system to SAP Identity Management.
`SPML_IDS_Identity store.mcc`	This template file provides an identity store and framework to use when integrating those SAP Business Suite applications (for example SAP CRM or SAP SRM) that send SPML requests using bgRFC from the SAP HCM system to SAP SAP NetWeaver Identity Management.

> **Tip**
>
> There are additional files contained in the template folder, for example, `IDServ_Provisioning_Framework.mcc`. These files are used by other use cases, for example, identity services, and described in the corresponding documentation.

3.1.2 Entry Types

The identity store stores the identity data according to a schema that consists of entry types and attributes. The entry types are objects that describe how the different identityrelevant objects are represented in the Identity Center. The entry types used when working with the SAP provisioning framework are:

- MX_PERSON
  This is the entry type used for user objects in the system.
- MX_ROLE
  This is the entry type used for business role objects. Nesting MX_ROLE entries is possible.
- MX_PRIVILEGE
  This is the entry type used for permission objects (that is, technical roles) in the system, for example,
  - ABAP roles and profiles
  - Portal and UME roles
  - UME database groups
  - LDAP groups
  - SAP HANA™ database roles

  Nesting is not possible.
- MX_GROUP
  This is the entry type used for LDAP and AS Java group hierarchies that contain privileges. For example, in addition to being a privilege itself, an LDAP or AS Java group can contain privileges that represent ABAP roles,

ABAP profiles, or portal roles. The MX_GROUP attribute contains the hierarchical structure used for assigning these privileges to the users.
For more information on the relationship between MX_GROUP and MX_PRIVILEGE, see *Group Concepts*.

- MX_COMPANY_ADDRESS
  This is the entry type used for company addresses.
- MX_HCM_EMPLOYEE
  This is an entry type used for employees read from the SAP HCM system. It allows for event-driven provisioning for SAP HCM identity data. It is included with the HCM staging area identity store.

These entry types are delivered with predefined sets of attributes that you can extend to meet your needs.

Related Information

Group Concepts [page 23]

3.1.3 Attributes

The schema used by the SAP provisioning framework contains a number of attributes that are used to describe the entry types (for example, MX_LASTNAME, MX_FIRSTNAME). See the identity store schema for a complete list of the attributes available.

Some of the most important are shown in the table below.

Attributes

Attribute	Description	Applicable Entry Type
MSKEYVALUE	Unique identifier for the identity object.	All
ACCOUNT<Repository>	Unique user ID for the user in the target repository.	MX_PERSON
MX_REPOSITORYNAME	Identifier for the home repository where the original privilege is defined.	MX_PRIVILEGE

For more information about the default schema delivered with the Identity Center, see the documentation on SCN.

Related Information

Identity Center – Identity Store Schema on the SAP NetWeaver Identity Management 7.2 Documentation page

3.1.4 Tasks and Jobs

Setting up SAP Identity Management for provisioning and the identity provisioning itself takes place using tasks and jobs. Although both are flexible and you can use either in many situations, we provide the following guidelines.

- Tasks
  Use tasks for provisioning identity data when changes occur. They are triggered if any attribute is changed for any reason (using the administration user interface or jobs), for example, when a user account is changed from the administration user interface.
- Jobs
  Use jobs for performing specific mass operations like initial loads or updates. You can start jobs explicitly or schedule them to run at a certain time.

The way that tasks and jobs are reflected when using the SAP provisioning framework is described below.

3.1.5 Task Templates

The framework provides a set of task templates that you can refer to when creating the tasks to use for identity management. These templates are divided into the following categories:

- CORE
  This group contains those tasks that apply to all connectors, for example, the core provisioning tasks, web-enabled tasks, or notification tasks.
- CONNECTORS
  This group includes task templates that are specific to the specific system type. They include tasks for AS ABAP, AS Java, Microsoft Active Directory Server, SUN LDAP servers, and SAP HANA database.

3.1.5.1 Job Templates

The framework also provides a set of templates that you can use for setting up jobs. The following jobs are supported:

- Initial Load jobs
  Run this job to retrieve the identity information from the connected system and store it in the identity store in the Identity Center. There is an initial load job for each connected system (i.e. ABAP, AS Java (Database/LDAP), Business Suite AS ABAP, LDAP (ADS/SUNONE), SAP HANA).
- ABAP Read Help Values
  Run this job prior to the initial load to read the value help from the ABAP system. The value help content is then written to the corresponding database table specified in the schema.
- ABAP - Provision Company Addresses to ABAP Repositories
  Run this job to provision the company addresses read during the initial load from the ABAP source system to other connected ABAP systems.
- Reset Delta jobs
  Run this job to reset the delta information. There are reset delta jobs available for ABAP and LDAP (ADS).

- Clean IS with Delta
  Run this job to delete all entries from the identity store, including any delta information (if used).
- Clean SAP_HR_Staging Area IS with Delta
  Run this job to delete all entries from the SAP HCM staging area identity store, including any delta information (if used).
- Clean SPML_Staging Area IS
  Run this job to delete all entries from the SPML staging area identity store.

During an initial load from a repository (for a system), a number of authorization privileges are created (if not already existing) using the following naming convention:

```
PRIV:<TYPE>:<REP_NAME>:<AUTH_NAME>
```

One privilege for each authorization in the repository/system is created. The privilege type depends on the system type for which the privilege applies, for example GROUP or PROFILE. Some examples are:

```
PRIV:GROUP:AD:CN\=TelnetClients\,CN\=Users\,DC\=testtrdl\,DC\=local
```

```
PRIV:PROFILE:ABAP:AUTHNAME
```

During the initial load, these privileges are assigned to the users read from the repository, depending on their authorizations.

Assignment of these privileges depends on the presence of the account privilege.

3.1.5.2 Function Set Privileges

When working with the enhanced SAP Business Suite use case, function set privileges are created for each of the SAP Business Suite applications that are activated for provisioning with SAP Identity Management. These privileges have the following syntax:

`PRIV:FUNCTION_SET:<Repository>:<BAdI_Filter_Value>`

Assign this privilege to business roles or identities that use the corresponding SAP Business Suite application.

> **Tip**
>
> Active SAP Business Suite applications are specified in the `IDM_BADI_FILTER BAdI` filter table.

3.1.5.3 System-Specific Privileges

The following system-specific privileges are created:

- `PRIV:SYSTEM:<Repository>`: This a system privilege that is used internally by the SAP provisioning framework. It is not visible in any user interfaces. Never manually assign (or unassign) it to any users.

- `PRIV:<Repository>:ONLY`: This is a system account privilege used for users or company addresses:
  - Assign it to a user when creating the user. This assignment indicates that changes to the user are to be provisioned to the corresponding system. To delete the user in the corresponding system, you remove this privilege.
  - Assign it to a company address. This assignment indicates that changes to the company address are to be provisioned to the corresponding system. To delete the company address in the corresponding system, you remove this privilege.

    > **Note**
    >
    > You can only delete company addresses that are not assigned to any user in the corresponding ABAP system.

3.1.6 Group Concepts

The Identity Center and the SAP provisioning framework support the following group concepts used in some repositories:

- A group defines the permissions the assigned users have in the back-end system and serves as a container object for all users needing the respective permissions (for example, Microsoft Active Directory).
- A group is just a set of users. Instead of assigning permissions (for example, roles) directly to users, administrators can assign permissions to group objects. The group members inherit the permissions assigned to the group automatically at runtime. The permissions are not directly, physically assigned to the users (for example, AS Java).

With the support of these group concepts, you can continue handling your group, role, and profile assignments in the repositories the way you used to. During the initial load, the group concept is applied automatically for the following repositories:

- ADS
- Sun One
- AS Java with database only
- AS Java with database and LDAP directory

> **Note**
>
> For AS ABAP repositories the provisioning of groups does not work, because the AS ABAP does not have a similar group concept. If the administrator tries, for example, to assign a group to a business role in AS ABAP, an error message appears.

Group Architecture

Group objects from repositories are represented in the Identity Center as a linked combination of an MX_GROUP object and an MX_PRIVILEGE object. This combines the advantages of the two entry types: Hierarchy support with the MX_GROUP and eventing support with the MX_PRIVILEGE. The SAP provisioning framework keeps these two

objects synchronized. Whenever an assignment between any of the two objects and an MX_PERSON or MX_PRIVILEGE is changed, the same change is automatically applied to the other object.

Identities assigned to a group object in the repository are assigned to the MX_GROUP object and the MX_PRIVILEGE object.

Repository roles (which are represented as MX_PRIVILEGE objects) assigned to a repository group object are assigned to the MX_GROUP object. Note: These assignments cannot be applied to the group privilege as well, as it is not possible to assign privileges to other privileges.

Assignments between different repository groups from the same repository are represented as a link between the different MX_GROUP objects. Note: These assignments cannot be applied to the group privilege as well, as it is not possible to assign privileges to other privileges.

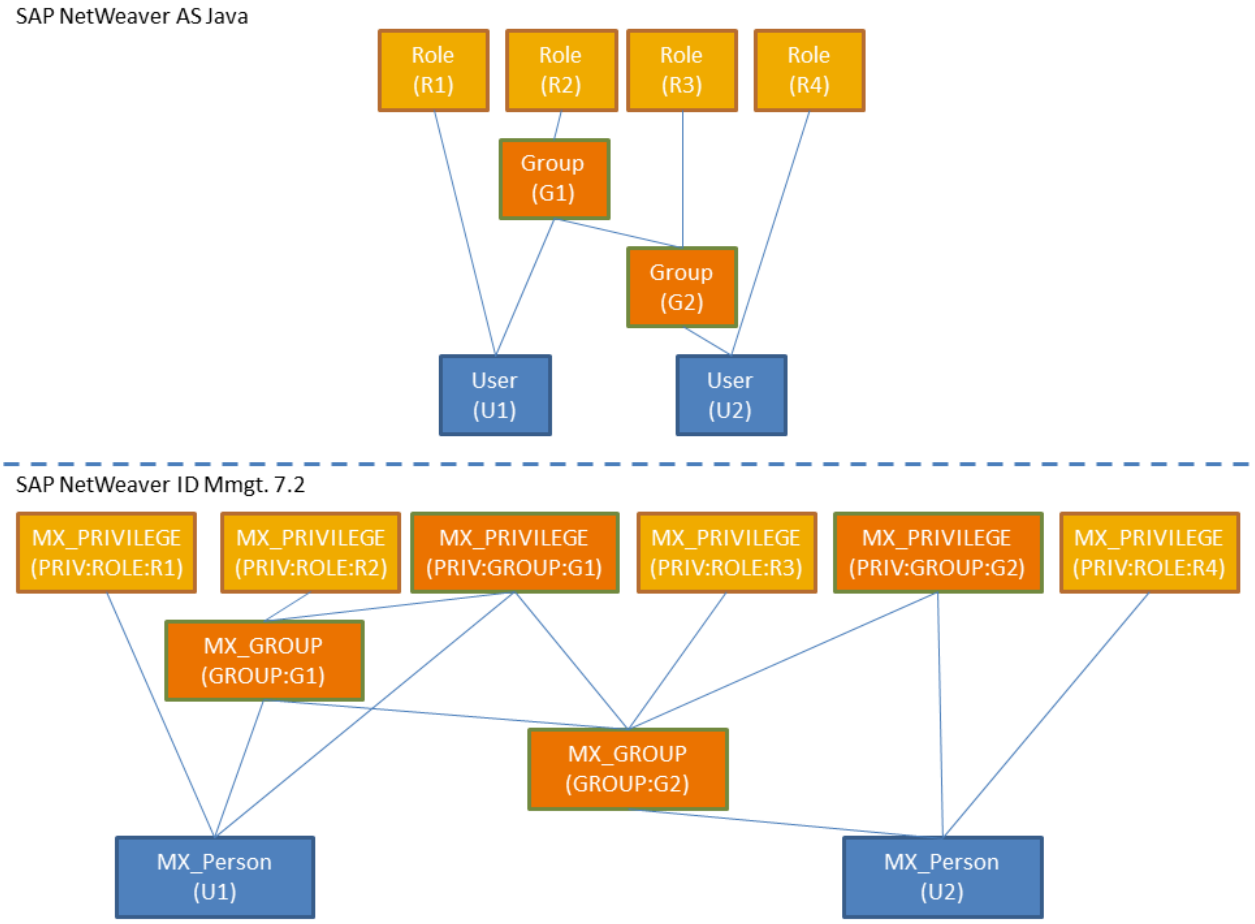
Consequently, the provisioning is triggered automatically as either the core part of the framework, an administrator or a job assigns the MX_PRIVILEGE (for the group object).

The following objects can be assigned to an MX_GROUP object:

- MX_GROUP
- MX_PERSON
- MX_PRIVILEGE

If all involved objects already exist in the back-end repository, the data is provisioned into the back-end system as it is.

As an example we take a closer look at an AS Java repository with DB-only configuration.



The Group (G1) of the AS Java is represented by the two objects MX_GROUP (GROUP:G1) and MX_PRIVILEGE (PROV: GROUP:G1) in the Identity Center.

On the AS Java, User (U1) is assigned to this Group (G1) and to the Role (R1) objects. Through the group assignment the user is also assigned Role (R2).

In Identity Management, the user is represented by the MX_ PERSON (U1) object. The AS Java Role (R1) is represented by the MX_PRIVILEGE (PRIV:ROLE:R1) object and is directly assigned to the MX_PERSON (U1) object. The user's assignment to Group (G1) is represented in the Identity Management by two assignments: One to the MX_GROUP (GROUP:G1) assignment and one to the MX_PRIVILEGE (PRIV:GROUP:G1) assignment.

If in the Identity Center an MX_PERSON object is assigned to an MX_PRIVILEGE that represents a group, this assignment triggers the provisioning of the MX_PERSONMX_ PRIVILEGE assignment to the repository. In addition, the core framework updates the assignment between the MX_PERSON and the corresponding MX_GROUP object.

On the AS Java there are groups from different datasources. If in the User Management Engine (UME) the datasource is a built-in groups adapter, then there is no user-to-group assignment in identity management. Such an assignment is not useful as the group membership of the users is determined at runtime. It depends on the status of the user, for example, whether he or she is authenticated or not. Identity Management does not display any members for the groups. If you add members to built-in UME groups using Identity Management and try to provision this group, UME displays an error message that the group is read-only.

For all other groups, Identity Management displays the group members and changes will be provisioned to the connected systems.

3.2 Rules and Recommendations

You most likely have to modify the jobs and tasks provided by the provisioning framework, for example, to set up your own Workflow approval process. There are several rules and recommendations that you need to take into account when adapting the framework to your own use case. See the points below.

3.2.1 Identity Stores

Each AS Java installation can only access one identity store. Therefore, to reduce the number of AS Java installations, we recommend that you set up one single identity store that is accessible from the user interface functions (for example, Workflow and Administration).

You may want to set up additional identity stores as staging areas (for example, with the SAP HCM use case), but these staging area identity stores do not have to be accessed by the user interfaces and therefore do not require additional AS Java installations.

3.2.2 Tasks

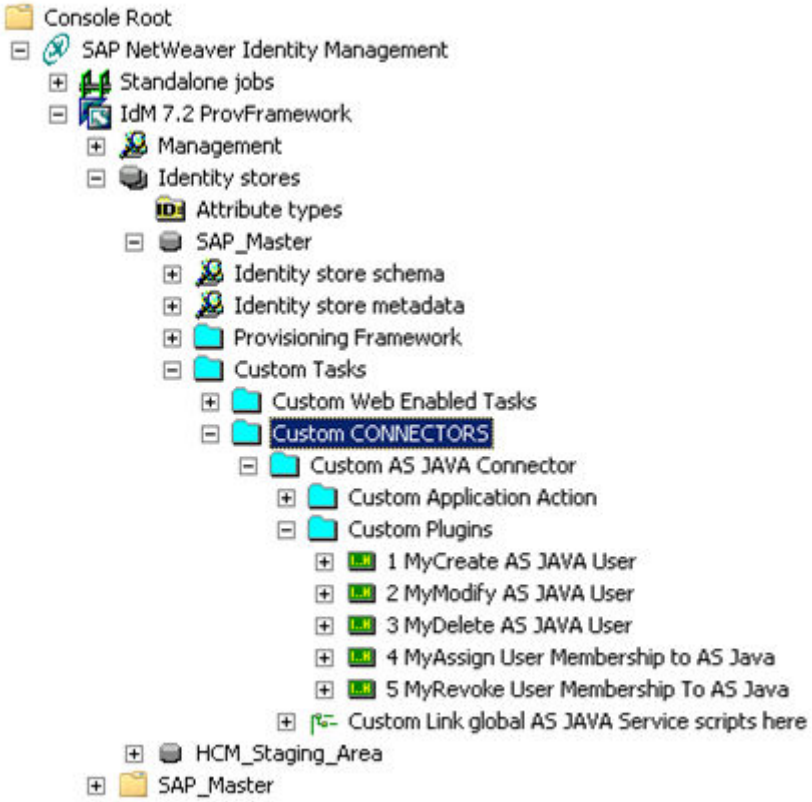
The SAP provisioning frameworks provides two primary task folders, one for core framework tasks and one for the connector-specific tasks. Note the following:

- The core framework tasks contain the common tasks needed for the SAP provisioning framework. Other than the web-enabled tasks, you do not need to make any adjustment, and doing so can cause the SAP provisioning framework to no longer function properly. After an upgrade, this part contains many changes.
- You probably have to modify the web-enabled tasks. Therefore, when setting up the user interfaces, create a second provisioning folder to use for your custom tasks (Custom Tasks in the example below). Copy the *Web Enabled Tasks* folder into this folder. Make your changes in this copied folder and not in the *SAP Provisioning Framework* folder. Disable any templates that are not used. See the example below.

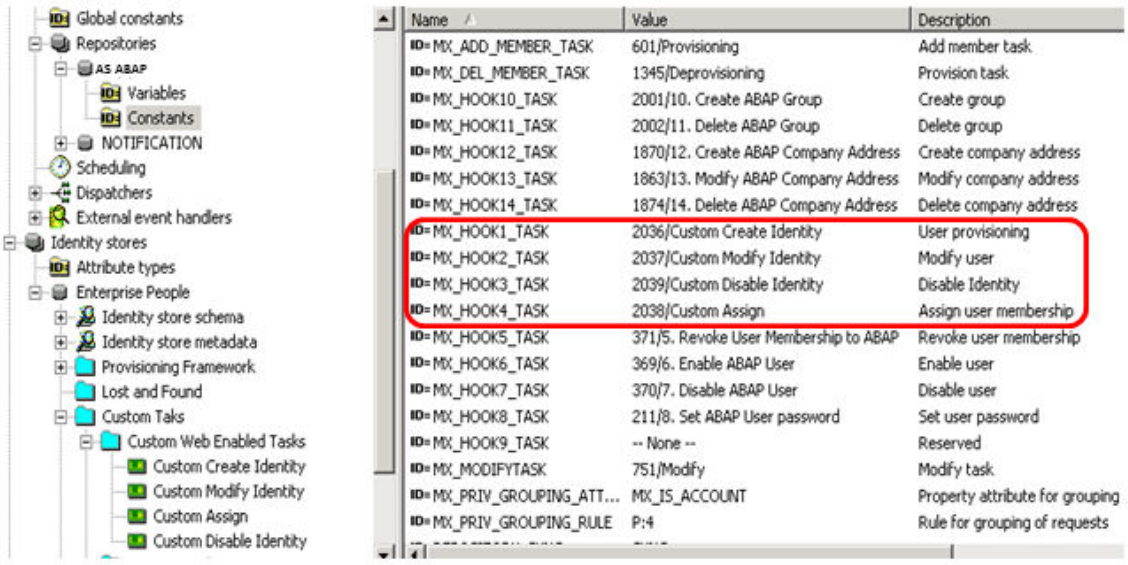
For more information, see *Set Up User Interfaces for User Administration (Workflow)*.

- If you need to make any other adjustments, then do so in the connector-specific tasks (for example, creating, modifying, and deleting users). In this case, also copy the tasks provided with the framework into your own folder(s) and modify them there. Note the following:
  - Only copy those plug-ins (HOOK tasks) you really want to change. Do not create superfluous copies.
  - Make sure that your copied plug-ins do not contain any links to standard tasks. Links to existing tasks also modify the original tasks and therefore such links are also overwritten if you import an updated version of the framework.
  - Modify the plug-ins as necessary. You should not need to modify the application actions or system type tasks.
  - Afterwards adjust the repository constants that contain the task numbers for the plug-ins.

  See the example below.



The figure below shows an ABAP repository with HOOK tasks containing linked custom tasks that are displayed as values:

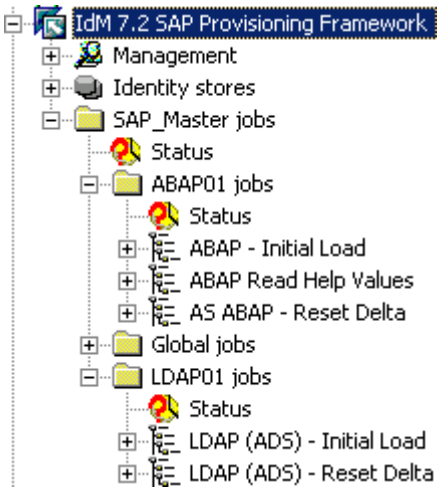


Related Information

Set Up User Interfaces for User Administration (Workflow) [page 105]

3.2.3 Jobs

- When you create the job folder that contains your jobs, we also recommend structuring the job folders according to each system. Use the repository name for the folder name. Set up a folder for global jobs as well. See the example below.



See the procedure for setting up the corresponding jobs.

> **Note**
>
> You are free to set up the job folders as you like, however, if you follow these recommendations and naming conventions, then it is easier to resolve consulting or support issues if they arise.

Related Information

Creating and Configuring the Jobs for Each Connector [page 96]

4 Implementation Process

To implement identity provisioning in SAP Identity Management based on the templates we provide, proceed as follows:

1. Import the provisioning framework for SAP systems into the SAP Identity Management Identity Center.
2. Perform the initial configuration. You must make some adjustments in the result handling so that the right tasks are triggered. In addition, check the global constants and adjust if necessary.
   The 7.2 version of this configuration guide is simplified as compared to its 7.1 version. Some manual steps are now automated and therefore superfluous in most cases, for example, creating event tasks or linking modify tasks. The exceptions that still need manual configuration are still described in this guide.
3. Determine your system landscape. Identify your leading identity system and your target systems.
4. Set up the landscape for the use case. This includes:
   - For system landscapes where you use the SAP HCM system as the leading system for employee data, you must also set up a staging area in the Identity Center, set up the Virtual Directory Server, configure the SAP HCM system, and maintain the attribute mappings.
   - Creating repositories for each system that you connect to the Identity Center.
   - Setting up the jobs to use for the use case.
   - Determine the leading system for attributes that use value help and read the value help from this system.
   - Import the identity data into the Identity Center's identity store by performing the initial loads.
   - Clean up the data that was collected from the initial loads. Changes will be provisioned back to the connected systems.
5. Set up the user interfaces for performing user administration.
6. Maintain the business roles in the Identity Center.

Afterwards, changes to user master records in the leading system and changes to technical roles or the corresponding user and role assignments (in the original system for the roles or their assignments) are provisioned to the various systems.

4.1 Importing the Provisioning Framework for SAP Systems

Prerequisites

- You have installed the Identity Center and performed the initial configuration. For more information, see the installation guides and the Identity Center Initial Configuration guide.
- You have created an Identity Center configuration to use for the provisioning framework for SAP systems. This is notated in the following procedure as `<IC_Configuration_for_SAP_Systems>`.
- You have created a dispatcher for running jobs.

- If you are connecting a central user administration (CUA) system to the Identity Center, then you have assigned the `SAP_BC_SEC_IDM_COMMUNICATION` role to the communication user (see *SAP Note 1557803*).

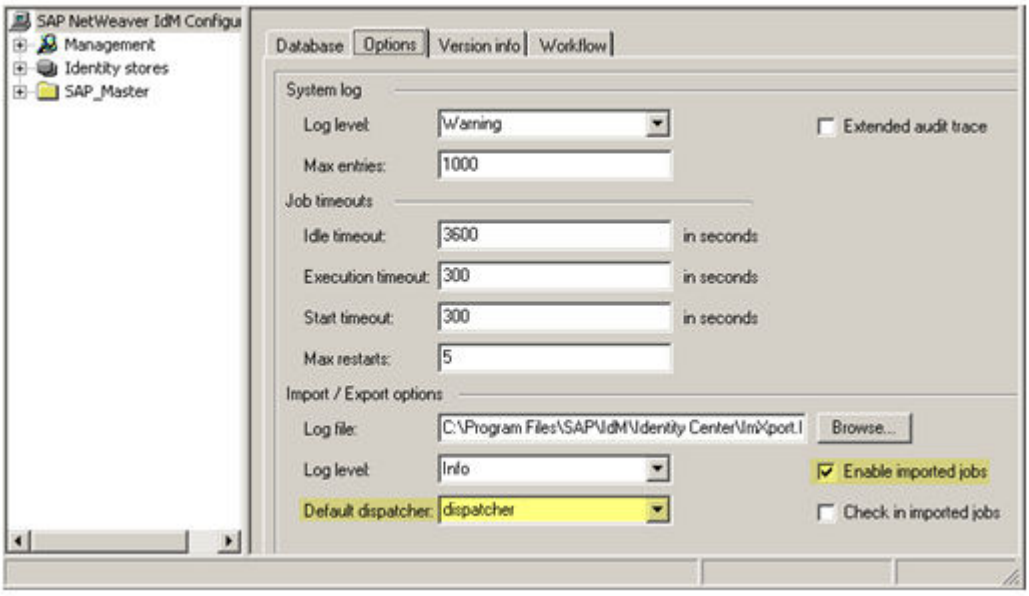
Context

The first step in working with the provisioning framework for SAP systems is to import them into the Identity Center.

If you are updating the framework from a previous version, see *Updating the Provisioning Framework*.

Procedure

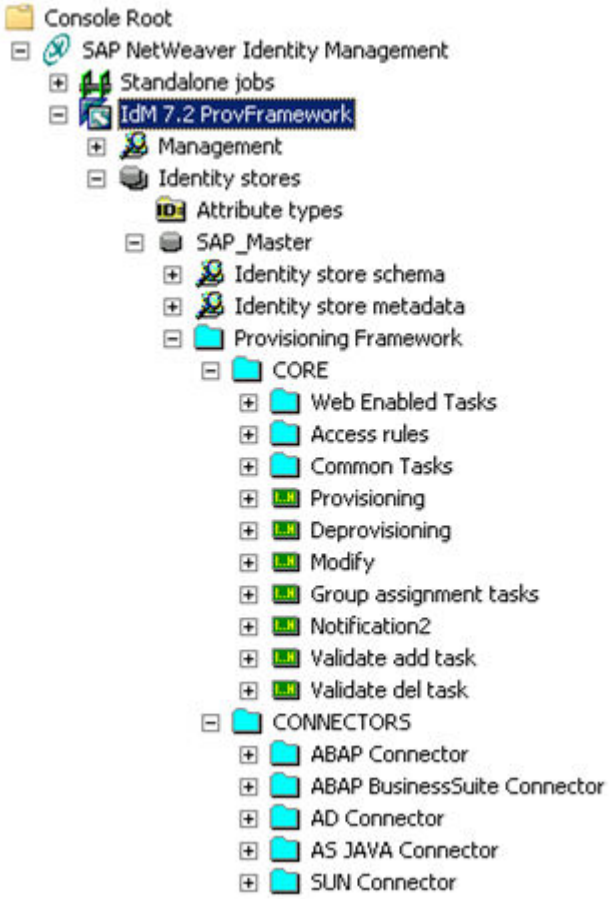
1. In the Identity Center, select the *<IC_Configuration_for_SAP_Systems>* and choose the *Options* tab page.
2. Make sure the *Enable imported jobs* option is activated and that you selected your dispatcher as the *Default dispatcher*. See the figure below.



   If you do not select these options, then you must enable all of the tasks and set the dispatcher for each task after importing the provisioning framework.
3. Create an identity store to use with the provisioning framework for SAP systems.
4. Import the SAP provisioning framework.

Results

The SAP provisioning framework is imported into the Identity Center. See the figure below.



Related Information

SAP Note 1557803 - Correction of role SAP_BC_SEC_IDM_COMMUNICATION
Installation and Initial Configuration Guides
Updating the Provisioning Framework [page 34]

4.1.1 Creating an Identity Store for the SAP Provisioning Framework

Context

Procedure

1. Under *Console Root* > *SAP NetWeaver Identity Management* > *<IC_Configuration_for_SAP_Systems>* > *Identity stores*, choose *New* > *Identity store...* from the context menu for the *Identity stores* node.
2. Follow the instructions provided by the wizard. Use the following data:

Field	Comment
Name	Specify a name for the identity store, for example, **`SAP_Master`**. Do not use special characters in the name.
Description	Optional
Automatically create new attributes	Deactivate (Recommended)
Entry types	Do not select any entry types.

> ⚠ Caution
>
> If you activate the option to automatically create new attributes and an error occurs in an attribute definition, for example, a typing error, then a corresponding erroneous attribute will also be automatically created in the identity store. This type of error is difficult to detect and fix.
>
> Therefore, we recommend not activating this option. In this case, you must manually create the missing attributes manually any time you create a repository. For more information about how to create these attributes and which entry types apply to each attribute, see *Creating Repositories*.

Related Information

Creating Repositories [page 44]

4.1.2 Importing the SAP Provisioning Framework

Context

Procedure

1. Choose *Import...* from the context menu for your identity store.
2. Select the *SAP Provisioning Framework.mcc* file from the file system and choose *Open*. You can find it in the folder *<Install_folder>\Templates\Identity Center\SAP Provisioning framework*. This file contains the templates available with the framework.
3. In the *Import option* screen that appears, select the following:
    1. *Import* (or *Update* if you are updating the framework from a previous support package).
    2. In the *Advanced* tab page, select the dispatcher(s) that will run the import jobs by selecting the *Run jobs* option for a default dispatcher.
4. Choose *Next*.
5. In the *Import provision group* screen, select the *SAP Provisioning Framework* node and choose *Import*.

    You receive a message about the status.

    > **Note**
    >
    > You can ignore warnings that refer to cyclic dependencies. Check however, for jobs and tasks for which a dispatcher could not be set.

6. Choose *Finish*.

4.2 Updating the Provisioning Framework

Context

If you are updating the framework from a previous version, then follow the instructions above for importing the framework (see also *SAP Note 1618734*). Note the following:

- Because updating the provisioning framework overwrites the existing framework, we do not recommend changing the framework itself, but instead, you should copy the templates to your own folders before you make changes (see *Rules and Recommendations*). If you did make changes to the framework, copy the changed folders to a separate location before performing the update.
- Make sure that you select the correct level in the structure to start the import. This is one level above the *Provisioning Framework* folder. In the example above, this is *SAP_Master*.

Procedure

1. Select *Import...* from the context menu for this node.

2. Select the *SAP Provisioning Framework.mcc* file from the file system and choose *Open*. You can find it in the `<Install_folder>\Templates\Identity Center\SAP Provisioning framework` folder. This file contains the templates available with the framework.
3. In the *Import option* screen, select *Update*. Then select the *Ignore timestamp* option. This ensures that the newest version of the framework is imported completely into the Identity Center.

   In addition, when you select the *Ignore timestamp* option, the *Remove groups from target system which have been deleted in source system* option is also automatically activated.
4. In the *Update global script* screen, select the *Overwrite* option and activate *Use this action for all matching global scripts*. Any changes to scripts will be overwritten with the updated provisioning framework.
5. In the *Import provision group* screen, select the *SAP Provisioning Framework* node and choose *Import*. You receive a message about the status.

   You can ignore warnings that refer to cyclic dependencies. Check however, for jobs and tasks for which a dispatcher could not be set.
6. Choose *Finish*.

Related Information

SAP Note 1618734 - Upgrading SAP Provisioning Framework
Rules and Recommendations [page 26]

4.3 Post Processing: Checking Result Handling and Global Constants

Context

After importing the framework, you must perform the following post-processing steps:

Procedure

1. Check the result handling.
2. Check the global constant SAP_MASTER_IDS_ID.

4.3.1 Checking the Result Handling for the Provisioning and Deprovisioning Tasks

Context

After importing the SAP provisioning framework, check the result handling for the provisioning and deprovisioning tasks. Perform the following:

Procedure

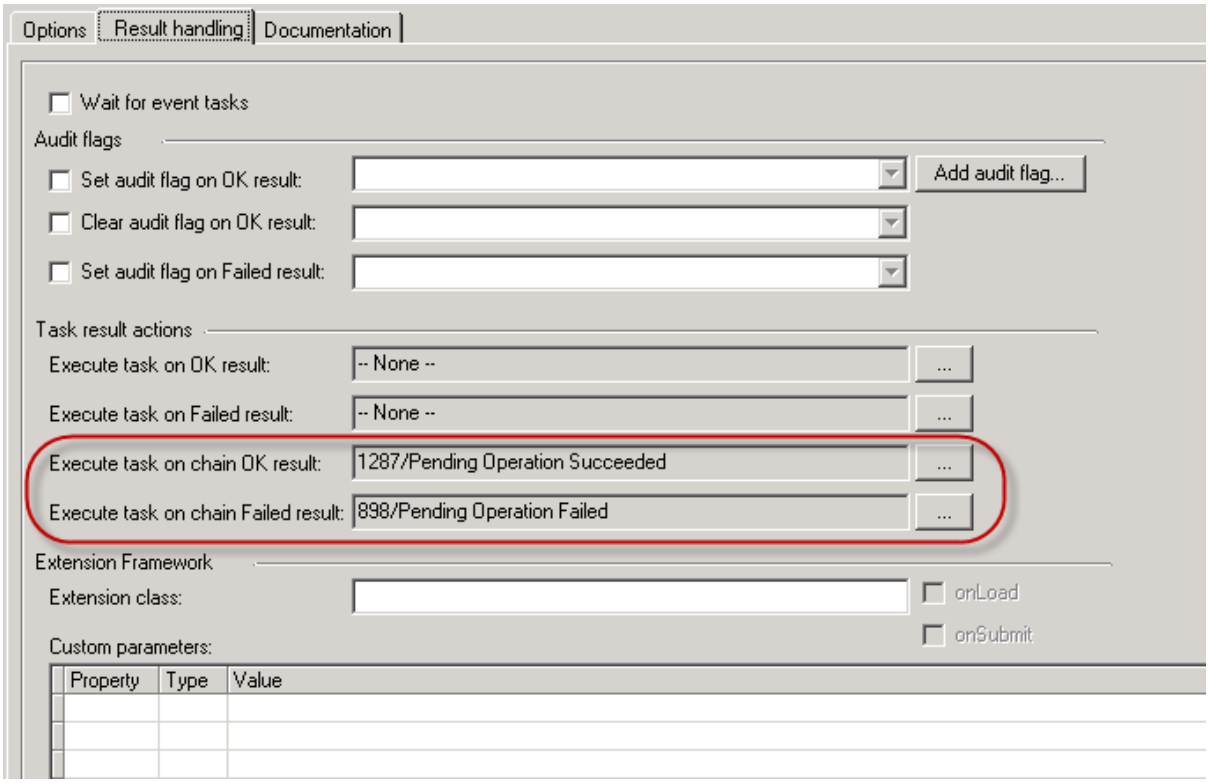
1. Navigate to the provisioning task.

   You can find this task under *<IC_Configuration_for_SAP_Systems>* > *Identity stores* > *<Identity_store>* > *Provisioning Framework* > *CORE* .

2. Select the *Provisioning* task.
3. Choose the *Result handling* tab.
4. Under *Task result actions* section, verify that the *Pending Operation Succeeded* task is set in the field *Execute task on chain OK result* and that the task *Pending Operation Failed* is set in the field *Execute task on chain Failed result*. If these are not set correctly, adjust them as necessary.

   You can find these tasks under *<Identity_store>* > *Provisioning Framework* > *CORE* > *Common Tasks* > *Status Tasks* .

   See the figure below.



5. Choose *Apply* if you made any changes.
6. Complete the above steps for the deprovisioning task also.

4.3.2 Post-Import Processing: Adjusting Global Constants

Context

After importing the framework, you must check the global constant `SAP_MASTER_IDS_ID`. Do the following steps:

Procedure

1. Check the identity store ID for the productive identity store.
2. Navigate to *<IC_Configuration_for_SAP_Systems>* > *Management* > *Global constants* and check the value of the global constant *SAP_MASTER_IDS_ID*.
3. Check if this constant is set to the productive identity store ID and change it, if necessary.

4.3.3 Enabling E-Mail Notification and Adjusting Notification Constants

There is a predefined repository provided with the SAP provisioning framework that is used for specifying how notifications should be handled.

Context

To set up the use of e-mail notifications, execute the following steps:

Procedure

1. Adjust the constants shown in the table below as necessary.
2. Set the *Add* and the *Modify* tasks for the MX_TRIGGER_NOTIFICATION attribute.

4.3.3.1 Setting the Add and the Modify Tasks for the MX_TRIGGER_NOTIFICATION Attribute

Context

Procedure

1. In the Identity Center, choose *<IC_Configuration_for_SAP_Systems>* > *Identity stores* > *<Identity_store>* > *Identity store schema* > *Attributes*.
2. Double-click the MX_TRIGGER_NOTIFICATION and choose the *Event tasks* tab.
3. Next to the *Add* and *Modify* fields, choose *...*.
4. In the *Select task* dialog window, choose *Identity Center* > *Provisioning Framework* > *CORE* > *Notification* > *<Notification Type>* > *(EMAIL)* > *<Send e-mail notification>*.
5. Choose *OK* twice to save the entry.

4.3.3.2 Triggering Notifications Using Events

Context

In addition, there are tasks in the core framework that trigger notifications for events not directly related to the provisioning framework, for example, assigning a business role. To use this kind of e-mail notification, for example, to notify users of a change in their assigned roles, set the Add and the Delete tasks for the MXREF_MX_ROLE attribute. This procedure also applies to the other notification tasks that are available in the same task folder.

Procedure

1. In the Identity Center, choose *<IC_Configuration_for_SAP_Systems>* > *Identity Stores* > *<Identity_Store>* > *Identity store schema* > *Attributes*.
2. Double-click the MXREF_MX_ROLE and choose the *Event tasks* tab.
3. Next to the *Add* and *Delete* fields, choose *....*
4. In the Select task dialog window, choose *Provisioning Framework* > *CORE* > *Common Tasks* > *Notification*:
   - For the *Add* field, choose the *Trigger notification: user assigned role task*.
   - For the *Delete* field, choose the Trigger notification: user role revoked task.
5. Choose *OK* twice to save each entry.

4.3.3.3 Repository Constants

You can find the repository and its constants under *<IC_Configuration_for_SAP_Systems>* > *Management* > *Repositories* > *NOTIFICATION* > *Constants*.

Repository Constants

Repository Constant	Value	Comment
DEFAULT_MAIL_ATTRIBUTE		Used to configure the name of the user attribute that the system uses to determine the e-mail address of the user for e-mail notifications. The default value is MX_MAIL_PRIMARY.

Repository Constant	Value	Comment
ENABLED_FOR	<List of Events for Notification>	The default value is the following list: • PASSWORD_CHANGED • CREATE_USER • MODIFY_USER • DELETE_USER • ASSIGN_USER • REVOKE_USER • ENABLE_USER • DISABLE_USER • ROLE_ASSIGNED • ROLE_REVOKED • FAILURE These are the valid names of the events that are enabled for notification.
MAIL_DEBUG	<TRUE/FALSE>	Sets whether debug mode is used.
MAIL_DEBUG_RECIPIENTS	<recipient_name> @<address>	Used if debug mode is on. If not set, then MX_PRIMARY_MAIL is used.
MAIL_ORIGINATOR	<originator_name> @<address>	This e-mail address is used by the task Send E-Mail when creating identities.
MAIL_SMTP_HOST	<hostname_of_mailserver>	This is the mail server to send mails when creating identities.
MAIL_SMTP_PORT	<SMTP_port_on_mailserver>	This is the SMTP port on the mail server that is used to send mails when creating identities.

Repository Constant	Value	Comment
MAIL_TEMPLATE_FOLDER	<folder_containing_ mail_template>	This is the folder containing a text template to use for mail notification. The default is `%$ddm.path% \Templates\ Identity Center \ Provisioning\ Notifications\`. Make sure the path uses the correct syntax for your operating system and contains the required e-mail template files. If you configure the e-mail notification jobs to be run by a dispatcher on a machine where no Identity Center Designtime Components are installed together with the Runtime Components, copy the template files from a Designtime Components installation to a folder on the dispatcher machine and adjust this constant accordingly.

4.4 Determine the System Landscape

Once you have set up the initial configuration, you must set up the Identity Center for your particular system landscape. You can use the information provided in *SAP Identity Management Provisioning Framework for SAP Systems: Architectural Overview* to determine which use case best fits to your system landscape. This can help when determining which system you use as the leading identity system. See the table below.

Use Case Overview

Use Case	Leading Identity System	Source System for Data	Provisioned Data
SAP HCM	SAP HCM	SAP HCM: Employee data (Identities)	SAP HCM: Employee data (Identities) LDAP server: Users and user/group assignments

Use Case	Leading Identity System	Source System for Data	Provisioned Data
SAP Enterprise Portal	Corporate LDAP directory	LDAP server: Users and groups AS Java: Portal roles, UME roles AS ABAP: ABAP roles, ABAP profiles, company addresses	AS Java (read from LDAP): UME users and UME groups AS Java (provisioned from IC): Role assignments AS ABAP: Users, user/role assignments, and user/profile assignments
Identity Lifecycle Management	SAP HCM	SAP HCM: Employee data (Identities) AS Java: Portal roles and UME roles AS ABAP: ABAP roles, ABAP profiles, company addresses	LDAP server: Users and user/group assignments AS Java (read from LDAP): UME users and UME groups AS Java (provisioned from IC): Role assignments AS ABAP: Users, user/role assignments, and user/profile assignments
Enhanced SAP Business Suite Integration	SAP HCM	SAP HCM: Employee data (Identities)	SAP HCM: Employee data (Identities) LDAP server: Users and user/group assignments SAP Business Suite systems: Users, user/role assignments, and user/profile assignments plus application-specific identity data according to SAP Business Suite scenario.
Central User Administration (CUA)	Central User Administration (CUA)	Identity Center	SAP Identity Management Identity data

Note

Keep in mind that when setting up the portal environment use case, the corporate LDAP directory is used as both the leading system for SAP Identity Management and as the user data store for the portal system. Therefore, set up the Identity Center to read the user data from the LDAP directory server and provision users to all of the target systems except for the AS Java that uses the LDAP directory server as its data source. This AS Java/portal system reads the user data directly from the LDAP directory server.

User/role assignments are provisioned to all systems, including the AS Java where the portal runs.

Based on this information:

1. Identify your leading identity system.
2. Identify your target systems.

3. Continue with setting up the landscape as described in the sections that follow.

Related Information

SAP Identity Management Provisioning Framework for SAP Systems: Architectural Overview

4.5 Setting up the Landscape

Context

Once you have identified the systems you want to connect to SAP Identity Management, set up the landscape accordingly. See *Limitations and Considerations* for considerations that apply to each use case and each connector type.

Proceed as follows:

Procedure

1. Create repositories for each of the systems.
2. For AS ABAP systems, read the value help content from the system(s) that provide the value help for attributes.
3. If you are using an SAP HCM system as the leading system for employee data, then set it up accordingly. If you are not using SAP HCM in your landscape, you can skip this step.
4. Create and configure the jobs needed for each connector.
5. Prepare the initial loads.
6. Run the initial loads for each connected system.
7. Clean up the collected data.

Related Information

SAP Identity Management Implementation Guide - Transport
Limitations and Considerations [page 8]

4.5.1 Creating Repositories

Context

The first step is to create a repository in the Identity Center for each system in the system landscape. The repository data provides the connection information to the system and other system-specific information.

> **Note**
>
> For AS ABAP systems, the repository entry corresponds to a logical system on the AS ABAP (that is, system ID and client).

Procedure

1. In the Identity Center under *<IC_Configuration_for_SAP_Systems>* > *Management* > *Repositories*, choose *New* > *Repository ...*.
2. In the wizard, select the template in the *<Install_folder>\Templates\Identity Center\Repositories* folder that applies to the system type, for example:
   - ADS for SAP PF
   - Business Suite AS ABAP (Load Balanced Connection)
   - SAP NetWeaver AS for ABAP (Load Balanced Connection)
   - SAP NetWeaver AS for Java repository
   - SAP NetWeaver Dual Stack (Load Balanced Connection)
   - SAP HANA database
3. In the wizard, enter a name and description for the repository and the data that applies to the system connection. When using Oracle, make sure the name of the repository is no longer than six characters.

   > **Note**
   >
   > The name can contain only letters (A-Z) and numbers (0-9). Spaces or special characters are not supported.

   > **Tip**
   >
   > When choosing a name, consider the later transport of the repository to the productive system. The name in the test system is transported to the productive system. There, you cannot rename the repository.

   - If you only need one repository of each type, you can choose a name that fits for the test system as well as for the productive system, for example, CORPORATE_ADS.
   - If you need several repositories of the same type, you transport the test system repository and copy it in the productive system to create them. In this case, you can create a repository in the test system named,

for example, ABAP_TEMPLATE. This you transport to the productive system and use it as a template to create other system-specific repositories with names you define during the copy process. For SAP systems, we recommend using **<SID><Client>** as the name of these new repositories.

4. Specify the repository constants that apply to the system type. See *Appendix A: Repository Constants* for a list of constants per repository type. This appendix also contains additional information, for example, that using SSL is a prerequisite for password provisioning.

> **Note**
>
> The user you create with a repository constant should be the same as the one in the system (AS Java, AS ABAP, LDAP, etc) you are connected to, which means that the repository and the system should have the same user. In addition, the user name defined by the repository constant must match with the user's logon ID in the Administration User Interface. That means that the logon ID of the SAP NetWeaver Identity Management maps to the user name in the repository.

> **Note**
>
> If you are setting up any SAP Business Suite systems and have provisioning tasks where a corresponding user account should not be created or maintained, then you must set up an additional repository for the system that contains the NO_USER_ACCOUNT constant with the value 1.

> **Caution**
>
> If the repository constants apply to an AS ABAP Release 4.6C, make sure you enter the password to use for the connection in upper case.

After using the wizard, you can maintain additional constants, for example, the options for using Secure Network Communications (SNC) to securely connect to the AS ABAP.

Results

The initial load job templates automatically adds the attributes shown in the table below to the identity store attributes for the repository.

To check these attributes, choose *<IC_Configuration_for_SAP_Systems>* > *Identity stores* > *<Identity_store>* > *Identity store schema* > *Attributes*. The data for the attributes are shown in the table below.

Identity Store Attributes

Attribute Name (Under General)	Applicable for Repository Type	Entry Types to Allow (Under Entry Types)
ACCOUNT <REPOSITORYNAME>	AS ABAP Dual-Stack SAP Business Suite	MX_PERSON

Attribute Name (Under General)	Applicable for Repository Type	Entry Types to Allow (Under Entry Types)
ACCOUNT <REPOSITORYNAME>	LDAP	MX_PERSON MX_PRIVILEGE MX_GROUP
ACCOUNT <REPOSITORYNAME>	AS Java	MX_PERSON MX_GROUP
ACCOUNT <REPOSITORYNAME>	SAP HANA	MX_PERSON MX_PRIVILEGE

Related Information

Appendix A: Repository Constants [page 121]

4.5.2 Attributes Using Value Help Content

There are certain attributes in the provisioning framework's identity store schema that make use of the value help provided by the AS ABAP system(s).

These attributes are classified into three categories, according to the storage location:

- Fixed values: The value help content is maintained in fixed domain values or data elements. Examples for this category include value help for date or number formats.
- System tables: The value help content is maintained in ABAP system tables (not modifiable). Examples for this category include value help for languages or time zones.
- Customer table entries: The value help content is available in tables that are modifiable by customers, for example, application tables, control tables, or Customizing tables. Examples for this category include value help for printer settings or salutations.

> **Note**
>
> For a complete list of attributes that support value help, see *Appendix C: Attributes that Support Value Help*.

The value help content that is either fixed or available in system tables is delivered with the provisioning framework for SAP systems and stored in the `mxi_AttrValueHelp` database table. The value help content that you can define yourself must be read from the corresponding AS ABAP system into this table. To do this, use the job *ABAP Read Help Values*.

> ⚠ Caution
>
> If there are discrepancies between the values maintained in the `mxi_AttrValueHelp` table and the data read from the system during an initial load, you will receive errors.
>
> Therefore, if you are connecting multiple AS ABAP systems to the Identity Center that all use value help, then choose one of these systems as the leading system for the value help for each attribute. Make sure the value help content is maintained in this system so that it can be used by all of the connected systems.

> ⚠ Caution
>
> If you do not read the value help (or maintain their values in the identity store schema manually), then these values are missing in the table and cannot be found for the corresponding attributes. In this case, you will receive errors during the initial loads.

Related Information

Appendix C: Attributes that Support Value Help [page 165]

4.5.3 Reading Value Help Content

Prerequisites

You know which system is the leading system to use for the value help for each attribute.

Context

Procedure

1. Set the properties for each attribute in the identity store schema that uses value help.

   For those attributes where the data is provided with the provisioning framework for SAP systems (as fixed values or in system tables), the properties should be set correctly. You can use the procedure below to check these properties.
2. Run the job that reads the value help from the leading system.

4.5.3.1 Changing the Properties for Each Attribute

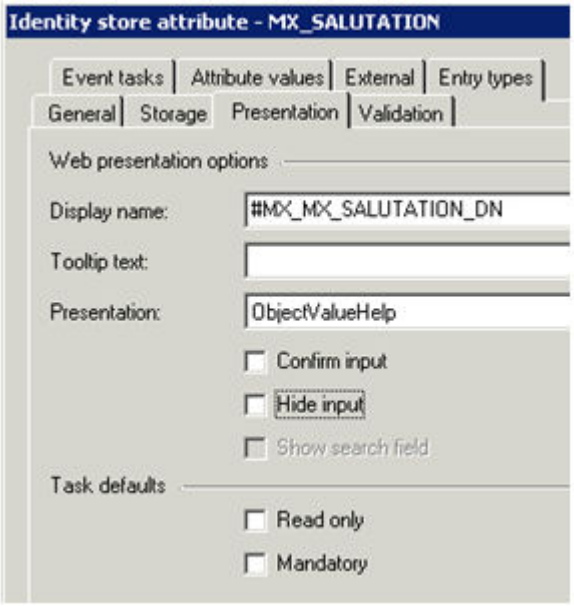
Context

Procedure

1. Navigate to the identity store schema attributes. (Choose *<IC_Configuration_for_SAP_Systems>* > *Identity stores* > *<Identity_store>* > *Identity store schema* > *Attributes* .)
2. Select the attribute to modify with a double-click. (See the table in *Appendix C: Attributes that Support Value Help*.

   The properties for the attribute appear.
3. Choose the *Presentation* tab page.
4. Set the *Presentation* option to *ObjectValueHelp*.

   See the example below for the MX_SALUTATION attribute.

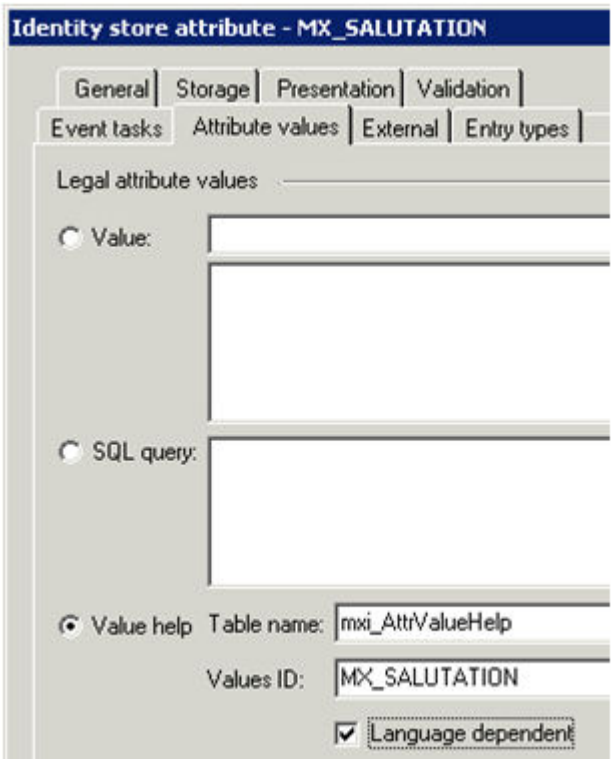


5. Choose the *Attribute values* tab page.
6. Enter **`mxi_AttrValueHelp`** as the *Value help Table name* and set the language dependency option.
7. Set the *Values ID* to the attribute name with the following exceptions as shown in the table below. For these attributes, use the values ID shown.

Values IDs

Attribute	Values ID
MX_ACADEMIC_TITLE_1	MX_ACADEMIC_TITLE
MX_ACADEMIC_TITLE_2	MX_ACADEMIC_TITLE
MX_NAME_PREFIX_1	MX_NAME_PREFIX
MX_NAME_PREFIX_2	MX_NAME_PREFIX

See the example below for the MX_SALUTATION attribute.



Related Information

Appendix C: Attributes that Support Value Help [page 165]

4.5.3.2 Running the Read Help Values Job

Context

Procedure

1. To organize the jobs for multiple systems, you can create subfolders. Choose *<IC_Configuration_for_SAP_Systems>* > *Job folder*. Choose *New* > *Folder...*.
2. To create the read help values job, choose *<IC_Configuration_for_SAP_Systems>* > *Job folder* > *<optionally_subfolder>*. Choose *New* > *Run job wizard...*.

   > **Note**
   >
   > If you have multiple systems that are leading systems for different attributes, then select the system that is the most appropriate.

3. Follow the instructions provided by the wizard. In step 2 of the wizard, choose *Identity Center* > *Jobs* > *SAP NetWeaver* > *ABAP Read Help Values*.
4. In step 3, select the leading system from which to load the help values as repository.
5. Choose *Finish*.

   The job is created in your folder.
6. Enable the job, select *Java* as the runtime engine, and select a dispatcher for the job.
7. If this system is not the leading system for the value help for all attributes, then adjust the repository for those passes that use a different system.
8. Save the data.

   > **Note**
   >
   > There are also passes for reading content for system-specific attributes such as MX_START_MENU or MX_PARAMETER. Although reading and provisioning such data is supported by the ABAP connector, these passes are deactivated by default because there is no support in the provisioning framework for storing and provisioning this data in a system-specific manner. If you want to read and provision this data, you must implement the provisioning rules yourself to meet your needs.

9. Run the job.

Related Information

Adjust the Repository for Passes Using a Different System [page 51]

4.5.3.2.1 Adjust the Repository for Passes Using a Different System

Context

Procedure

1. To change the source repository for a specific attribute, choose the respective task, for example, for the *Address Salutation* task.
2. In the *Job* folder, select the task in the *ABAP Read Help Values* job.
3. Go to the *Repository* tab page.
4. From the dropdown box, choose the source repository for this attribute.

> **Note**
>
> If the *Repository* field is not active, check whether you added a repository for the Help Value task. Select the *Help Value* task and check the *Repository* field. If it contains an entry, you cannot set a different repository for an individual attribute.

4.5.4 Setting up an SAP HCM System

Prerequisites

- The Virtual Directory Server is installed.
- The Identity Center is installed and configured.
- The SAP HCM system is installed and contains employee data.
- The user who exports the data from the SAP HCM system has the following PFCG roles assigned:
  - SAP_HR_LDAP_EXTRACTION (execution of data extraction)
  - SAP_HR_LDAP_PREPARE_EXTRACTION (needed for attribute mapping)
- An LDAP Connector is configured on the SAP HCM system.

- You have decided how to assign a user account name to an employee. See the *Limitations and Considerations When Using the SAP HCM Use Case*.

Context

When connecting an SAP HCM system to SAP Identity Management, the identity data is exported from the SAP HCM system and imported into the Identity Center. For this, the Virtual Directory Server is used as the common interface for processing the data. You can therefore use the export functions in SAP HCM that are available for exporting data to an LDAP directory. This data is then imported into a staging area in the Identity Center before being replicated into the productive identity store. Once the data is in the productive identity store, it can be provisioned to the connected systems, for example, another LDAP directory server.

Using a staging area instead of writing directly to the identity store has the following advantages:

- You can work with the data in the staging area before processing it further. For example, you can also set up the Workflow approval tasks to access the data in the staging area before writing it to the productive identity store.
- If you make changes to the database schema used for identity data in the SAP HCM system, you can adjust the attribute mapping in the staging area accordingly and you do not have to change the productive identity store's schema.

> **Note**
>
> We provide a template to use for setting up the staging area in the Identity Center.

To set up an SAP HCM system, proceed as described below.

Procedure

1. Import the staging area template.
2. Adjust the event handling for the MX_HCM_EMPLOYEE entry type.
3. Set up the Identity Center to assign the user account name.
4. Configure the Virtual Directory Server.
5. Configure the SAP HCM system and export the data.

   In systems with SAP ERP 6.0 SAP Enhancement Package 5 or higher, you can use the LDAP wizard (transaction `HRIDMWIZARD_START`) instead of the manual procedure described in this step.

Related Information

Limitations and Considerations When Using the SAP HCM Use Case [page 9]

4.5.4.1 Importing the Staging Area Template

Prerequisites

- You have followed the procedure in section Reading Value Help Content [page 47] for your HCM system. Otherwise you will get the following error message after running an HCM extract: `Value not legal for this attribute: Attribute: MX_SALUTATION` when storing attribute MX_SALUTATION=value.

Context

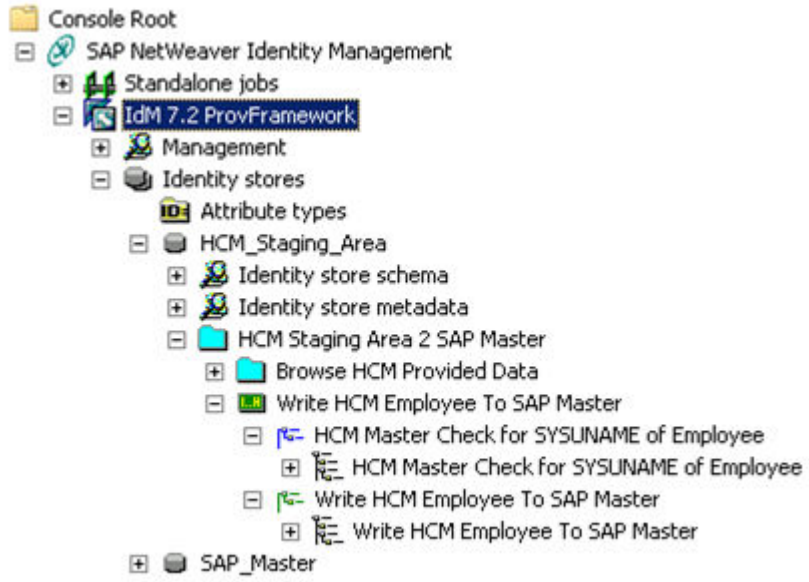
In this step, you import the template that contains the staging area identity store to use for SAP HCM, as well as the corresponding tasks for writing the identity data from the staging area to the productive identity store.

In the Identity Center, navigate to the staging area identity store.

Procedure

1. In the Identity Center, choose *Import...* from the context menu for the *Identity stores*.
2. Select the `HCM_Staging_Area_Identity store.mcc` file from the file system and choose *Open*. You can find it in the folder `<Install_folder>\Templates\Identity Center\SAP Provisioning framework`.

   The staging area identity store and corresponding provisioning tasks are imported into the Identity Center. See the figure below.



Note the identity store ID for the HCM staging area identity store. You need it when configuring the Virtual Directory Server. Make sure your HCM Staging area identity store ID is filled with a value after the import. This value must not collide with other identity store IDs that are already present.

3. On the *General* tab of the new identity store, set the *Automatically create attributes* flag. Also note the numeric ID for the SPML staging area identity store, which you can find on the same tab in the *ID/Name* field. Store the ID in the HR_STAGING_AREA_IDS_ID global constant under *<Identity Center>* > *Management* > *Global constants*. By default the value is set to 2. In case you already have other identity stores, you need to change this value to the actual number. You need this value again when configuring the Virtual Directory Server.

> **Note**
>
> Make sure that both tasks *HCM Master Check for SYSUNAME of Employee* and *Write HCM Employee to SAP Master* are enabled after import.
>
> Note that during import, one or more *Update global script* dialog windows may appear. Select *Use Existing* and set the flag *Use this action for all matching global scripts* and choose *Next*.

> **Note**
>
> When importing `HCM_Staging_Area_Identity store.mcc` file, make sure that your dispatcher is selected to run the staging area's jobs.

4.5.4.2 Adjusting the Event Handling for MX_HCM_EMPLOYEE

Context

After importing the staging area identity store, adjust the event handling for the MX_HCM_EMPLOYEE entry type.

Procedure

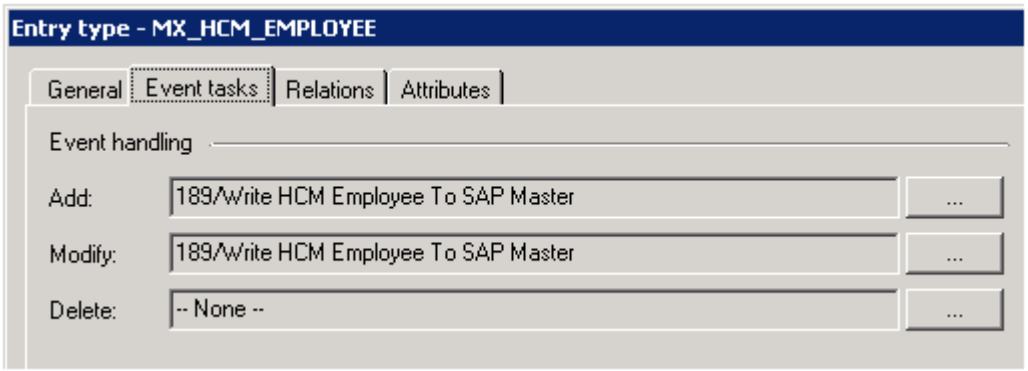
1. Open *Identity store schema* > *Entry types*.

> **Tip**
>
> Make sure you expand the Identity store schema of HCM_Staging_Area and not the one of the Enterprise People.

2. Select the *MX_HCM_Employee* entry type with a double-click.
3. Choose the *Event tasks* tab.

4. Under *Event handling*, select the *Write HCM Employee To SAP Master* ordered task for the *Add* and *Modify* event. You can find this task in the *Select task* screen under *Identity Center* > *HCM Staging Area 2 SAP Master*.

   See the screen shot below.



   Note that there is no *Delete* event task. This is due to the fact that users which are deleted in HCM are marked inactive in the Identity Management, using a *Modify* operation.

4.5.4.3 Setting up the Identity Center to Assign the User Account Name

Context

By default, for the SAP HCM use case, the user account name is determined by the SAP HCM system using the *P0105-SYHR_A_P0105_AF_SYSUNAME* field. As an alternative, the provisioning framework also supports using the *P0000-PERNR* field. To activate this mechanism, see the procedure below.

If you want to set up other mechanisms, then you must manually modify the tasks mentioned below according to your needs.

Procedure

1. In the Identity Center, navigate to the provisioning task for *HCM Master Check for SYSUNAME of Employee*.
2. To have the Identity Center determine the user name account using the *P0000-PERNR* field, disable this task. For the default set-up (use the *SYSUNAME* field), leave the task as it is.
3. Navigate to the *Write HCM Employee To SAP Master* pass in the task with the same name.
4. Choose the *Destination* tab page.
5. Depending on your set up, make sure the MSKEYVALUE attribute has the following value.

Values for MSKEYVALUE

Set Up	Value for MSKEYVALUE
User account name is determined by the SAP HCM system using the *SYSUNAME* field (default).	`$FUNCTION.sap_getSysUname(%P0000-PERNR %!!%P0105-SYHR_A_P0105_AF_SYSUNAME%!!% $WRITE_FUTURE_DATED_HIRES%)$$`
User account name is determined by the Identity Center using the *PERNR* field.	`$FUNCTION.sap_calcID(%P0000- PERNR%!! %P0105- SYHR_A_P0105_AF_SYSUNAME%!! %MSKEYVALUE%)$$`

6. Enable and disable the MSKEYVALUE rows accordingly and move the active MSKEYVALUE entry to the first row. It is then displayed in blue.

> **Note**
>
> This `sap_getSysUname` function could call a custom exit named `custom_generateHRID(Par)` that uses the attributes P0000-PERNR, SYHR_A_P0105_AF_SYSUNAME and Employee-Key (which is the MSKEYVALUE of the HCM staging area) as input parameters.
>
> Currently, the `custom_generateHRID` function returns an empty string. If necessary, change this function to adjust the MSKEYVALUE to fit your needs.

> **Tip**
>
> You can find the custom exit jscript `custom_generateHRID` under *Global scripts* > *JScript*. For editing **jscripts** it is recommended using a text editor, such as **jedit** or **notepad++**. You need to open the script that you work on in the Identity Center editor, copy it to your editor, do your changes and copy it back into the Identity Center editor.

4.5.4.4 Configuring the Virtual Directory Server

Prerequisites

- You have maintained the database connection for the identity store in Identity Center and know the password for the database user.
- The JDBC driver to use to access the Identity Center database is maintained in the class path for the Virtual Directory Server. (Maintain the driver under *Tools* > *Options* > *Classpath*.)
- You have imported the HCM staging area identity store into the Identity Center.

Context

In this section, we describe how to configure the Virtual Directory Server (VDS) so that the SAP HCM system can connect to it for the data export.

Procedure

1. Start the Virtual Directory Server console.
2. To maintain the configuration, choose *File* > *New*.
3. On the *New configuration* dialog that appears, choose *Group SAP NetWeaver 7.2* > *Template HCM LDAP EXTRACT for IDM* and then choose *OK*.
4. Configure the parameters to use for the VDS as shown in the table below.

VDS Parameters

Field	Value	Example	Comment
Port	389	389	Select a different port if 389 is already being used.
Display Name	<Name_of_VDS>	Identity Store	

Field	Value	Example	Comment
Identity Center URL	<Database_ Connection_ Parameters>	jdbc:sqlserver://localhost:1433; databasename=mxmc_db; user=mxmc_rt; password=<password>	Use the wizard (three dots) to maintain the URL. Examples for Microsoft SQL Server parameters are shown in the table that follows. **Tip** When going through the wizard for setting up the jdbc connection to the Identity Center database: you can find the name of your Identity Center database in your Identity Center. **Note** Make sure to use the '_rt' user when imputing the user for the jdbc connection, for example 'IDM_720_SP_COR_rt'
Identity Store ID	<Staging_Area_ Identity_Store _ID>	2	This ID was determined when setting up the staging area identity store.
Path to keys.ini	<Path_to_ keys.ini_File>	C:\usr\sap\IdM\ Identity Center\ Key\Keys.ini	Make sure the path and file name use the syntax needed for your operating system.
Username	<Directory_ Server_User>	hruser	This is the user that is used for the bind to the VDS. It is created if it does not yet exist.
Password	<Directory_ Server_User_ Password>	<password>	

VDS Parameters: Examples

Field	Value	Example	Comment
Server	<Server_Name>	localhost	

Field	Value	Example	Comment
Port	<Port>	MSSQL: 1433 Oracle Thin Driver: 1521 DB2: 50000	
Database	<Database_ Identifier>	mxmc_db	
User	<Database_ User>	mxmc_rt	Runtime user
Password	<Database_ User_Password>	<password>	You specified the password for the runtime user during the installation of the Identity Center database.
SID	<Service_Name>		Field only relevant for Oracle.
Schema	<Prefix_oper>	mxdb2_oper	Field only relevant for DB2.
FunctionPath	<Prefix_oper>	mxdb2_oper	Field only relevant for DB2.

5. Save the configuration.
6. Start the server.

4.5.4.5 Configure the SAP HCM System and Export the Data

Context

This topic describes how to configure the SAP HCM to export data to the Virtual Directory Server.

Procedure

1. Create the query to use for the export.
2. Maintain the attribute mapping between the HR fields and the input attributes used by the LDAP synchronization.
3. Create an RFC destination to use for the connection to the VDS.
4. Configure the parameters to use for this connection.
5. Maintain the mappings between the attributes used by the LDAP synchronization and the VDS.
6. Export the data.

> **Tip**
>
> Because the VDS does not use a specific LDAP schema for attributes, you can freely choose names for the attributes. To make maintenance easier, we recommend using the same attribute names throughout all of the mappings.

4.5.4.5.1 Creating the Query to Use for the Export

Context

In this step, you set up the query to use for the export. For this purpose, you can use the existing `LDAPEXTRACT604` query as a template. This query is assigned to the user group `SAPQUERY/L1`.

Create or modify the query in the SAP HCM Customizing development system and transport it to the productive system.

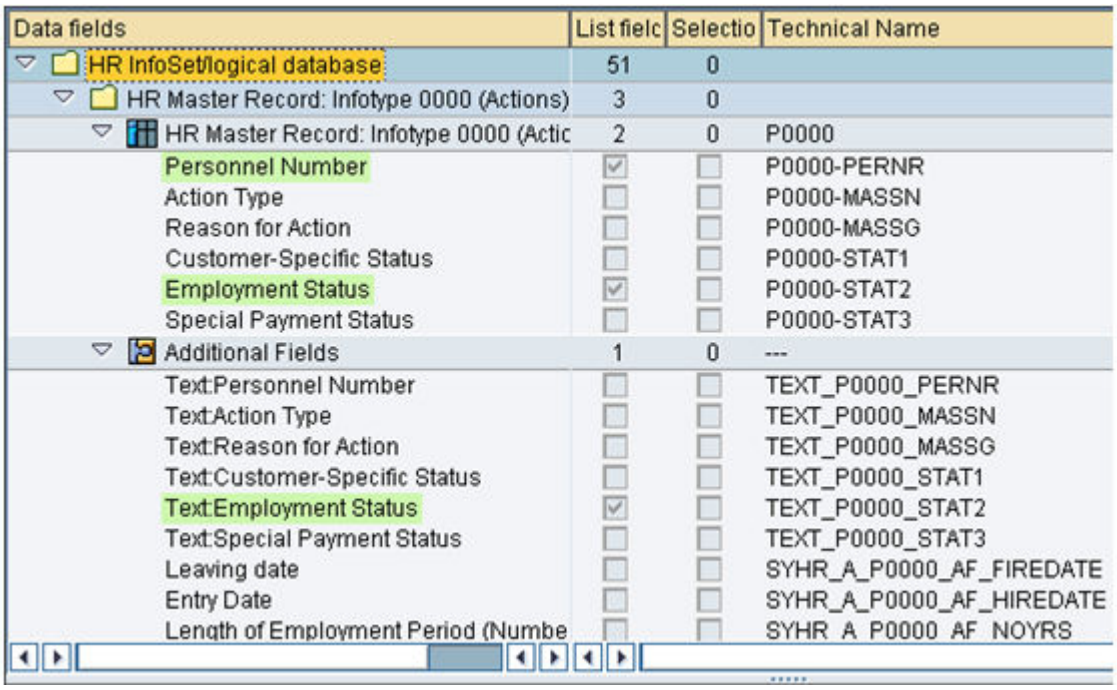
Procedure

1. Start query maintenance (transaction `SQ01`).
2. Choose *Edit* > *Other user group* and select the *SAPQUERY/L1* user group.

   The queries available for this user group are displayed.
3. Select *LDAPEXTRACT604* with a double-click and choose *Query* > *Copy*.
4. In the dialog that follows, enter a name for the new query, for example, LDAP_QUERY.
   a. The *Object Editing: Initial Screen* pop-up appears. Choose *OK*.
   b. In the *Create Object Directory Entry* dialog, enter Package **`/SAPQUERY/HR`** and choose *Save*.
   c. A *Warning* pop-up appears. Choose *OK*.
   d. In the *Prompt for transportable Workbench request* dialog, choose *New* if you need to create a request. After selecting a request, choose *OK*.
5. Select this query with a double-click and choose *Query* > *Change*.

   The attributes for the query appear.
6. To see the HR fields used by this query, choose *Basic List*.
7. To view the fields that are already selected in the example query, expand the data fields. These are the fields that are supported by the provisioning framework for SAP systems.

   See the figure below for a subset of the fields for Infotype 0000.



Caution

The attributes marked in the *LDAPEXTRACT604* sample query are supported by the SAP provisioning framework, meaning they are included in the schema and in the passes used for writing to the staging area and the productive identity store.

You can remove certain attributes from the query if you do not need to have them provisioned. However, if you add attributes, you will receive error messages when attempting to process the data further.

8. Note the Infotype number that the attributes belong to. You need this number when you maintain the attribute mapping in the next step.
9. Save the query and return to the initial screen.
10. Activate the query by executing it.

    If you need to create a variant for the copied query, proceed with the following steps:

    a. In the menu of transaction `sq01`, choose *Goto* > *Maintain variants...*
    b. In the *ABAP: Variants - Initial Screen* dialog, enter a variant name, for example: **`Z_TEST_IDM`**. Choose *Create*.
    c. Select a *Period*, for example *Current year* and choose *Variant Attributes*.
    d. Enter a description and choose *Save*.

Note

You must execute the query once so that the query is generated and available for later steps.

> **Tip**
>
> You can reduce the amount of data selected for this initial execution of the query by using a limited time period (for example, *Today*) and a range for the *Personnel Number* (for example, 1 to 1000).

4.5.4.5.2 Specifying the Attribute Mapping Between the HR Fields and LDAP Synchronization

Prerequisites

The query used for extracting the data is active.

Context

In this step, you map the HR fields that are selected by the query to the input attributes used by LDAP synchronization.

Procedure

1. Using field assignment maintenance (transaction `HRLDAP_MAP`), select the *Global Work Area* indicator.
2. Enter **`/SAPQUERY/L1`** as the *User Group*.
3. Enter the name of your query, for example, **`LDAP_QUERY`**.
4. Choose *Import*.

   The fields assigned to your query appear.
5. Maintain the *Attribute Grp* and *Attrib.Name* fields for each query field. Specify the attribute group so that it corresponds to the Infotype number you noted in the last step.

> **Tip**
>
> We recommend using the query field names as the attribute names.

> **Note**
>
> To omit a field, set the *Tech. Field* field. Fields marked as such are not exported.

> **Note**
>
> When maintaining the field assignments for data export (transaction `HRLDAP_MAP`), you can derive the *Attribute Group* from the query field's name. Example: P0001-KOSTL => Attribute Group P001. The only exception is query field SOURCE_SYSTEM. This query field must be mapped to attribute group 'P0002'.

The table below shows a subset of the fields, based on the sample query used in *Creating the Query to Use for the Export*.

VDS Parameters: MS SQL Example

Query Fld	Description	Attribute Grp	Attrib.Name
P0000-PERNR	Personnel Number	P0000	P0000-PERNR
P8003-OBJID	Object ID	P8003	P8003-OBJID
SYHR_A_P0002_AF_SPLIT_BEG	Split Start	P0002	SYHR_A_P0002_AF_SPLIT_BEG
SYHR_A_P0002_AF_SPLIT_END	Split End	P0002	SYHR_A_P0002_AF_SPLIT_END
P0002-NACHN	Last Name	P0002	P0002-NACHN
P0002-VORNA	First Name	P0002	P0002-VORNA
P0002-NAME2	Name at Birth	P0002	P0002-NAME2
P0001-ENAME	Formatted Name of Employee or Applicant	P0001	P0001-ENAME
TEXT_P0002_TITLE	Text: Title	P0002	TEXT_P0002_TITEL
P0002-TITEL	Title	P0002	P0002-TITEL
P0002-ANRED	Form-of- Address Key	P0002	P0002-ANRED
TEXT_P0002_ANRED	Text:Form-of- Address Key	P0002	TEXT_P0002_ANRED
...	...	...	...
SOURCE_SYSTEM	Source System	P0002	SOURCE_SYSTEM
SYHR_A_P0001_AF_PL_STRAS	House Number and Street	P0001	SYHR_A_P0001_AF_PL_STRAS
SYHR_A_P0001_AF_PL_ROOM1	Physical Room Number	P0001	SYHR_A_P0001_AF_PL_ROOM1
SYHR_A_P0001_AF_P_IS_MGR	Personnel Number is Manager	P0001	SYHR_A_P0001_AF_P_IS_MGR

6. Save the data.

Related Information

Creating the Query to Use for the Export [page 60]

4.5.4.5.3 Creating an RFC Destination to Use for the LDAP Connector

Context

Procedure

1. Using destination maintenance (transaction `SM59`), create an RFC destination with the following properties:
   - *Type*: T (TCP/IP Connection)
   - *Name*: <Destination_Name> (for example, LDAP_VD)
   - *Activation Type*: Registered server program
   - *Program ID*: <Program_ID> (for example, LDAP_VD)

     > **Tip**
     >
     > For easier reference in traces and logs, use the RFC destination name for the program ID.

   - *Gateway host*: <Gateway_host> (host where the system's gateway runs)
   - *Gateway service*: <Gateway_service> (name of the gateway service, for example sapgw<sys_nr>)

     > **Tip**
     >
     > To find out gateway service and gateway host:
     > 1. Call transaction `SMGW`.
     > 2. Choose *Goto* > *Parameters* > *Display*.

   - *MDMP & Unicode* tab page under *Communication Type with Target System:* Select the *Non-Unicode* or *Unicode* radio button according to whether you extract Unicode data or not.
2. Save the data.

> **Note**
>
> The *Connection Test* will only work if the LDAP connector is configured. See section *Configuring the Parameters to Use for the Connection to the VDS*.
>
> If you receive the error message `ERROR: program LDAP_VD not registered`, the LDAP Connector is not started. To start it, open transaction `ldap` and then *LDAP Connectors* > *LDAP_VD* and choose *Start connector* button.

4.5.4.5.4 Configuring the Parameters to Use for the Connection to the VDS

Context

Procedure

1. Using directory service connection maintenance (transaction `LDAP`), set up the LDAP connector.

   > **Note**
   >
   > Make sure to start the LDAP connector by choosing *Start connector* button. It also makes sense to set the *Status* to *Connector is Active* so the connector starts automatically if it goes down.

2. Set up a service user to use for the connection. Choose *System Users*, switch to edit mode, and choose *New Entries*.
3. Enter the properties for the system user.
4. Create an entry for the LDAP server.

4.5.4.5.4.1 Setting Up the LDAP Connector

Context

Procedure

1. Choose *LDAP Connectors*.
2. On the *LDAP Connector (Maintenance View)* screen that appears, choose *Display/Change* to switch to edit mode.
3. Choose *New Entries*.
4. Enter the name of the RFC destination you created in the last step (for example, **`LDAP_VD`**).
5. Maintain the LDAP connector settings as necessary.

   > **Tip**
   >
   > The application server name is the name of the server as specified in the `rdisp/myname` profile parameter. You can also check for the name to use using transaction `SM51`

6. Save the data.
7. To activate the connector, choose the *Start Connector* pushbutton.
8. Return to the main screen for the directory service connection maintenance.

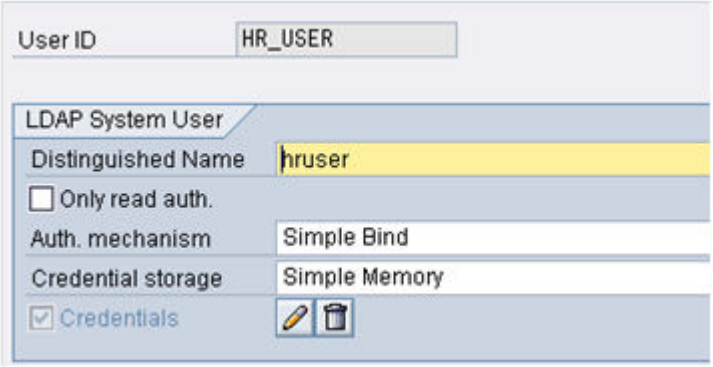
4.5.4.5.4.2 Entering the User's Properties

Context

Procedure

1. For the *Distinguished Name*, use the user ID that you specified for the VDS in *Configuring the Virtual Directory Server*, step 4.
   - *User ID*: <User_ID> (for example, HR_USER)
   - *Distinguished Name*: <Directory_Server_User> (for example, hruser)
   - *Auth. mechanism*: Simple Bind
   - *Credential storage*: Simple Memory
2. For the *Credentials*, choose the symbol for *Change* to enter the directory server user's password. (This password must also match the password specified for the directory server user in step 4 referenced above.)

   See the figure below.



3. Save the data and return to the main screen for directory service connection maintenance.

Related Information

Configuring the Virtual Directory Server [page 56]

4.5.4.5.4.3 Creating an Entry for the LDAP Server

Context

Procedure

1. Choose *LDAP Servers*.
2. Choose *Display/Change* to change to edit mode.
3. Choose *New Entries*.
4. Enter the properties for the VDS as follows:
   - *Host name*: <VDS_Host>
   - *Port number*: <LDAP_Port> (for example, 1389)
   - *Product name*: <blank>
   - *Protocol version*: LDAP version 3
   - *LDAP Application*: Employee
   - *Default*: Inactive (unless the VDS should be the default LDAP server)
   - *Base entry*: (for example, o=idstore)
     The path is defined in the virtual tree of the virtual directory server.

- *System Logon*: <User_ID> (Use the user ID you specified in the last step, for example, HR_USER.)
- *Read Anonymously*: Inactive

5. Save the data and return to the main screen for directory service connection maintenance.

4.5.4.5.5 Maintain the Attribute Mappings

Context

Procedure

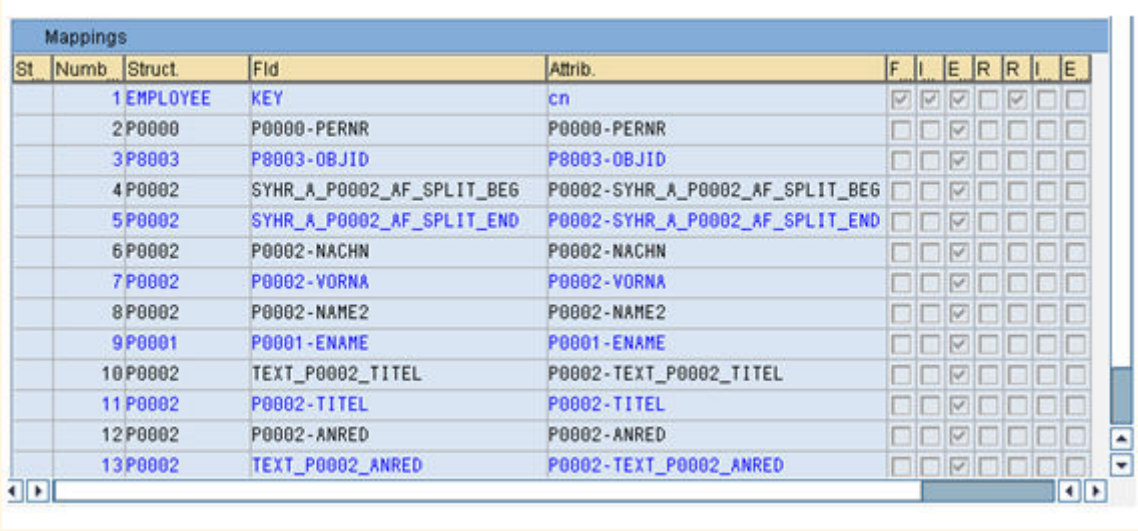
1. Using directory service connection maintenance (transaction `LDAP`), choose *LDAP Servers*.
2. Select the LDAP server to maintain (for example, **`LDAP_VD`**) so that the row is marked.

3. If you are not in edit mode, then switch to edit mode.
4. In the left frame, select *Mapping* with a double-click.
5. In the *Mapping Overview* screen that appears, enter **`sapIdentity`** in the *ObjectClasses* list.
6. Maintain the mappings between the fields used by the LDAP synchronization and the VDS.

> **Note**
>
> The mappings are available on the installation CD (or in the installation package) in the subfolder `Designtime Components\Misc`, in the `HCM Ldap Mapping.xml` file. You can upload the mappings using the XML Import function.
>
> To maintain the mappings manually, see *Maintaining Mappings Manually*.

7. Go back and save the data.

> **Example**
>
> For an example of the LDAP attribute mappings, see the figure below.



Related Information

Maintaining Mappings Manually [page 69]

4.5.4.5.5.1 Maintaining Mappings Manually

Context

Procedure

1. Using directory service connection maintenance (transaction LDAP), choose *LDAP Servers*.
2. Select the LDAP server to maintain (for example, LDAP_VD) so that the row is marked.

3. If you are not in edit mode, then switch to edit mode.

4. In the left frame, select *Mapping* with a double-click.
5. In the *Mapping Overview* screen that appears, enter **`sapIdentity`** in the *ObjectClasses* list.
6. Create an entry that maps the structure EMPLOYEE, field KEY, to the attribute cn. To create a new entry, choose *Edit* > *Add New Mapping*.
7. Specify the rest of the entries to map the fields used by the HR LDAP query to identically-named attributes.

> **Caution**
>
> The entries for *Structure* and *Field* must be identical to the *Attribute Grp* and *Attrib.Name* entries you created for the query mapping in *Specifying the Attribute Mapping Between the HR Fields and LDAP Synchronization*.

Mapping Data

Structure	Field	Attribute	Flags to Set
EMPLOYEE	KEY	cn	Filter Import Mapping Export Mapping RDN Mapping
P0000	P0000-PERNR	P0000-PERNR	Export Mapping
P8003	P8003-OBJID	P8003-OBJID	Export Mapping
P0002	SYHR_A_P0002_AF_SPLIT_BEG	SYHR_A_P0002_AF_SPLIT_BEG	Export Mapping
P0002	SYHR_A_P0002_AF_SPLIT_END	SYHR_A_P0002_AF_SPLIT_END	Export Mapping
P0002	P0002-NACHN	P0002-NACHN	Export Mapping
P0002	P0002-VORNA	P0002-VORNA	Export Mapping
P0002	P0002-NAME2	P0002-NAME2	Export Mapping
P0001	P0001-ENAME	P0001-ENAME	Export Mapping
P0002	TEXT_P0002_TITLE	TEXT_P0002_TITLE	Export Mapping
P0002	P0002-TITEL	P0002-TITEL	Export Mapping
P0002	P0002-ANRED	P0002-ANRED	Export Mapping
P0002	TEXT_P0002_ANRED	TEXT_P0002_ANRED	Export Mapping

8. Go back and save the data.

Related Information

Specifying the Attribute Mapping Between the HR Fields and LDAP Synchronization [page 62]

4.5.4.5.6 Exporting the Data

Context

To export the data, execute the `RPLDAP_EXTRACT_IDM` report. This report writes the HR data to the LDAP directory server, in this case, the VDS.

> **Note**
>
> The `HRLDAP_EXTRACT` report implements the RPAD00INFTY and HRPAD00INFTYDB BAdIs. Its implementation of the UPDATE method only marks the infotypes 0000, 0001, 0002, and 0105 as relevant for the LDAP extraction.
>
> If you want to include other infotypes in the UPDATE method of the BAdI, create your own implementation of the UPDATE method for the infotype you want to extract.
>
> For more information, see the documentation of `RPLDAP_EXTRACT_IDM` report (using, for example, transaction `SE38`).

Procedure

1. Using the ABAP editor (transaction `SA38`), enter **`RPLDAP_EXTRACT_IDM`** as the program and choose *Execute*.
2. Enter the criteria to use for the report. Note the following for the corresponding fields.
   - *RFC Connection*: <blank>
     The system searches for an active connector.
   - *LDAP Server*: <LDAP_Server> (for example, LDAP_VD)
   - Data source: Enter the data that corresponds to the query you defined in *Creating the Query to Use for the Export*.

     > **Note**
     >
     > For example:
     >
     > - *Global Work Area*: Activate
     > - *User Group*: /SAPQUERY/L1
     > - *Name*: <Query_Name>, for example, LDAP_QUERY

- *Variant*: <blank>
  If the standard variant does not exist for your query and you have created a different variant as described in section *Creating the Query to Use for the Export*, add the name of that variant to the execution task of `RPLDAP_EXTRACT_IDM` report.

- *Options*: Delete Person in Directory with Employment Status 3
  Activate this option if you want to delete user master records for users who have left the company.

  > **Note**
  >
  > The users are then deleted in the Identity Center's identity store, but not in the SAP HCM system.

3. Execute the report.

> **Note**
>
> If the extract fails in the LDAP Connector Trace, you can see something like this:
>
> ```
> [Wed Apr 18 16:27:49 2012]
> Slot 0 (IDM_PETER): >>> ldap_initU(host="10.66.185.62", port=389)
> Slot 0 (IDM_PETER): <<< ldap_initU() == <NOT NULL> := connected
> Slot 0 (IDM_PETER): >>> ldap_set_option(version=3)
> Slot 0 (IDM_PETER): <<< ldap_set_option() == 0
> Slot 0 (IDM_PETER): >>> ldap_simple_bind_sU(dn="hruser", password: not initial)
> [Wed Apr 18 16:28:10 2012]
> Slot 0 (IDM_PETER): <<< ldap_simple_bind_sU() == 81 := failed
> ```
>
> Use antoher port, e.g. 1389 on the ldap server VDS_HOST and also on the VDS, and try again.

Related Information

Creating the Query to Use for the Export [page 60]

4.5.4.5.6.1 Scheduling the Job to Run Periodically

Context

To regularly export identity data, create a variant and schedule a job that runs using this variant. Proceed as follows:

Procedure

1. To create a variant, enter the data for the report and save it instead of executing it. When saving it, enter a name for the variant and a short description.
2. Using job maintenance (transaction `SM36`), create a job that executes the `RPLDAP_EXTRACT_IDM` report. Configure the frequency of the job execution under *Start condition* and configure the report and variant names under *Step*.

Results

After configuring the LDAP connection to the VDS and executing this report, the identity data is extracted from the SAP HCM system and written to the VDS and the staging area in the Identity Center.

In VDS, the identities are assigned to the MX_HCM_EMPLOYEE entry type. This allows the Identity Center to recognize events for the entry type and to trigger the corresponding tasks when the entry type is changed.

4.5.4.5.6.2 Troubleshooting the Data Export

You can troubleshoot problems with the export from the SAP HCM system with the following tools:

- View the log produced for the export from the SAP HCM system using `SPLDAP_DISPLAY_LOG_TABLES` report.
- View traces for the LDAP Connector using `RSLDAPTRACE` report.
- Check connections using `RSBDCOS0` report.
- Show the result using transaction `LDAP`.

4.5.5 Setting up an SAP Business Suite System

Prerequisites

- The Virtual Directory Server is installed.
- The Identity Center is installed and configured.
- The SAP Identity Management user interface is deployed on the AS Java.
- The SAP Business Suite system release 7.02 or higher is installed, including any of the applications that support this integration scenario, and the relevant application contains business partner data that is supported for this scenario.

Context

Various SAP Business Suite applications, for example, SAP SRM or SAP CRM, can send identity information to SAP Identity Management using the SPML protocol. In this scenario, the SAP Business Suite system sends the SPML request to a Business Suite Connector service deployed on an AS Java, which is used as the common interface for receiving the data. The identity data of the SAP Business Suite system is then forwarded into a staging area in the Identity Center before being applied to the productive identity store. Once the data is in the productive identity store, it can be provisioned to other connected systems, for example, another LDAP directory server.

Using a staging area instead of writing directly to the identity store has the following advantages:

- You can work with the data in the staging area before processing it further. For example, you can also set up workflow approval tasks to access the data in the staging area before writing it to the productive identity store.
- If you make changes to the data schema or the format used for identity data in the SAP Business Suite system, you can adjust the attribute mapping in the staging area accordingly. You do not have to change the schema of the productive identity store.
- > **Note**
>
> We provide a template to use for setting up the staging area in the Identity Center.

To set up an SAP Business Suite system for this scenario, proceed as described below.

Procedure

1. Import the staging area template.
2. Configure the Virtual Directory Server, generate, deploy, and configure the Business Suite Connector service on the AS Java.
3. To secure the connection between the SAP Business Suite system and the AS Java, configure the use of SSL on the AS Java.

4. Configure the SAP Business Suite system.

4.5.5.1 Importing the Staging Area Template

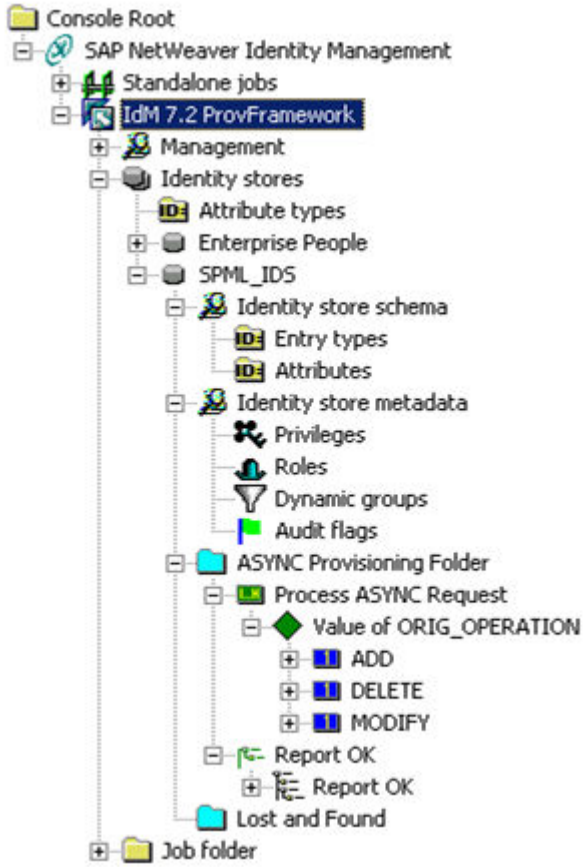
Context

In this step, you import the template that contains the staging area identity store to use for the SAP Business Suite system, as well as the corresponding tasks for writing the identity data from the staging area to the productive identity store.

Procedure

1. In the Identity Center, navigate to the staging area identity store.
2. In the Identity Center, choose *Import...* from the context menu for the Identity stores.
3. Select the `SPML_IDS_Identity store.mcc` file from the file system and choose *Open*. You can find it in the folder `<Install_folder>\Templates\Identity Center\SAP Provisioning framework`.

   The staging area identity store and corresponding provisioning tasks are imported into the Identity Center. See the figure below.



4. On the *General* tab of the new identity store, set the *Automatically create attributes* flag. Also note the numeric ID for the SPML staging area identity store, which you can find on the same tab in the *ID/Name* field. Store the ID in the SAP_SPML_STAGING_AREA global constant under ▶ *<Identity Center>* ▶ *Management* ▶ *Global constants* ◀. By default the value is set to 2. In case you already have other identity stores, you need to change this value to the actual number. You need this value again when configuring the Virtual Directory Server.

4.5.5.2 Configuring the Virtual Directory Server

Prerequisites

- You have maintained the database connection for the identity store in Identity Center and know the password for the database user.
- The JDBC driver to use to access the Identity Center database is maintained in the class path for the Virtual Directory Server. (Maintain the driver under ▶ *Tools* ▶ *Options* ▶ *Classpath* ◀.) The *Java compiler* flags are set under ▶ *Tools* ▶ *Options* ▶ *General* ◀ (*Enable compilation* and *Use specified compiler*).
- You have imported the staging area identity store of the SAP Business Suite system into the Identity Center.

Context

In this section, we describe how to configure the Virtual Directory Server (VDS) to create an AS Java application. This application is then deployed on the AS Java. With this deployed application the data is exported from the SAP Business Suite system to the SPML staging area.

Procedure

1. Start the Virtual Directory Server console.
2. To maintain the configuration, choose *File* > *New*.
3. On the *New configuration* dialog that appears, select the *Group SAP NetWeaver 7.2* and the *Template BUSINESS SUITE CONNECTOR Service* and choose *OK*.
4. Enter the following data in the wizard.

Wizard Data

Field	Value	Example	Comment
User	<new user for Business Suite SPML client>		
Password	<New password>		
Identity Center URL	<value concatenated using JDBC URL WizardN>	jdbc:sqlserver://loc alhost:1433;database name=mxmc_db;user=mxmc_rt;password={DES3 CBC}1:667071db1465cbacc9c0e77f083df8a77fa53828c541c71d;	This ID was determined when setting up the staging area identity store. 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	<Staging_Area_ Identity_Store _ID>		This ID was determined when setting up the staging area identity store.

Wizard Data

Field	Value	Example	Comment
Server	<Server_Name>	localhost	

Field	Value	Example	Comment
Port	<Port>	MSSQL: 1433 Oracle Thin Driver: 1521 DB2: 50000	
Database	<Database_ Identifier>	mxmc_db	
User	<Database_ User>	mxmc_rt	Runtime user
Password	<Database_ User_Password>	<password>	You specified the password for the runtime user during the installation of the Identity Center database.
SID	<Service_Name>		Field only relevant for Oracle.
Schema	<Prefix_oper>	mxdb2_oper	Field only relevant for DB2.
FunctionPath	<Prefix_oper>	mxdb2_oper	Field only relevant for DB2.

5. Enter a name for the new configuration, for example, **`BSConnector`**.
6. Save the configuration.
7. Compile the `attrClass extension` class.
   a. In the Virtual Directory Server tree, open *Extension classes* > *Attributes* and double-click *attrClass*.
   b. In the pane that opens, choose *Compile*.
8. To check for errors, start the server. If the VDS console displays that the server started all right, stop the server.
9. Deploy the configuration.

4.5.5.2.1 Deploying the Configuration

Context

Procedure

1. Include the necessary JDBC drivers in the ear file.
2. Configure the deployment.

3. Deploy the configuration on the AS Java.

   See the documentation relevant to your version of AS Java.
4. Execute post-deployment tasks on the AS Java.

Related Information

SAP NetWeaver AS for Java as of Release 7.0, section Deployment with the SAP Software Deployment Manager

4.5.5.2.1.1 Including Necessary JDBC Drivers in Ear File

Context

Procedure

1. To view the JAR files defined for your configuration, choose *Tools/Options...* and select the *Classpath* tab.
2. Create a folder named `lib` in the configuration's workspace (for example, `C:\usr\sap\IdM\Virtual Directory Server\configurations\IdServ72`).
3. Copy the defined JAR files from the specified directories to the `lib` folder.

4.5.5.2.1.2 Configuring the Deployment

Context

Procedure

1. To view the properties of the connector web service deployment, choose *Deployments\Web service deployments\Identity Service* in the console tree and then choose *Properties...* from the context menu. Make sure that *NetWeaver* is selected in the *Server* field.

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. Choose *OK* to close the dialog box that confirms the creation of the EAR file.

4.5.5.2.1.3 Deploying the Configuration on EHP 1 for SAP NetWeaver CE 7.1/ SAP NetWeaver CE 7.2/ SAP NetWeaver 7.3

Context

To update the configuration on versions EHP 1 for SAP NetWeaver CE 7.1, SAP CE 7.2 and SAP NetWeaver 7.3, do the following:

Procedure

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 (SAP NetWeaver Packaging Tool), which can be used to create an SCA file from an EAR file.
2. Use the Java Support Package Manager (JSPM) to update with the new configuration (the generated SCA file) on the SAP NetWeaver. See the documentation relevant for your release.
   - EHP 1 for SAP NetWeaver CE 7.1
   - SAP NetWeaver CE 7.2
   - SAP NetWeaver 7.3
   - SAP NetWeaver 7.3 EHP1

Related Information

SAP Note 1223957: Usage of SAP NetWeaver Packaging Tool
EHP 1 for SAP NetWeaver CE 7.1
SAP NetWeaver CE 7.2
SAP NetWeaver 7.3 Ehp1
SAP NetWeaver 7.3

4.5.5.2.1.4 Executing Post-Deployment Tasks on AS Java Release 7.0

Context

Procedure

1. In Visual Administrator, specify the path to the `keys.ini` file.
2. In the *Cluster* tree, open *Server* > *Services* > *Configuration Adapter*.
3. On the *Display configuration* tab, switch to *Edit* mode and open *apps* > *sap.com* > *vds-ids* > *appcfg* > *Propertysheet application.global.properties*.
4. To change the configuration, double-click *Propertysheet application.global.properties*.
5. To enter the keys.ini file path, double-click *com.sap.idm.vds.keyfile*.
6. Enter the path in the *Custom* field.
7. The Identity Center installation generates the `keys.ini` file. On the AS Java you need access to this file. If the AS Java does not run on the same host, you have to copy the keys.ini file to the machine running the AS Java. Indicate the path to `keys.ini` as appropriate, for example, `C:\usr\sap\IdM\Identity Center\Key\Keys.ini`.
8. Choose *Apply custom*.
9. Choose *OK*.
10. Restart the vds-ids application as described in *How to Restart an Application*.

Related Information

How to Restart an Application

4.5.5.2.1.5 Executing Post-Deployement Tasks on EHP 1 for SAP NetWeaver CE 7.1/ SAP NetWeaver CE 7.2/ SAP NetWeaver 7.3

Context

Procedure

1. In the SAP NetWeaver Administrator, specify the path to the `keys.ini` file.
2. Choose *Configuration Management* > *Infrastructure* > *Java System Properties*.
3. On the *Application* tab, select your vds-ids application.
4. Select the *com.sap.idm.vds.keyfile* property and switch to *Change* mode.
5. Enter the path to the keys.ini file.
6. Save your data.
7. To restart the application vds-ids, choose *Operation Management* > *Systems* > *Start&Stop* in SAP NetWeaver Administrator.
8. Choose *Java EE Applications* and select the vds-ids application.
9. Stop the application and restart it.

4.5.5.3 Configuring a Secure Connection for SAP NetWeaver AS Java

You need to configure the secure connection with regard to your version of AS Java. See the following sections.

4.5.5.3.1 Configure a Secure Connection for SAP NetWeaver AS Java as of Release 7.0

Context

Procedure

1. Set up SSL on the AS Java.

   For more information, see *Configuring the Use of SSL on the J2EE Engine* in the SAP Library.
2. Export the SSL certificate of the AS Java to the file system.

   For more information, see *Managing Entries* in the SAP Library.
3. Import the SSL certificate of the AS Java into the AS ABAP.

   For more information, see *Maintaining PSEs and Managing Certificates* in the SAP Library.
4. Specify the SSL certificate of the AS Java when creating the RFC destination on the AS ABAP.

   See section *Creating an RFC Destination*.

Related Information

Configuring the Use of SSL on the J2EE Engine
Managing Entries
Maintaining PSEs and Managing Certificates
Creating an RFC Destination [page 84]

4.5.5.3.2 Configure a Secure Connection for AS Java as of EHP 1 for SAP NetWeaver CE 7.1/ SAP NetWeaver CE 7.2/ SAP NetWeaver 7.3

Context

Procedure

1. Set up SSL on the AS Java.
2. Export the SSL certificate of the AS Java to the file system.

   For more information, see *Configuring the Use of SSL* and *Managing Entries* on the AS Java in the SAP Library relevant for your release on the Help Portal.
3. Import the SSL certificate of the AS Java into the AS ABAP.

   For more information, see *Maintaining PSEs and Managing Certificates* in the SAP Library.

4. Specify the SSL certificate of the AS Java when creating the RFC destination on the AS ABAP.

   See section *Creating an RFC Destination*.

Related Information

SAP Library on the Help Portal
Creating an RFC Destination [page 84]

4.5.5.4 Configuring the SAP Business Suite System

Context

To configure the SAP Business Suite system to export data to the Virtual Directory Server, you must:

Procedure

1. Create an RFC destination to use for the connection to the VDS.
2. Define a corresponding inbound destination.
3. Change the SAP Identity Management SPML configuration.
4. Monitor and manage queue entries.

4.5.5.4.1 Creating an RFC Destination

Context

Procedure

1. Using destination maintenance (transaction `SM59`), create an HTTP connection to an external server. Create an RFC destination with the following properties.

Technical Settings

- *RFC Destination*: `<Destination_Name>` (for example, SPML_TO_IDM_STAGING)
- *Type*: G (HTTP Connection to external server)
- *Description 1*: Enter a description for your destination.
- *Target Host*: `<host_of_the_AS_Java>`.
- *Service No.*: `<number_of_the_AS_Java>`
- *Path Prefix*: /ids/router

Global Configuration

- Set the *Proxy Setting is Active* and *No Proxy Setting for Local Server* flags

Logon & Security

Enter the data for the basic authentication mechanism.

- User: `<User you defined for the VDS configuration.>`
- Password: `<Password you defined for the VDS configuration.>`
- If you configured SSL on the AS Java, set the *Active* flag for SSL and indicate the SSL certificate the AS Java uses, and which you uploaded to the AS ABAP using the Trust Manager.

2. Save the data.

4.5.5.4.2 Defining an Inbound Queue

Context

Using bgRFC configuration (transaction `SBGRFCCONF`), create an inbound queue.

Procedure

1. On the *Define Inbound Dest. Tab*, create an inbound destination with the following properties:
   - *Inb. Dest. Name*: Enter a name, for example, SPML_INBOUND_QUEUE.
   - *Add Queue Prefix*: SPML_IDM
2. Save the data.

Related Information

SAP Library for your release, section "bgRFC Configuration"

4.5.5.4.3 Changing the Identity Management SPML Configuration

Context

Using table maintenance (transaction `SM30`), insert the entries into `IDM_INTEG_CUST` table:

Procedure

1. Choose *New Entries*.
   - *bgRFC for IDM*: `<name of the inbound destination>`, for example, SPML_INBOUND_QUEUE
   - *RFC to Staging Area*: `<name of the staging area RFC destination>`
2. Set the *IDM Integrat. Status* flag.

4.5.5.4.4 Monitoring and Managing Queue Entries

Context

Procedure

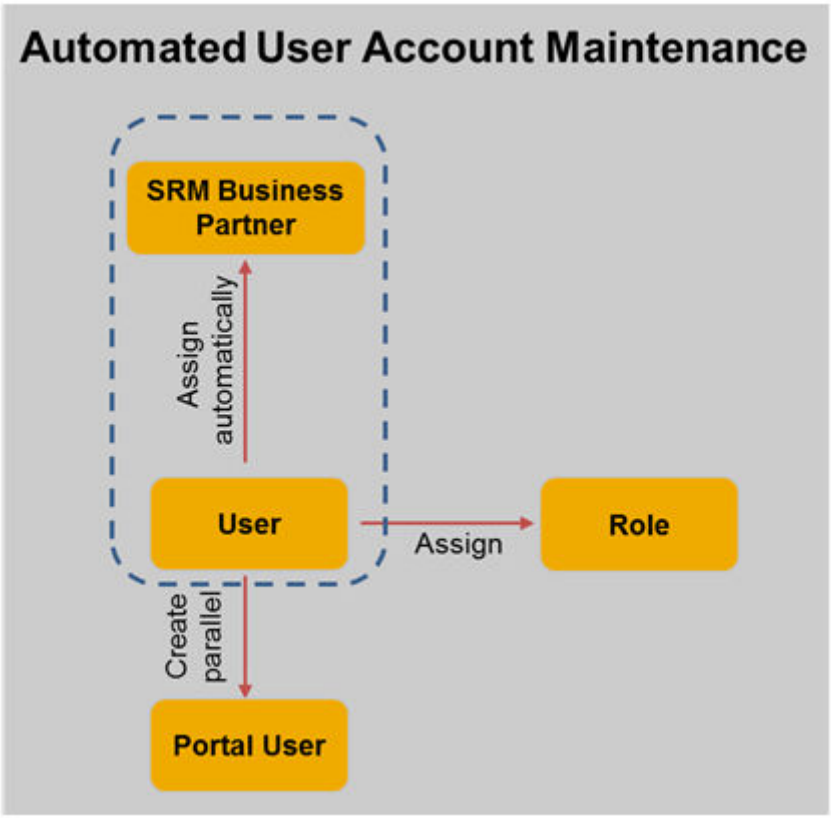
Using the bgRFC monitor, search for the inbound queue you created. For more information, see *bgRFC: Administration* in SAP Library for your release.

Related Information

SAP Library

4.5.5.4.5 Setting Up Business Role Provisioning

This section describes how to set up automated user account maintenance for SAP Business Suite Applications using SAP SRM 2007 as sample system. You configure the SPML staging area using the management console in the Identity Center to automatically create a business partner and assign business roles when creating the user account. In SAP SRM 2007 each user account also needs a portal user with corresponding portal roles.



4.5.5.4.5.1 How the SPML Staging Area Works

SPML Requests are sent to the Business Suite Connector service, which is deployed on an AS Java. This service extracts the attributes of the SPML request and writes them into the SPML staging area identity store of the identity management database as an MX_ASYNC_REQUEST entry.

Once a new entry arrives in the staging area, one of the tasks *On Async Add*, *On Async Modify*, or *On Async Delete* (depending on the value of the MX_ASYNC_ORIG_OPERATION attribute of the entry) processes the new entry including its attributes. Each incoming MX_ASYNC_REQUEST entry then adds, modifies, or deletes a corresponding business user (that is an MX_PERSON entry) in the productive identity store.

The *On Async Add* and *On Async Modify* tasks both contain an entry script, which is called to prepare each entry for task processing. These entry scripts call the `custom_DetermineRole` global script, which allows you to specify the business roles a user will be assigned or unassigned, depending on his or her attributes. The *On Async Delete* task is not relevant for business role assignments because it deletes business users.

The `custom_DetermineRole` global script is delivered with the following content:

```
// Main function: custom_determineRole
function custom_determineRole(HashMap){
      //Example calling application specific assignment of roles
   //This script is called from entry scripts 'sap_insertNewEntry'
   //and 'sapModifyEntry'. The code below is a sample and returns an
//empty string for attribute MXREF_MX_ROLE.
//Please replace it according to your needs.
//UserFunc.uWarning("custom_determineRole enter: " + HashMap);
// Import required Java types.
importClass(java.util.HashMap);
var mxref_mx_role = "MXREF_MX_ROLE";
//HashMap = UserFunc.custom_determineRoleSRM(HashMap);
//HashMap = UserFunc.custom_determineRoleCRM(HashMap);
//HashMap = UserFunc.custom_determineRoleSCM(HashMap);
//HashMap = UserFunc.custom_determineRoleSLcM(HashMap);
//UserFunc.uWarning("custom_determineRole returns mxref_mx_role value
//: " + HashMap.get(mxref_mx_role) );
return HashMap;
}
```

Using this method you compile the value of the MXREF_MX_ROLE multivalue attribute. By default, the method does not deliver a value for this attribute. Therefore, no business role is assigned to the MX_PERSON entry that corresponds to the incoming MX_ASYNC_REQUEST entry.

Specific examples for several Business Suite scenarios are available, for each of which a custom script exists:

- `custom_determineRoleSRM`
- `custom_determineRoleCRM`
- `custom_determineRoleSCM`
- `custom_determineRoleSLcM`

To view these scripts, choose *Console Root* > *SAP NetWeaver Identity Management* > *<IC_Configuration_for_SAP_Systems>* > *<identity_store>* > *<identity_store>* > *Management* > *Global scripts* > *Jscript* in your Identity Center management console.

The script parameter for each of these scripts is a hashmap containing all attributes of an incoming MX_ASYNC_REQUEST entry. These attributes help you decide, which business roles to add or to delete from the corresponding MX_PERSON entry. For example, you could automatically assign some basic country-specific role here if the user mentioned in the MX_ASYNC_REQUEST is located in the respective country.

A business role assignment is specified by the MSKEYVALUE of the business role, for example, `BUSINESSROLE_1`. Using the `{A}` or `{d}` operator, respectively, you can specify whether you want to add or remove the role from the corresponding user.

You can also add a validity interval to a role assignment to indicate when the role becomes valid and when the role will be removed from the user again. An example for a validity period is [20111108-20121108] with the yyyyMMdd format.

Since MXREF_MX_ROLE is a multivalue attribute, you can assign more than one role. Multiple assignments are separated by a pipe (|) character.

Sample Value:

```
{A}<BUSINESSROLE_1>|[20111108-20121108]
{A}<BUSINESSROLE_2>|{d}BUSINESSROLE_3
```

This sample value has the following effects:

- You add the `BUSINESSROLE_1` role with a validity from 20111108-20121108.
- You add the `BUSINESSROLE_2` role immediately for an unlimited time.
- You delete the `BUSINESSROLE_3` role.

4.5.6 Setting up an SAP HANA System

This document helps you understand the main functionality of the SAP HANA Connector and explains how to configure your Identity Management and SAP HANA systems so that the connector works properly.

Overview

SAP HANA Connector for SAP NetWeaver (NW) Identity Management (IDM) is used for communication between IDM and SAP HANA systems. To configure the SAP HANA Connector, you have to use the *toHANA* pass type. It supports the following operations:

- Provisioning and de-provisioning of users with attributes.
- Assigning roles to users or removing roles from users.
- Assigning system or application privileges to users or removing privileges from users.

In addition, SAP HANA Connector supports the modification of user mappings related to multiple SAML providers. You can see the list of all defined SAML providers in the Identity Management User Interface. In the *Change Identity task* > *Account attributes* > *SAML Mapping* section you can select a provider to form a mapping to an external identity (unique user ID for HANA system).

Prerequisites

You have a technical user on the SAP HANA system with the required permissions to create new technical users on the system.

> **Remember**
>
> The technical user must not be deleted, because all assignments made using it would also be deleted. For more information about creating users on an SAP HANA system, see the SAP HANA Security Guide on the SAP HANA Platform page.

Before you start the setup process, familiarize with the limitations and the additional prerequisites for the SAP HANA Connector.

For more information about securing the SAP HANA connection, see *SAP HANA Network and Communication Security* > *Securing Data Communication* > *Configuring SSL for ODBC/JDBC Client Access* of the *SAP HANA Security Guide*.

Supported Roles

As of SAP NetWeaver IDM 7.20 Support Package Stack (SPS) 9, the SAP HANA Connector, working with the SAP HANA Platform SPS 4 and higher, supports more than the runtime roles.

Supported Operations According to SPS of SAP NetWeaver IDM and SAP HANA Platform

	IDM 7.20 SPS 8	IDM 7.20 SPS 9 or higher
SAP HANA Platform SPS 4	Catalog roles	Catalog roles System privileges Application privileges
SAP HANA Platform SPS 5	Catalog roles	Repository roles Catalog roles System privileges Application privileges SAML
SAP HANA Platform SPS 6	Catalog roles	Repository roles Catalog roles System privileges Application privileges SAML Validity X.509
SAP HANA Platform SPS 7	Catalog roles	Repository roles Catalog roles System privileges Application privileges SAML Validity X.509 SAP Logon Ticket SAP Assertion Ticket

For more information about SAP HANA database roles and the difference between Catalog roles and Repository roles, see Roles and Catalog Roles and Repository Roles Compared.

Privileges

Since multiple assignments of privileges are not supported in the SAP HANA system, by default no grouping is set for the assignment grouping of privileges in the Identity Center. For this reason, as of SAP NetWeaver IDM SPS 9, grouping is disabled in existing SAP HANA repositories.

As of SAP NetWeaver IDM SPS 9, the system supports the following new privilege types:

- SYSTEMPRIVILEGE
  The new entry for the Identity Center looks like this: `<PRIV:SYSTEMPRIVILEGE:<repository>:<HANA privilege>`.
- APPLICATIONPRIVILEGE
  The new entry for the Identity Center looks like this: `<PRIV:APPLICATIONPRIVILEGE:<repository>:<HANA privilege>`.

Authentication Methods

The SAP HANA Connector supports the provisioning of the following authentication methods:

- Basic
- Kerberos
- SAML
- X.509
- SAP Logon Ticket
- SAP Assertion Ticket

On the user interface, these methods can be set or modified for any users, as long as the methods are also defined in the SAP HANA system.

> **Note**
>
> When you use the Basic authentication method, *Enable password provisioning* on the *Password policy* tab of the identity store must be selected.

User Attributes

Attribute Mappings

HANA Attribute	IDM Attribute	Mapping Format	Description
USER_NAME	ACCOUNT<Repository>/ MSKEYVALUE	String	For SAP HANA systems, the default value provisioned as USER_NAME is the Account<Repository> / MSKEYVALUE of the entry. However, due to limitations of permitted characters in In-Memory database user names, you might want to implement your custom logic to generate a user name for your In-Memory Database users here. This customizations should be implemented in the script sap_hana_generateUsername.
EXTERNAL_IDENTITY	MX_KERBEROS_IDENTITY	String	This attribute contains Kerberos identity and is used for Kerberos authentication.
VALID_FROM	MX_VALIDFROM	Date or Date and Time	This attribute shows the start date of user's validity.
VALID_UNTIL	MX_VALIDTO	Date or Date and Time	This attribute shows the end date of user's validity.
USER_DEACTIVATED	MX_DISABLED	Boolean	The attribute is true if the user is disabled.
IS_PASSWORD_ENABLED	MX_PASSWORD_DISABLED	Boolean	This attribute is true when basic authentication is disabled.
IS_KERBEROS_ENABLED	MX_KERBEROS_ENABLED	Boolean	This attribute is true when Kerberos authentication is enabled.
IS_SAML_ENABLED	MX_SAML_ENABLED	Boolean	This attribute is true when SAML authentication is enabled.
IS_X509_ENABLED	MX_X509_ENABLED	Boolean	This attribute is true when X509 authentication is enabled.
IS_SAP_LOGON_TICKET_ENABLED	MX_LOGON_TICKET_ENABLED	Boolean	This attribute is true when SAP logon ticket authentication is enabled.

HANA Attribute	IDM Attribute	Mapping Format	Description
IS_SAP_ASSERTION_TICKET_ENABLED	MX_ASSERTION_TICKET_ENABLED	Boolean	This attribute is true when authentication with SAP assertion ticket is enabled.
USER PARAMETERS	MX_USER_PARAMS	Multi-Value String	Except for e-mail address, locale, and timezone user parameters, the mapping for the general purpose user parameters follows the pattern `<parameter name>==<value>`. It replicates what the user has to enter in the SAP HANA system. **Example** `CONTRACT_ID==89312642`

HANA Attribute	IDM Attribute	Mapping Format	Description
SAML USER MAPPING	MX_SAML_MAPPING	SAML mapping	The expected format for SAML mapping attribute is configured in the Identity Management User Interface. In the *Change Identity task* > *Account attributes* > *SAML Mapping* section you need to select <provider name> and its mapping <external identity>. If the desired mapping is to use the user from the target system, use the string <ANY>" for an external identity. **Example** The following creates a mapping to username *John* in the Identity Management User Interface. It is displayed in a two-column table. The first column displays the provider name: AC_SAML_PROVIDER and the second column displays the external identity: John The following creates a mapping with the user from the SAP HANA Platform: Provider Name: CORP_SAML External Identity: <ANY>

HANA Attribute	IDM Attribute	Mapping Format	Description
X509 USER MAPPING	MX_X509_MAPPING	Multi-Value String	The expected format for X509 mapping attribute is `<subject DN>==<issuer DN>`. It replicates what the user has to enter in the SAP HANA system. **Example** `C=US, ST=California, L=San Francisco, O=Comapny A, OU=Unit A,CN=www.unita.org/ emailAddress=companya@unita.org==C=US,ST=Illinois, L=Chicago, O=Company B, OU=Certification Services Division, CN=Company B Server CA/ emailAddress=server-certs@companyb.com`

On the user interface, these user attributes can be defined or modified for any users.

Related Information

Restrictions for SAP HANA Connectors [page 15]
Additional Prerequisites for SAP HANA Connector [page 16]
Repository Constants for SAP HANA Database [page 145]

4.5.7 Creating and Configuring the Jobs for Each Connector

Prerequisites

- A repository entry exists for each of the systems used in the landscape.
- The Identity Center is installed and configured.
- The leading system contains the identity data.
- If a corporate LDAP directory server is used as the leading system, then the communication user used for the connection between the Identity Center and the LDAP directory server should have read-only access for the LDAP directory server. If the LDAP directory server is a target system that receives provisioned data, then the communication user must have write permissions.
- If you want to provision user/role assignments to a portal that uses an LDAP directory server as its data source, then the users must exist in the LDAP directory before the assignments can be provisioned. In this case, make sure the users exist in the directory by creating them and assigning them to the appropriate LDAP groups before any provisioning tasks or jobs run.

Context

In this step, you create and configure the jobs for each connector used in the system landscape.

Procedure

1. In the Identity Center, create a job folder in your structure to use for the provisioning jobs, for example, ▶ *SAP NetWeaver Identity Management* ▶ *<IC_Configuration_for_SAP_Systems>* ▶ *Identity stores* ▶ *<Identity_store>* ▶, for example SAP_Master. Choose ▶ *New* ▶ *Folder* ▶ from the context menu for your Identity Center configuration.

   > **Note**
   >
   > See the structuring recommendations in *Jobs*.

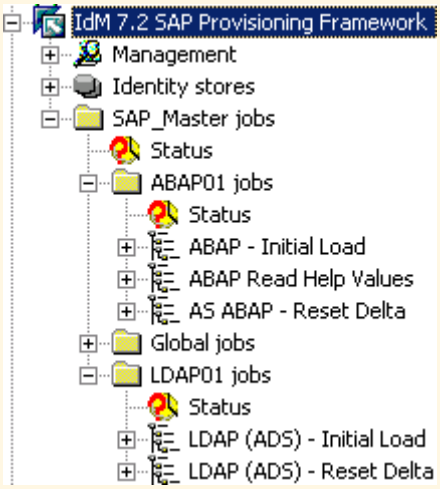
2. Create a subfolder for each system.
3. In each system folder, create a job for each task that applies to the system.
4. Repeat for each job and each system that applies.

Results

Each system used in the use case has a set of jobs to be used for initial load and resetting the delta in the database.

Example

The following figure shows the jobs for an SAP HCM system and an LDAP directory server.



Sample Jobs for Each Connector

System	Jobs	Comment
SAP HCM	ABAP Read Help Values (optional) Initial Load (Optional) Reset Delta	ABAP Read Help Values: Set up this job if you want to retrieve value help content from the AS ABAP system. See *Reading Value Help Content*. Initial Load: Set up this job if you want to read `SU01` data from the AS ABAP system.
AS ABAP (independent of SAP HCM or SAP Business Suite systems)	ABAP Read Help Values (optional) Initial Load Reset Delta	ABAP Read Help Values: Set up this job if you want to read value help content from the AS ABAP system. See *Reading Value Help Content*.
AS Java (with portal)	Initial Load Reset Delta	Reconciliation: This job is only applicable for AS Java installations where an LDAP data source is used for user management.
SAP Business Suite application systems	ABAP Read Help Values (optional) Initial Load (Optional) Reset Delta	ABAP Read Help Values: Set up this job if you want to retrieve value help content from the AS ABAP system. See *Reading Value Help Content*. Initial Load: Set up this job if you want to read `SU01` data from the AS ABAP system.

System	Jobs	Comment
LDAP Directory Server	Initial Load Reset Delta	
SAP HANA database	SAP HANA - Initial Load	

> **Note**
>
> You can also include additional systems in the landscape that are not explicitly shown in these tables, for example, other AS ABAP systems, AS Java systems, or non-SAP systems.
>
> For dual-stack systems, use the AS ABAP job templates.

Related Information

Jobs [page 29]
Reading Value Help Content [page 47]

4.5.8 Password Provisioning

4.5.8.1 Provisioning Productive Instead of Initial Passwords

By default, the connectors contained in the SAP provisioning framework provision initial passwords, as far as the target system distinguishes between initial and productive passwords. This applies to AS ABAP (including SAP Business Suite and other variations), AS Java and SAP HANA. That means, users typically need to change their passwords when they log on to the target system for the first time after provisioning.

If users set their passwords in the Identity Center, provisioning those passwords as initial passwords does not make sense because there is no use in changing this password in the target system again immediately. For this scenario, most target systems allow setting productive instead of initial passwords when certain configuration prerequisites, such as usage of a secure communication channel, are fulfilled. You can configure the connectors to these target systems to provision productive instead of initial passwords.

To provision productive passwords to AS ABAP systems, see *SAP Note 1575445*.

To provision productive passwords to AS Java systems, set the SPML passwordchangerequired attribute in the relevant provisioning jobs to false. Do so in the AS Java Connector under *Plugins* > *8 Set AS JAVA User password* > *Check backendtype* > *DB* > *SetPasswordJavaUser* > *SetPasswordJavaUser* > *SetPasswordJavaUser* > *ToSPML-*

USER. During the Create task the settings of the security policy of the AS Java are enforced. Therefore, the SPML settings for the password are overruled, and using the Create task you cannot make sure that productive passwords are provisioned.

Provisioning of productive passwords to SAP HANA is currently not possible. Whereas password provisioning for SUN and Active Directory Server repositories only provisions productive passwords. Even if the administrator sets a password this password is provisioned without forcing the user to change his password on the first logon to the back-end system.

Related Information

SAP Note 1575445: Setting productive password in ABAP Systems

4.5.9 Single Sign-On for AS ABAP Systems

If you configured Single Sign-On (SSO) on your AS ABAP source system that you use for the initial load, you assigned a unique SNC name to each user, which is displayed, for example, in the SU01 transaction. The user's SNC name is stored in the table USRACL. You can schedule the `RSUSR300` report to fill this table automatically on a regular basis.

For more information about SNC, see the *SNC User's Guide*.

The initial load jobs of the ABAP Connector and the ABAP BusinessSuite Connector write the user's SNC name to the MX_SNC_Name attribute of the user. If the user is created or modified the SNCName attribute of the connector is filled with the value of the MX_SNC_Name attribute. Users then no longer need to provide manual authentication when logging on to the AS ABAP system.

For more information about how to enable Single Sign-On on the AS ABAP, see *User Authentication and Single Sign-On* in the SAP NetWeaver documentation for your release on the Help Portal.

For an easy to implement SSO solution that integrates well with SAP Identity Management, see *SAP Single Sign-On* on the Help Portal.

Related Information

Security in Detail > *Secure User Access* > *Authentication & Single Sign-On* > *SNC User's Guide*
User Authentication and Single Sign-On for SAP NetWeaver 7.3 EHP1
SAP Single Sign-On

4.5.10 Preparing the Initial Loads

Context

There are some preparations to make after you have set up the connectors for the systems in your system landscape but before you run the actual initial loads. These include:

Procedure

1. Determining the leading system for attributes.
2. Determine how initial passwords are generated.
3. Run a test initial load.
4. Fix any inconsistencies or other problems.

4.5.10.1 Determining the Leading System for Attributes

Before proceeding, you must determine which system is the leading system for each attribute and role assignment. Then adjust the attributes in the *Destination* tab pages for each write pass in the initial load jobs. Set the period (.) in the first column of the pass definition for attributes in non-leading systems so that these attributes do not overwrite those from the leading one. For role assignments use the `{A}` option in the pass value if the role assignment is to be added to any existing role assignments. Also adjust the Workflow interface so that these attributes cannot be mistakenly overwritten.

> **Caution**
>
> This step is very important. If you do not specify the leading system per attribute correctly, attributes could be overwritten from other system, leading to unexpected results.

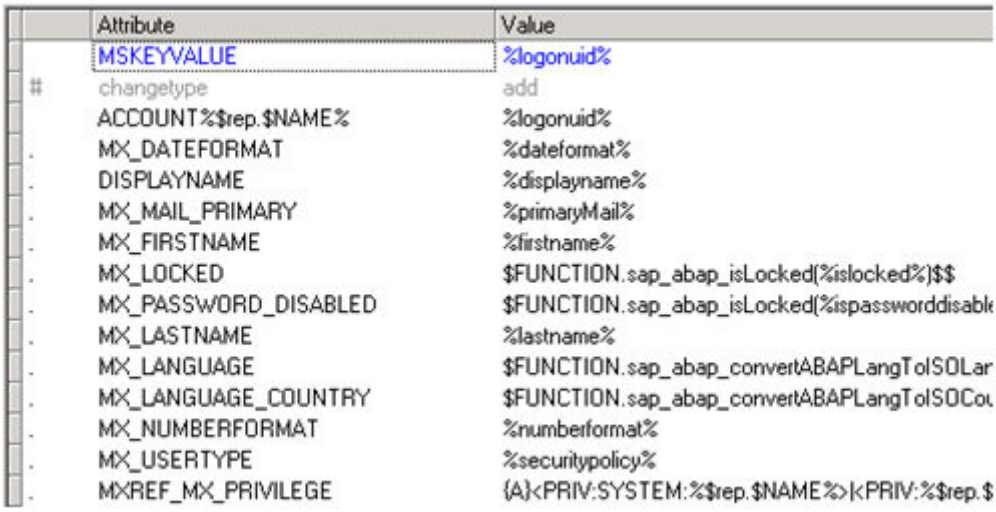
Example:

For example, the following configuration is for an LDAP directory server that is the leading system for the attributes in the pass. No period is set for these attributes in the WriteABAPUsers pass.

Attribute	Value
MSKEYVALUE	%userid%
MX_MAIL_PRIMARY	%mail%
MX_FIRSTNAME	%givenName%
MX_LASTNAME	%sn%
ACCOUNT%$rep.$NAME%	%dn%

In the example below, in the WriteABAPUsers pass for the ABAP initial load, these attributes should not be written to the identity store if the entry already exists. Therefore, the period is set for these attributes. For attributes where the ABAP system is to be the leading system (for example, date format and user type in the example below), no period is set.

In addition, the privilege specified by MXREF_MX_PRIVILEGE is only added if the entry in the identity store does not already exist. Existing role and privilege assignments are not overwritten.



	Attribute	Value
	MSKEYVALUE	%logonuid%
#	changetype	add
	ACCOUNT%$rep.$NAME%	%logonuid%
.	MX_DATEFORMAT	%dateformat%
.	DISPLAYNAME	%displayname%
.	MX_MAIL_PRIMARY	%primaryMail%
.	MX_FIRSTNAME	%firstname%
.	MX_LOCKED	$FUNCTION.sap_abap_isLocked(%islocked%)$$
.	MX_PASSWORD_DISABLED	$FUNCTION.sap_abap_isLocked(%ispassworddisable
.	MX_LASTNAME	%lastname%
.	MX_LANGUAGE	$FUNCTION.sap_abap_convertABAPLangToISOLar
.	MX_LANGUAGE_COUNTRY	$FUNCTION.sap_abap_convertABAPLangToISOCou
.	MX_NUMBERFORMAT	%numberformat%
.	MX_USERTYPE	%securitypolicy%
.	MXREF_MX_PRIVILEGE	{A}<PRIV:SYSTEM:%$rep.$NAME%>|<PRIV:%$rep.$

> **Note**
>
> The screen shots above show examples about how the attributes can be set. They do not coincide with the default configuration.

4.5.10.2 Determine How Initial Passwords are Generated

During the initial load or any other task that creates identities in the identity store, the SAP provisioning framework can generate initial passwords for the users. By default, it uses the password policy as specified in the Identity Center. If nothing is specified in the Identity Center password policy, no initial passwords are generated. If you want to specify your own rules, adapt the global Jscript custom_initializePassword.

Optimization option: If you want to ensure that all new identities get some well-defined default values, for example, a default password, and that well-defined workflows are initiated for all new identities, then create a provisioning task that sets the default values and register this task as an *Add event* task for the MX_PERSON entry type. This task can also trigger additional Workflow tasks, for example, a task that sends an e-mail.

4.5.10.3 Running a Test Initial Load

You can run a test initial load by creating a temporary identity store to use for the initial load passes. Set the SAP_MASTER_IDS_ID global constant to the temporary identity store. Run the initial loads and check if everything

works as expected. Before proceeding with the productive initial load, run the `Reset Delta` job for each repository and change the global constant back to the productive identity store.

See the following sections for typical inconsistencies or errors that you should resolve before performing the initial load.

4.5.10.4 Fix Inconsistencies or Problems

See the sections that follow for possible sources of inconsistencies or problems that may occur during the initial loads. These include the ones listed under Related Links.

Related Information

Fixing Inconsistencies with Privileges (AS ABAP) [page 102]
Out of Memory: Adjusting the Heap Size [page 103]
Timeout: Too many Identities (AS ABAP) [page 104]

4.5.10.4.1 Fixing Inconsistencies with Privileges (AS ABAP)

Context

There may be inconsistencies with privileges on the AS ABAP that lead to errors in the initial load. This can happen due to the order of processing in the initial load, which is:

1. The initial load first reads the AS ABAP roles and creates them in the identity store (in the ReadABAPRoles pass).
2. It then creates the privileges that apply to this role (in the WriteABAPRolePrivileges pass).
3. It then assigns the privileges to the user (in the WriteABAPUsersRolePrivilegeAssignments pass).

Inconsistencies can occur if, for example, the user is assigned to a role or profile that no longer exists. In this case, the initial load cannot read the role or profile and therefore it cannot create the privileges. An error then occurs during the attempt to assign privileges to a user because either the role or privilege does not exist.

If this happens:

Procedure

1. Check whether the role exists on the AS ABAP (use transaction `PFCG`).
2. If the role does not exist anymore, run the `RHAUTUPD_NEW` report on the AS ABAP to get a new consistent state. This report eliminates inconsistencies with deleted roles and leftover role assignments.
3. If AUTO_USERCOMPARE is not active, also run the `PFCG_TIME_DEPENDENCY` report to generate the appropriate profiles.

4.5.10.4.2 Out of Memory: Adjusting the Heap Size

Context

The heap size is specified in the property file for the dispatcher. For more information about how to locate this file and which properties to set, see *SAP Note 1347301*.

If you receive an out of memory error during the initial load due to processing a large number of identities:

Procedure

1. Set up a separate dispatcher to use for the initial loads.
2. Adjust the heap size for this dispatcher.

Related Information

SAP Note 1347301: SAP NetWeaver IdM Identity Center: OutOfMemoryError

4.5.10.4.3 Timeout: Too many Identities (AS ABAP)

If you receive a timeout during the initial load due to reading a large number of identities from an AS ABAP system, you can one of the following options:

- Activate the bootstrap option for the initial load jobs.
  This allows more time for the jobs before a timeout occurs.
- Use the filter mechanism to split up the initial load into several passes. For more information, see *SAP Note 1398976*.

Related Information

SAP Note 1398976 - SAP ID Management: Filter definition for initial load of ABAP entities

4.5.11 Running the Initial Loads

Prerequisites

Prerequisites When Using Central User Administration:

1. Make sure that all data is synchronized in the CUA, for example, company address data. To do this, execute the transaction `SCUG` in the central system.
2. Remove any unnecessary CUA entries that may exist in CUA tables. To do this, execute the `RSDELCUA` report. Activate the option *Invalid Content in CUA Tables*.
3. Make sure role assignments are up-to-date by executing the user master record comparison (sometimes referred to as text comparison) function in the CUA master system. Execute it for all child systems and activate the *Delete invalid assignments* option.
4. Clean up profiles that are not assigned to any roles by executing the `PFUD` transaction in the master system. Select the *Cleanups* option.

Context

> **Tip**
>
> If you are running an initial load in an already existing productive environment, deactivate provisioning on the dispatcher so that the data read is not provisioned into the various systems. Reactivate provisioning on the dispatcher once the initial load has been completed.

Procedure

1. Activate the *Bootstrap job* option and choose *Apply*. With this option, the bootstrap timeouts are applied to the job instead of the normal job timeouts, giving more time for longer job runs.
2. Run the initial loads for your systems. Select each job and choose *Run now*.

> ⚠ Caution
>
> Make sure you run the jobs in the correct order.

4.5.12 Cleaning up the Collected Data

After performing the initial loads, the identity data from all systems is stored in the Identity Center's identity store. It is likely that the quality of this data is quite low. Attributes may be duplicated or missing in some sources, or there may be conflicts between attributes. For example, an identity may be represented in several sources by different user IDs, or different identities may be represented in different sources using the same ID. You therefore need to consolidate and clean up this low-quality data and resolve any conflicts before continuing with the provisioning process.

> ℹ Note
>
> When resolving the data for the use cases described in this document, the user ID is the determining attribute for the identity. This means that each unique user ID that is read from the various data sources is identified and used as the criteria for creating and maintaining identities in the system that is provisioned to.

4.6 Set Up User Interfaces for User Administration (Workflow)

Prerequistes

- The user administrator accounts that should have access to the Workflow tasks exist in the identity store.
- If you do not have any user administrator accounts, you can create them in the Identity Center.

4.6.1 Creating a User Administrator Account (Optional)

Context

To set up a user administrator account for using the Workflow application in the Identity Center:

Procedure

1. Select the identity store to configure (for example, `SAP_Master`).
2. In the *General* tab, choose *Add* user.
3. In the dialog that follows, specify the **`Entry type MX_PERSON`**, create an administrator user and specify a password for this user.
4. Select *Add manager privileges* and *Add administrator privileges* as appropriate. The option *Add manager privileges* gives the user access to the Workflow UIs, and *Add administrator privileges* gives the user access to the Monitoring and Transport UIs.
5. Apply the changes.

4.6.2 Configuring the User Interfaces

Context

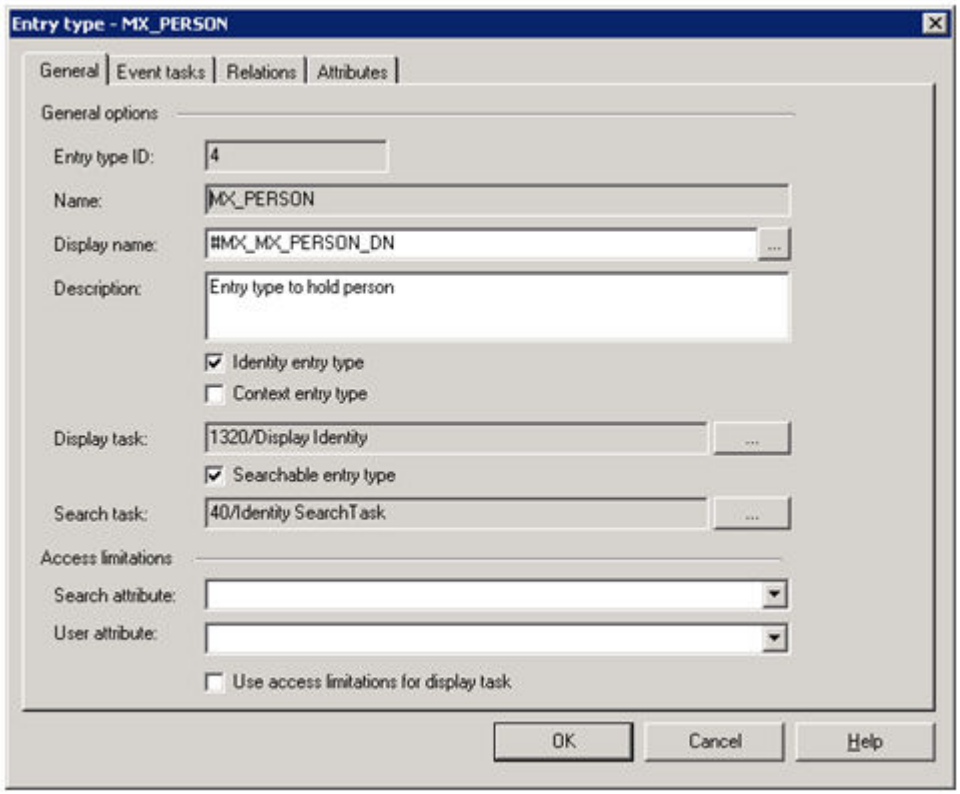
To configure the User Interfaces, do the following:

Procedure

1. To assign the access rights, you must modify the web-enabled tasks. Therefore, copy these tasks to a custom Web-Enabled Tasks folder.

   See the recommendations in *Tasks*.
2. Set the display and search tasks for identities, privileges, and roles as described in *Displaying and Searching Tasks*.
3. To make tasks appear in the Workflow application, assign the access control rights so that user administrators can access the task.

4. To do this, select the task and choose the *Access control* tab page. Add the users, roles or privileges that should have access to the application. Make sure the tasks are enabled and that the *UI task* option is activated.
5. You can also create and set up additional tasks as necessary.
6. In the *Attributes* tab page, adjust the attributes to display as necessary.



7. Apply the changes.

Related Information

Tasks [page 26]
Displaying and Searching Tasks [page 107]

4.6.2.1 Displaying and Searching Tasks

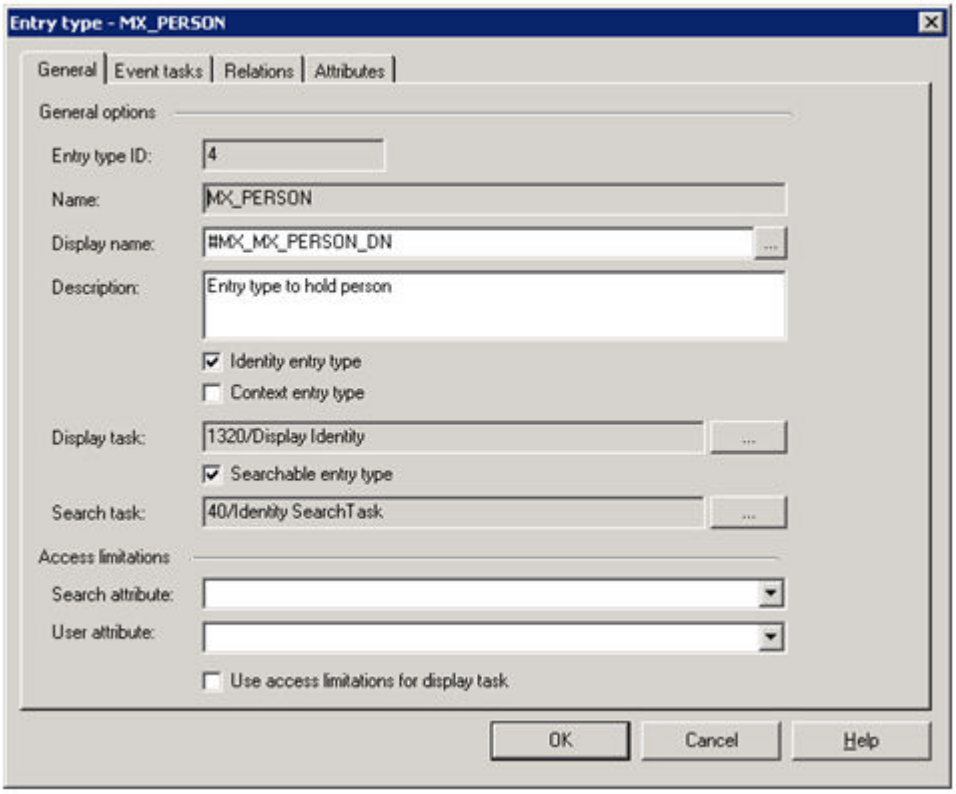
Context

Procedure

1. Under *Console Root* > *SAP NetWeaver Identity Management* > *<IC_Configuration_for_SAP_Systems>* > *Identity stores* > *<Identity Store>* > *Identity store schema* > *Entry types* , select the corresponding entry type (MX_PERSON, MX_PRIVILEGE, or MX_ROLE) with a double-click.
2. In the *General* tab, in the *Display task:* field, select the *Display <Identity/Privilege/Role>* task
3. In the *Search task:* field, select the *<Identity/Privilege/Role> Search* task.
4. Repeat for the entry types (MX_PERSON, MX_PRIVILEGE, MX_ROLE).

Example

See the screen shot below for MX_PERSON.



4.7 Maintaining Business Roles

Prerequisites

You have set up the role model and know which privileges (technical roles) apply to which business roles.

Context

Once you have set up the workflow tasks, you can maintain your business roles in the identity store.

> **Note**
>
> The exact procedure depends on your own processes. For example, if you have set up an approval process, then you have to take this into account. The procedure below describes the basic process.

Procedure

1. Start the web application and log on as a user administrator.

   The application has the URL `<host>:<port>/idm`. If you do not know the host and port, contact the AS Java administrator.
2. To create or edit a business role, choose the *Manage* tab page.
3. Select *Role* in the *Show* field.
4. Create a new role.
5. Edit an existing role (including the one you just created).
6. Add privileges to the role.
7. Repeat these steps until all appropriate privileges are assigned.
8. Save the data.
9. To assign users to the business role, choose the *Assigned Identities* tab, select the identities and add them to the business role in the same way.

   > **Note**
   >
   > You can assign other objects to the role in the same way, for example, other roles or groups.

4.7.1 Creating a New Role

Context

Procedure

1. Choose *Create...*.

   The *Tasks Available for this Entry* dialog appears. The list of tasks shown depends on how you have set up your web-enabled tasks.
2. Expand the available entries until you find the task to use for creating roles (for example, *Web-Enabled Tasks* > *Role* > *Create Business Role*).
3. Choose *Choose Task*.
4. On the *Create Business Role* screen, enter a name and a unique ID for the role.

   > **Tip**
   >
   > We recommend using a naming convention with the following syntax `ROLE:BUSINESS:<Role_Name>` for the business role.
5. Save the role and close the screen.

4.7.2 Editing an Existing Role

Context

Procedure

1. Search for the role to edit, select it from the list and choose *Choose Task*.

   The *Tasks Available for this Entry* dialog appears.
2. Expand the available entries until you find the task to use for creating roles (for example, *Web-Enabled Tasks* > *Role* > *Change Business Role*).

The *Change Business Role* screen appears

4.7.3 Adding Privileges to a Role

Context

Procedure

1. Choose the *Assigned Privileges* tab.
2. Search for the privilege to assign to the role.

   The syntax for the privilege's detailed information is `PRIV:<Privilege_Type>:<Repository>:<ID>`, where the syntax for the `<Privilege_Type>` depends on the system type for which the privilege applies.
3. Choose *Add*.

   The privilege is added to the list of privileges in the *Assigned* section.

4.8 Assigning the System Account Privilege to Users or Company Addresses

To specify in which connected systems a user has an account or a company address exists, there is the system account privilege. This system account privilege has the syntax `PRIV:<Repository>:ONLY`.

During an initial load for a repository, this system account privilege is automatically assigned to the identities and company addresses read from the corresponding system. However, when creating identities, or if you want to provision identities to other connected systems, assign the corresponding system account privileges to the identity. To provision a company address to other connected systems, assign the corresponding system account privileges to the company address.

4.9 Using an Update Job for Reading New Privileges and New Company Addresses

Set up this job to run occasionally to update data from the connected systems. This job checks for new privileges and new company addresses in the connected system. These privileges and addresses are then read into the Identity Center.

This update job does not delete privileges that have been deleted in the back-end systems.

A prerequisite for using an update job is that the initial load job has already been executed for the repository before the update job is started.

4.9.1 Creating an Update Job

Context

Procedure

1. In the Identity Center, choose *<IC_Configuration_for_SAP_Systems>* > *Job folder* > *<optionally_subfolder>*. Choose *New* > *Run job wizard...* from the context menu.
2. Follow the instructions provided by the wizard. In step 2 of the wizard, choose *Identity Center* > *Jobs* > *SAP NetWeaver* > *<system> - Initial Load*.
3. In step 3, select the system for which to create the update job as repository.
4. Choose *Finish*.

   The job is created in your folder.
5. Rename the job's misleading name to a more accurate one, for example, *<system> - Update*, for example, *ABAP - Update*.
6. Adjust the job. The following describes an ABAP or Dual Stack update job. You can modify the initial load job of other systems in a similar manner. Leave only the following passes active. Using the context menu, deselect the *Pass enabled* menu option to deactivate each of the other passes.
   - ReadABAPRoles
   - ReadABAPProfiles
   - ReadABAPCompanyAddress
   - ReadJavaRoles
   - WriteABAPRolePrivileges: only if corresponding Read pass is active

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

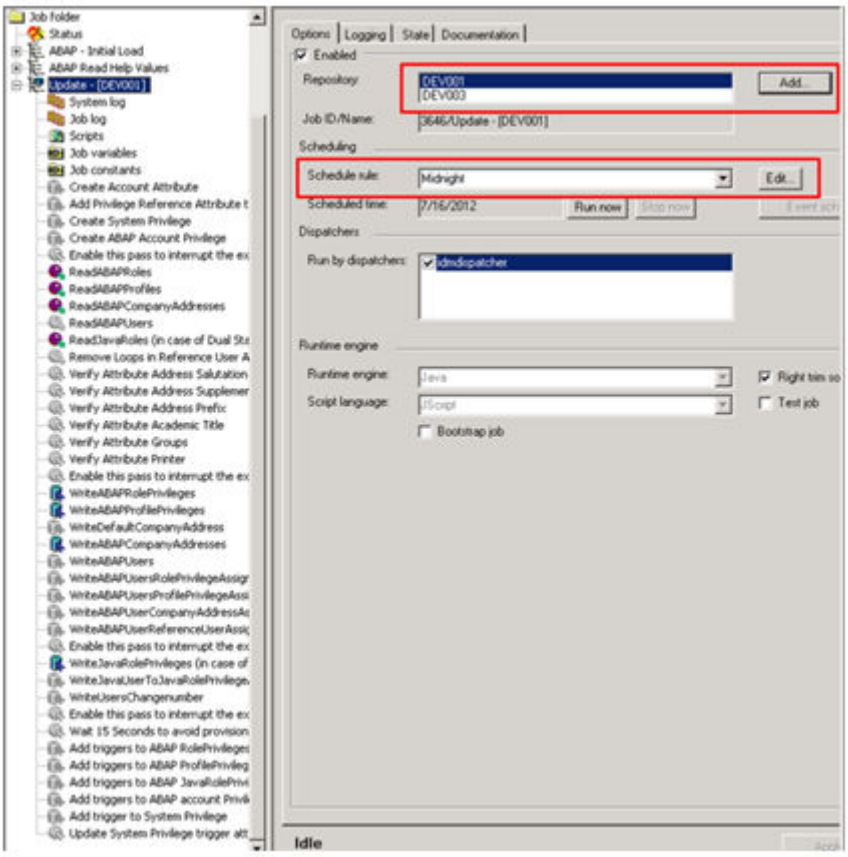
> **Note**
>
> Make sure that you set the triggers for the privileges in the write tasks. If you upload a privilege and assign it to a user before the AddTrigger executes, the privilege might not be assigned properly. Then, for example, the Identity Center displays the assignment of the privilege to the user, but in the back-end system, no such assignment exists, because the provisioning was not triggered.
>
> Therefore, set the triggers in the write tasks, for example, as follows:

Triggers for Write Tasks: Sample

Write Task	Trigger
MX_ADD_MEMBER_TASK	{D}
MX_DEL_MEMBER_TASK	{D}
MX_PROVISIONTASK	{D}
MX_DEPROVISIONTASK	{D}
MX_VALIDATE_ADD_TASK	{D}
MX_VALIDATE_DEL_TASK	{D}
MX_MODIFYTASK	-1

As for all jobs, you can create job templates. In the case of update jobs, you create a template per repository type. Then you can define multiple repositories (of the same type) for the job and set different (or the same) scheduling rules for them.

See the sample update job below.



4.9.2 Scheduling an Update Job

Context

Depending on how often you add new privileges in the back-end systems, schedule the update jobs to run frequently, for example, daily.

To schedule the job:

Procedure

1. Select the update job you created for each system that should be updated.
2. Select the schedule rule that applies, for example, *Midnight*.

3. Choose *Edit...* and specify the exact times and days for the job to run.
4. Apply the changes.

4.10 Assigning Function Set Privileges to Users for SAP Business Suite Applications

Context

When working with the enhanced SAP Business Suite use case, function set privileges are created for each of the SAP Business Suite applications that are activated for provisioning with SAP Identity Management. These privileges have the following syntax:

```
PRIV:FUNCTION_SET:<Repository>:<BAdI_Filter_Value>
```

Procedure

Assign this privilege to business roles or identities that use the corresponding SAP Business Suite application.

> **Note**
>
> Active SAP Business Suite applications are specified in the `IDM_BADI_FILTER BAdI` filter table.

4.11 Provisioning

Changes you make to identity data using the Identity Management workflow application are then provisioned to the appropriate systems.

4.12 Next Steps

4.12.1 Monitoring

Choose the *Monitoring* tab page in the Identity Management workflow application to access the various logs. These include:

- Approval Queue
- Dispatcher status
- Job log
- Job status
- Provisioning audit
- Provisioning log
- Provisioning queue
- System log

In these logs, you can check the status of jobs or tasks, check for tasks that are in the processing queue, or analyze error or warning messages.

The job status, job log, and system log are also available in the Identity Center for the case that the system is offline.

4.12.2 Setting up an SAP Java Connector (SAP JCo) and Related Traces

To analyze errors related to an issue with a connection from the Identity Center to an AS ABAP, you must first activate traces to get more information.

Context

These traces log information for all ABAP-related passes of the relevant dispatcher. In connection with JCo the following traces are available: JCo trace, JRFC trace, and CPIC trace. In this order they contain more and more technical details.

> **Note**
>
> We recommend that you start the analysis using the JCo trace. Only if this does not collect enough technical details, use the JRFC or even the CPIC trace.

To set up the SAP JCo related tracing, you can either configure tracing for all ABAP-related passes of the relevant dispatcher using Java system properties or you can just trace specific passes. For more information on tracing specific passes, see the *Related Links* section.

> **Tip**
>
> For performance reasons and to avoid unnecessary amounts of data in the traces, make sure that you only trace as much as necessary. Rather use pass-specific traces than traces for the complete dispatcher.

For more information about analysis of JCo traces in general, see *JCo Exceptions* in the SAP Library for your AS Java release.

Procedure

1. In the Identity Center, choose *<IC_Configuration_for_SAP_Systems>* > *Management* > *Dispatchers* > *<dispatcher>*.
2. Choose the *Policy* tab.
3. In the *Java options* field, enter the global trace parameters for JCo. Make sure to place **-D** in front of every single parameter and separate multiple options with a space character.

   The table below shows the available traces going from the most global one to the one containing most technical details.

   Global Trace Parameters

Parameter	Possible Values	Description

jco.trace_path	Enter an existing path.	Sets the location of the path for JCo trace files.
		To output the JCo trace into a file, set the path value, to an existing directory. If the directory does not exist, no log files are written.
		Note
		If there are spaces in the path name, make sure that you use quotation marks ("), for example:
		`-Djco.trace_path="C:\usr\sap\IdM\Identity Center" -Djco.trace_level=8 -Djrfc.trace=1`
		For each event a trace is written into a log file with the following syntax:
		`JCO<date>_<timestamp>.trc`
		Available for JCo3 and JCo2.

jco.trace_level	Valid values: levels 0 to 10. The commonly used ones are described in the Trace Levels table below. Default value: 0	Turns on the JCo trace. Available for JCo3 and JCo2.

Parameter	Possible Values	Description
jrfc.trace	0: trace is off 1: RFC trace is on Default value: 0	If set to 1, RFC trace is turned on for all connections within JCo. The trace is written to the location as indicated in jco.trace_path. For each event a trace is written into a log file with the following syntax: `jco_rfc<identifier>_<number>.trc` **Note** For performance reasons, only use this parameter in case of emergency to activate an RFC trace. Rather activate the RFC trace for specific passes. By default, the RFC trace is disabled. The destination name is the repository name. Available for JCo3 only.
cpic.trace	4 Valid Values: 0 to 3 0: trace is off 3: most verbose trace Default value: 0	The trace level for the CPIC layer. The CPIC trace is always written into the Identity Center installation directory, for example, `\usr\sap\IdM\Identity Center`. Depending on where the trace is configured, the file name is: ○ CPIC<date>_<Timestamp>.trc, when configured globally in the dispatcher. ○ CPICTRC<identifier>, when configured in the pass. Available for JCo3 only.

Trace Levels

Value	Description
0	No trace.
1	Traces errors.
2	Traces errors and warnings.

Value	Description
3	Traces info messages, errors, and warnings.
4	Traces execution path, info messages, errors, and warnings.
5	Verbose trace of execution path, info messages, errors, and warnings.
6	Verbose trace of execution path, limited data dumps, info messages, errors, and warnings.
7	Full trace of execution path, data dumps with metadata, verbose info messages, errors, and warnings.
8	Full trace of execution path, full data dumps with metadata, verbose info messages, errors, and warnings.

4. To save your changes, choose *Apply*.
5. Regenerate the dispatcher scripts.
6. For the changes to take effect, restart the relevant dispatchers.
7. For performance reasons, deactivate the traces as soon as possible.

Related Information

JCo Exceptions. This topic describes the exceptions for an SAP NetWeaver AS for Java. The properties of the exceptions basically also apply for the Identity Management use case. The file locations differ.

Restricting the CPIC or JRFC Trace to a Specific Pass [page 119]

4.12.2.1 Restricting the CPIC or JRFC Trace to a Specific Pass

Identity Management system administrators can configure CPIC and JRFC traces (only trace level) for specific ABAP-related passes with an additional parameter in the From/ToCustom passes with pass types FromSAP, FromSAPIdentity, ToSAP and ToSAPIdentity.

Context

Then only those connections that cause problems are traced.

Procedure

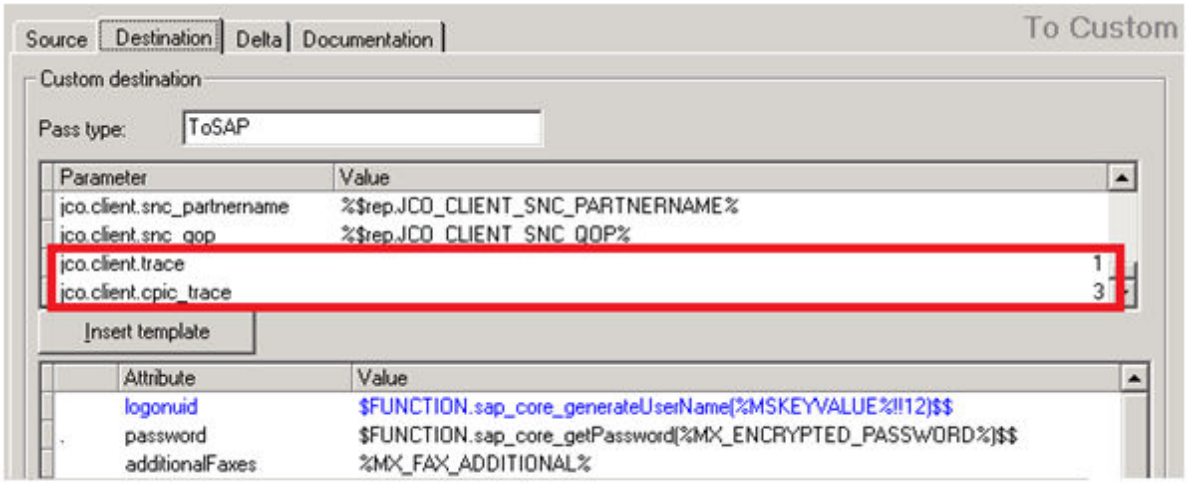
1. In the Identity Center, choose *<IC_Configuration_for_SAP_Systems>* > *Management* > *Identity stores* > *<identity_store>* > *Provisioning Framework* > *CONNECTORS* > *ABAP Connector* > *AS ABAP Tasks* > *<specific task>* > *<job>* > *<pass>*.

   > **Note**
   >
   > This is also valid for the ABAP BusinessSuite Connector passes of the listed types in standalone jobs like initial load and read help values (actually: ABAP - Initial Load, ABAP - Provision Company Addresses to ABAP Repositories, ABAP Read Help Values, BusinessSuite AS ABAP - Initial Load) as well as for custom provisioning jobs and standalone jobs using these pass types.

2. Choose the *Destination* tab for provisioning job passes or the *Source* tab for standalone job passes.
3. Select a line in the parameter-value table.
4. To add a parameter and its value, choose *Insert* from the context menu.
5. Enter the parameters using the following data:

   Trace Parameters

Parameter	Value	Comment
jco.client.trace	1	This is the pass-specific variant of the jrfc.trace parameter.
jco.client.cpic_trace	3	This is the pass-specific variant of the cpic.trace parameter.



6. To save your changes, choose *Apply*.

5 Appendix A: Repository Constants

The tables below show the repository constants used for each repository type.

For more information about constants, see *Identity Center - Identity Store Schema*.

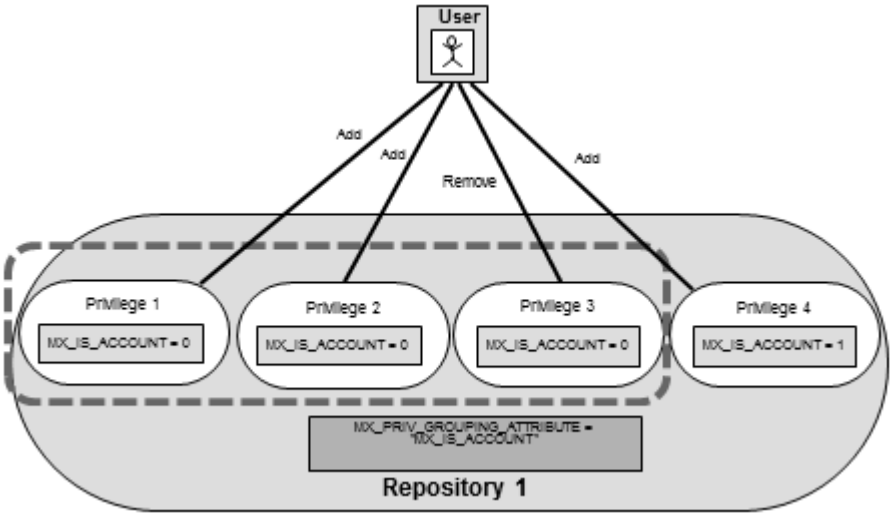
General Remarks on Repository Constants

- All repository constants listed in the tables are set automatically using the data you enter in the configuration wizard.
- You should not change any of the following constants
  - MX_PRIV_GROUPING_ATTRIBUTE
    Property attribute for grouping.
  - MX_GROUPING_RULE
    The repository templates use the following values:

    Values for MX_GROUPING_RULE

Value	Comment
P:4	With this value, the system groups privilege assignments if the assigned privileges have the same value for the attribute defined in MX_PRIV_GROUPING_ATTRIBUTE constant of their repository.
P:5	Same as P:4 but the operation type, for example, remove or add is also taken into account. Privilege assignments are only grouped if the operation type is also the same.

    Example for Privilege Grouping in AS ABAP Repositories



P:4
The MX_PRIV_GROUPING_ATTRIBUTE repository constant has the value MX_IS_ACCOUNT. MX_IS_ACCOUNT is an attribute defined at the privilege. It has the value 0 for all privileges representing ABAP roles or profiles, while the system-specific privileges `PRIV:SYSTEM:<Repository>` and `PRIV:<Repository>:ONLY` have another value. Therefore, all assignments of ABAP roles and profiles are grouped and thus are processed in a single provisioning. This applies to privileges 1, 2, and 3. The different operation types shown in the figure above are not relevant with this grouping rule.
If the attribute has a different value the privilege is not grouped (privilege 4). P:5 (not included in the figure above).
In addition to the criteria valid for P:4, the operation type for the privilege is also taken into account. Privilege 3 would not be grouped together with privileges 1 and 2 because it has a remove operation.

  - REPOSITORY_SYNC
  - REPOSITORY_TYPE
    Describes what kind of system is connected. In the templates the values are, for example, ABAP, DUALABAP, JAVA, LDAP, and SUN.

  You can replace HOOK (plug-in) tasks with your own tasks. You can also set HOOK tasks. if you do not wish to use a certain functionality you can disable HOOK tasks by selecting “-- None --“.

- To adapt connectivity constants that define the connection to the back-end system, you adjust them directly without having to delete and re-create the repository.

Related Information

SAP NetWeaver Identity Management Identity Center - Identity Store Schema - Technical Reference

5.1 Repository Constants for AS ABAP (Load Balanced Connection)

Repository Constants

Repository Wizard Field	Repository Constant	Value
Message Server	JCO_CLIENT_MSHOST	<message_server_hostname>
System ID	JCO_CLIENT_R3NAME	<SID>
Logon Group	JCO_CLIENT_GROUP	<Group>, for example, Public
User Name	JCO_CLIENT_USER	<user_ID>
Password	JCO_CLIENT_PASSWD	<password> For AS ABAP Release 4.6C, use upper-case.
Client	JCO_CLIENT_CLIENT	<client>
Language	JCO_CLIENT_LANG	<language ID>, for example, EN
CUA System	CUA_MASTER	<TRUE/FALSE>
System privilege	SYSTEM_PRIVILEGE	PRIV:SYSTEM:<Repository> where <Repository> is the exact name of the repository to which the constants belongs.

The following constants are automatically created and therefore not visible in the wizard.

Additional Repository Constants

Repository Constant	Value
JCO_CLIENT_ASHOST	<application_server_hostname>
JCO_CLIENT_GWHOST	<gateway hostname> To find out the data for your Gateway, choose *Administration* > *System Administration* > *Monitor* > *System Monitoring* > *Gateway Monitor*. A list is displayed of all the SAP Gateways connected to your SAP System. Usually, an Gateway is assigned to each SAP application server and database server.
JCO_CLIENT_GWSERV	<gateway service> (for example, “sapgw00”)

Repository Constant	Value
JCO_CLIENT_SYSNR	<system number>
MX_ADD_MEMBER_TASK	<task number for Provisioning>
MX_DEL_MEMBER_TASK	<task number for Deprovisioning>
MX_MODIFYTASK	<task number for Modify>
MX_PRIV_GROUPING_ATTRIBUTE	MX_IS_ACCOUNT
MX_PRIV_GROUPING_RULE	P:4 With this value, entries are grouped if they have the same attribute defined in the repository constant MX_PRIV_GROUPING_ATTRIBUTE.
MX_HOOK1_TASK	<task number for AS ABAP PlugIn 1> (1. Create ABAP User)
MX_HOOK2_TASK	<task number for AS ABAP PlugIn 2> (2. Modify ABAP User)
MX_HOOK3_TASK	<task number for AS ABAP PlugIn 3> (3. Delete ABAP User)
MX_HOOK4_TASK	<task number for AS ABAP PlugIn 4> (4. Assign User Membership to ABAP)
MX_HOOK5_TASK	<task number for AS ABAP PlugIn 5> (5. Revoke User Membership to ABAP)
MX_HOOK6_TASK	<task number for AS ABAP PlugIn 6> (6. Enable ABAP User)
MX_HOOK7_TASK	<task number for AS ABAP PlugIn 7> (7. Disable ABAP User)
MX_HOOK8_TASK	<task number for AS ABAP PlugIn 8> (8. Set ABAP User Password)
MX_HOOK9_TASK	--None--
MX_HOOK10_TASK	<task number for AS ABAP PlugIn 10> (10. Create Group)

Repository Constant	Value
MX_HOOK11_TASK	<task number for AS ABAP PlugIn 11> (11. Delete Group)
MX_HOOK12_TASK	<task number for AS ABAP PlugIn 12> (12. Create ABAP Company Address)
MX_HOOK13_TASK	<task number for AS ABAP PlugIn 13> (13. Modify ABAP Company Address)
MX_HOOK14_TASK	<task number for AS ABAP PlugIn 14> (14. Delete ABAP Company Address)
REPOSITORY_SYNC	SYNC
REPOSITORY_TYPE	ABAP

There are additional constants for configuring Secure Network Communications (SNC). For more information, see Appendix D: Configuring the ABAP Connector to use SNC.

Related Information

Appendix D: Configuring the ABAP Connector to Use SNC [page 167]

5.2 Repository Constants for AS ABAP (Specific Application Server)

Repository Constants

Repository Wizard Field	Repository Constant	Value
Target Host	JCO_CLIENT_ASHOST	<hostname>
System Number	JCO_CLIENT_SYSNR	<system number>
User Name	JCO_CLIENT_USER	<user_ID>
Password	JCO_CLIENT_PASSWD	<password> For AS ABAP Release 4.6C, use upper-case.

Repository Wizard Field	Repository Constant	Value
Client	JCO_CLIENT_CLIENT	<client>
Language	JCO_CLIENT_LANG	<language ID>, for example, EN
CUA System	CUA_MASTER	<TRUE/FALSE>
System privilege	SYSTEM_PRIVILEGE	PRIV:SYSTEM:<Repository> where <Repository> is the exact name of the repository to which the constants belongs.

The following constants are automatically created and therefore not visible in the wizard.

Additional Repository Constants

Repository Constant	Value
JCO_CLIENT_GROUP	<Group>, for example, Public
JCO_CLIENT_GWHOST	<gateway hostname> To find out the data for your Gateway, choose *Administration* > *System Administration* > *Monitor* > *System Monitoring* > *Gateway Monitor*. A list is displayed of all the SAP Gateways connected to your SAP System. Usually, an Gateway is assigned to each SAP application server and database server.
JCO_CLIENT_GWSERV	<gateway service> (for example, “sapgw00”)
JCO_CLIENT_MSHOST	<message_server_hostname>
JCO_CLIENT_R3NAME	<SID>
MX_ADD_MEMBER_TASK	<task number for Provisioning>
MX_DEL_MEMBER_TASK	<task number for Deprovisioning>
MX_MODIFYTASK	<task number for Modify>
MX_PRIV_GROUPING_ATTRIBUTE	MX_IS_ACCOUNT
MX_PRIV_GROUPING_RULE	P:4 With this value, entries are grouped if they have the same attribute defined in the repository constant MX_PRIV_GROUPING_ATTRIBUTE.

Repository Constant	Value
MX_HOOK1_TASK	<task number for AS ABAP PlugIn 1> (1. Create ABAP User)
MX_HOOK2_TASK	<task number for AS ABAP PlugIn 2> (2. Modify ABAP User)
MX_HOOK3_TASK	<task number for AS ABAP PlugIn 3> (3. Delete ABAP User)
MX_HOOK4_TASK	<task number for AS ABAP PlugIn 4> (4. Assign User Membership to ABAP)
MX_HOOK5_TASK	<task number for AS ABAP PlugIn 5> (5. Revoke User Membership to ABAP)
MX_HOOK6_TASK	<task number for AS ABAP PlugIn 6> (6. Enable ABAP User)
MX_HOOK7_TASK	<task number for AS ABAP PlugIn 7> (7. Disable ABAP User)
MX_HOOK8_TASK	<task number for AS ABAP PlugIn 8> (8. Set ABAP User Password)
MX_HOOK9_TASK	--None--
MX_HOOK10_TASK	<task number for AS ABAP PlugIn 10> (10. Create Group)
MX_HOOK11_TASK	<task number for AS ABAP PlugIn 11> (11. Delete Group)
MX_HOOK12_TASK	<task number for AS ABAP PlugIn 12> (12. Create ABAP Company Address)
MX_HOOK13_TASK	<task number for AS ABAP PlugIn 13> (13. Modify ABAP Company Address)
MX_HOOK14_TASK	<task number for AS ABAP PlugIn 14> (14. Delete ABAP Company Address)
REPOSITORY_SYNC	SYNC

Repository Constant	Value
REPOSITORY_TYPE	ABAP

There are additional constants for configuring Secure Network Communications (SNC). For more information, see Appendix D: Configuring the ABAP Connector to use SNC.

Related Information

Appendix D: Configuring the ABAP Connector to Use SNC [page 167]

5.3 Repository Constants for AS Java (LDAP Backend)

Repository Constants

Repository Wizard Field	Repository Constant	Value
HTTP Protocol	HTTP_Protocol	<http/https> For password provisioning SSL must be set up.<TRUE/FALSE>
Target Host	APPLICATION_HOST	<hostname>
HTTP Port	HTTP_PORT	<http_port>
User Name	HTTP_AUTH_USER	<user_ID>
Password	HTTP_AUTH_PWD	<password>
Backend Repository Name	BACKEND_ REPOSITORYNAME	<LDAP directory repository name>
System privilege	SYSTEM_PRIVILEGE	PRIV:SYSTEM:<Repository> where <Repository> is the exact name of the repository to which the constants belongs.

The following constants are automatically created and therefore not visible in the wizard.

Additional Repository Constants

Repository Constant	Value
BACKEND_TYPE	LDAP

Repository Constant	Value
MX_ADD_MEMBER_TASK	<task number for Provisioning>
MX_DEL_MEMBER_TASK	<task number for Deprovisioning>
MX_MODIFYTASK	<task number for Modify>
MX_PRIV_GROUPING_ATTRIBUTE	MX_PRIVILEGE_TYPE
MX_PRIV_GROUPING_RULE	P:5 With this value, entries are grouped if they have the same attribute defined in the repository constant MX_PRIV_GROUPING_ATTRIBUTE and if they are of the same operation type, for example, add or remove.
MX_HOOK1_TASK	<task number for AS Java PlugIn 1> (1 Create AS JAVA User)
MX_HOOK2_TASK	<task number for AS Java PlugIn 2> (2 Modify AS JAVA User)
MX_HOOK3_TASK	<task number for AS Java PlugIn 3> (3 Delete AS JAVA User)
MX_HOOK4_TASK	<task number for AS Java PlugIn 4> (4 Assign User Membership to AS Java)
MX_HOOK5_TASK	<task number for AS Java PlugIn 5> (5 Revoke User Membership to AS Java)
MX_HOOK6_TASK	<task number for AS Java PlugIn 6> (6 Enable AS Java User)
MX_HOOK7_TASK	<task number for AS Java PlugIn 7> (7 Disable AS Java User)
MX_HOOK8_TASK	<task number for AS Java PlugIn 8> (8 Set AS Java User Password)
MX_HOOK9_TASK	<blank>
MX_HOOK10_TASK	<task number for AS Java PlugIn 10> (10 Create Group)

Repository Constant	Value
MX_HOOK11_TASK	<task number for AS Java PlugIn 11> (11 Delete Group)
REPOSITORY_SYNC	SYNC
REPOSITORY_TYPE	JAVA

5.4 Repository Constants for AS Java

Repository Constants

Repository Wizard Field	Repository Constant	Value
HTTP Protocol	HTTP_Protocol	<http/https> For password provisioning SSL must be set up.<TRUE/FALSE>
Target Host	APPLICATION_HOST	<hostname>
HTTP Port	HTTP_PORT	<http_port>
User Name	HTTP_AUTH_USER	<user_ID>
Password	HTTP_AUTH_PWD	<password>
System privilege	SYSTEM_PRIVILEGE	PRIV:SYSTEM:<Repository> where <Repository> is the exact name of the repository to which the constants belongs.

The following constants are automatically created and therefore not visible in the wizard.

Additional Repository Constants

Repository Constant	Value
BACKEND_TYPE	DB
MX_ADD_MEMBER_TASK	<task number for Provisioning>
MX_DEL_MEMBER_TASK	<task number for Deprovisioning>
MX_MODIFYTASK	<task number for Modify>

Repository Constant	Value
MX_PRIV_GROUPING_ATTRIBUTE	MX_PRIVILEGE_TYPE
MX_PRIV_GROUPING_RULE	P:5 With this value, entries are grouped if they have the same attribute defined in the repository constant MX_PRIV_GROUPING_ATTRIBUTE and if they are of the same operation type, for example, add or remove.
MX_HOOK1_TASK	<task number for AS Java PlugIn 1> (1 Create AS JAVA User)
MX_HOOK2_TASK	<task number for AS Java PlugIn 2> (2 Modify AS JAVA User)
MX_HOOK3_TASK	<task number for AS Java PlugIn 3> (3 Delete AS JAVA User)
MX_HOOK4_TASK	<task number for AS Java PlugIn 4> (4 Assign User Membership to AS Java)
MX_HOOK5_TASK	<task number for AS Java PlugIn 5> (5 Revoke User Membership to AS Java)
MX_HOOK6_TASK	<task number for AS Java PlugIn 6> (6 Enable AS Java User)
MX_HOOK7_TASK	<task number for AS Java PlugIn 7> (7 Disable AS Java User)
MX_HOOK8_TASK	<task number for AS Java PlugIn 8> (8 Set AS Java User Password)
MX_HOOK9_TASK	<blank>
MX_HOOK10_TASK	<task number for AS Java PlugIn 10> (10 Create Group)
MX_HOOK11_TASK	<task number for AS Java PlugIn 11> (11 Delete Group)
REPOSITORY_SYNC	SYNC
REPOSITORY_TYPE	JAVA

5.5 Repository Constants for a Dual-Stack System (Load Balanced Connection)

Repository Constants

Repository Wizard Field	Repository Constant	Value
AS ABAP User Name	JCO_CLIENT_USER	<user_ID>
AS ABAP Password	JCO_CLIENT_PASSWD	<password> For AS ABAP Release 4.6C, use upper-case.
AS ABAP Message Server	JCO_CLIENT_MSHOST	<message_server_hostname>
AS ABAP System ID	JCO_CLIENT_R3NAME	<SID>
AS ABAP Logon Group	JCO_CLIENT_GROUP	<Group>, for example, Public
AS ABAP Client	JCO_CLIENT_CLIENT	<client>
AS ABAP Language	JCO_CLIENT_LANG	<language ID>, for example, EN
AS Java HTTP Protocol	HTTP_PROTOCOL	<http/https>
AS Java Target Host	APPLICATION_HOST	<hostname>
AS Java HTTP Port	HTTP_PORT	<http_port>
AS Java User Name	HTTP_AUTH_USER	<user_ID>
AS Java Password	HTTP_AUTH_PWD	<password>
System privilege	SYSTEM_PRIVILEGE	PRIV:SYSTEM:<Repository> where <Repository> is the exact name of the repository to which the constants belongs.
AS ABAP CUA System	CUA_MASTER	<TRUE/FALSE>

The following constants are automatically created and therefore not visible in the wizard.

Additional Repository Constants

Repository Constant	Value
JCO_CLIENT_ASHOST	<hostname>

Repository Constant	Value
JCO_CLIENT_GWHOST	<gateway hostname> To find out the data for your Gateway, choose *Administration* > *System Administration* > *Monitor* > *System Monitoring* > *Gateway Monitor*. A list is displayed of all the SAP Gateways connected to your SAP System. Usually, an Gateway is assigned to each SAP application server and database server.
JCO_CLIENT_GWSERV	<gateway service> (for example, “sapgw00”)
JCO_CLIENT_SYSNR	<system number>
MX_ADD_MEMBER_TASK	<task number for Provisioning>
MX_DEL_MEMBER_TASK	<task number for Deprovisioning>
MX_MODIFYTASK	<task number for Modify>
MX_PRIV_GROUPING_ATTRIBUTE	MX_IS_ACCOUNT
MX_PRIV_GROUPING_RULE	P:4 With this value, entries are grouped if they have the same attribute defined in the repository constant MX_PRIV_GROUPING_ATTRIBUTE.
MX_HOOK1_TASK	<task number for AS ABAP PlugIn 1> (1. Create ABAP User)
MX_HOOK2_TASK	<task number for AS ABAP PlugIn 2> (2. Modify ABAP User)
MX_HOOK3_TASK	<task number for AS ABAP PlugIn 3> (3. Delete ABAP User)
MX_HOOK4_TASK	<task number for AS ABAP PlugIn 4> (4. Assign User Membership to ABAP)
MX_HOOK5_TASK	<task number for AS ABAP PlugIn 5> (5. Revoke User Membership to ABAP)
MX_HOOK6_TASK	<task number for AS ABAP PlugIn 6> (6. Enable ABAP User)

Repository Constant	Value
MX_HOOK7_TASK	<task number for AS ABAP PlugIn 7> (7. Disable ABAP User)
MX_HOOK8_TASK	<task number for AS ABAP PlugIn 8> (8. Set ABAP User Password)
MX_HOOK9_TASK	--None--
MX_HOOK10_TASK	<task number for AS ABAP PlugIn 10> (10. Create Group)
MX_HOOK11_TASK	<task number for AS ABAP PlugIn 11> (11. Delete Group)
MX_HOOK12_TASK	<task number for AS ABAP PlugIn 12> (12. Create ABAP Company Address)
MX_HOOK13_TASK	<task number for AS ABAP PlugIn 13> (13. Modify ABAP Company Address)
MX_HOOK14_TASK	<task number for AS ABAP PlugIn 14> (14. Delete ABAP Company Address)
REPOSITORY_SYNC	SYNC
REPOSITORY_TYPE	DUALABAP

There are additional constants for configuring Secure Network Communications (SNC). For more information, see Appendix D: Configuring the ABAP Connector to use SNC.

Related Information

Appendix D: Configuring the ABAP Connector to Use SNC [page 167]

5.6 Repository Constants for a Dual-Stack System (Specific Application Server)

Repository Constants

Repository Wizard Field	Repository Constant	Value
AS ABAP User Name	JCO_CLIENT_USER	<user_ID>
AS ABAP Target Host	JCO_CLIENT_ASHOST	<hostname>
AS ABAP System Number	JCO_CLIENT_SYSNR	<system number>
AS ABAP Password	JCO_CLIENT_PASSWD	<password> For AS ABAP Release 4.6C, use upper-case.
AS ABAP Client	JCO_CLIENT_CLIENT	<client>
AS ABAP Language	JCO_CLIENT_LANG	<language ID>, for example, EN
AS Java HTTP Protocol	HTTP_PROTOCOL	<http/https>
AS Java Target Host	APPLICATION_HOST	<hostname>
AS Java HTTP Port	HTTP_PORT	<http_port>
AS Java User Name	HTTP_AUTH_USER	<user_ID>
AS Java Password	HTTP_AUTH_PWD	<password>
AS ABAP CUA System	CUA_MASTER	<TRUE/FALSE>
System privilege	SYSTEM_PRIVILEGE	PRIV:SYSTEM:<Repository> where <Repository> is the exact name of the repository to which the constants belongs.

The following constants are automatically created and therefore not visible in the wizard.

Additional Repository Constants

Repository Constant	Value
JCO_CLIENT_GROUP	<Group>, for example, Public

Repository Constant	Value
JCO_CLIENT_GWHOST	<gateway hostname> To find out the data for your Gateway, choose *Administration* > *System Administration* > *Monitor* > *System Monitoring* > *Gateway Monitor*. A list is displayed of all the SAP Gateways connected to your SAP System. Usually, an Gateway is assigned to each SAP application server and database server.
JCO_CLIENT_GWSERV	<gateway service> (for example, “sapgw00”)
JCO_CLIENT_MSHOST	<message_server_hostname>
JCO_CLIENT_R3NAME	<SID>
MX_ADD_MEMBER_TASK	<task number for Provisioning>
MX_DEL_MEMBER_TASK	<task number for Deprovisioning>
MX_MODIFYTASK	<task number for Modify>
MX_PRIV_GROUPING_ATTRIBUTE	MX_IS_ACCOUNT
MX_PRIV_GROUPING_RULE	P:4 With this value, entries are grouped if they have the same attribute defined in the repository constant MX_PRIV_GROUPING_ATTRIBUTE.
MX_HOOK1_TASK	<task number for AS ABAP PlugIn 1> (1. Create ABAP User)
MX_HOOK2_TASK	<task number for AS ABAP PlugIn 2> (2. Modify ABAP User)
MX_HOOK3_TASK	<task number for AS ABAP PlugIn 3> (3. Delete ABAP User)
MX_HOOK4_TASK	<task number for AS ABAP PlugIn 4> (4. Assign User Membership to ABAP)
MX_HOOK5_TASK	<task number for AS ABAP PlugIn 5> (5. Revoke User Membership to ABAP)
MX_HOOK6_TASK	<task number for AS ABAP PlugIn 6> (6. Enable ABAP User)

Repository Constant	Value
MX_HOOK7_TASK	<task number for AS ABAP PlugIn 7> (7. Disable ABAP User)
MX_HOOK8_TASK	<task number for AS ABAP PlugIn 8> (8. Set ABAP User Password)
MX_HOOK9_TASK	--None--
MX_HOOK10_TASK	<task number for AS ABAP PlugIn 10> (10. Create Group)
MX_HOOK11_TASK	<task number for AS ABAP PlugIn 11> (11. Delete Group)
MX_HOOK12_TASK	<task number for AS ABAP PlugIn 12> (12. Create ABAP Company Address)
MX_HOOK13_TASK	<task number for AS ABAP PlugIn 13> (13. Modify ABAP Company Address)
MX_HOOK14_TASK	<task number for AS ABAP PlugIn 14> (14. Delete ABAP Company Address)
REPOSITORY_SYNC	SYNC
REPOSITORY_TYPE	DUALABAP

There are additional constants for configuring Secure Network Communications (SNC). For more information, see Appendix D: Configuring the ABAP Connector to use SNC.

Related Information

Appendix D: Configuring the ABAP Connector to Use SNC [page 167]

5.7 Repository Constants for Business Suite AS ABAP (Load Balanced Connection)

Repository Constants

Repository Wizard Field	Repository Constant	Value
Message Server	JCO_CLIENT_MSHOST	<message_server_hostname>
System ID	JCO_CLIENT_R3NAME	<SID>
Logon Group	JCO_CLIENT_GROUP	<Group>, for example, Public
User Name	JCO_CLIENT_USER	<user_ID>
Password	JCO_CLIENT_PASSWD	<password> For AS ABAP Release 4.6C, use upper-case.
Client	JCO_CLIENT_CLIENT	<client>
Language	JCO_CLIENT_LANG	<language ID>, for example, EN
System privilege	SYSTEM_PRIVILEGE	PRIV:SYSTEM:<Repository> where <Repository> is the exact name of the repository to which the constants belongs.

The following constants are automatically created and therefore not visible in the wizard.

Additional Repository Constants

Repository Constant	Value
CUA_MASTER	<TRUE/FALSE>
JCO_CLIENT_ASHOST	<hostname>
JCO_CLIENT_GWHOST	<gateway hostname> To find out the data for your Gateway, choose *Administration* > *System Administration* > *Monitor* > *System Monitoring* > *Gateway Monitor*. A list is displayed of all the SAP Gateways connected to your SAP System. Usually, an Gateway is assigned to each SAP application server and database server.
JCO_CLIENT_GWSERV	<gateway service> (for example, “sapgw00”)

Repository Constant	Value
JCO_CLIENT_SYSNR	<system number>
NO_USER_ACCOUNT	0 Default value, this means that the connector creates ABAP users and business suite objects (for example, employees). If you do not want a user account created in the target system for an identity, set the value to 1.
MX_ADD_MEMBER_TASK	<task number for Provisioning>
MX_DEL_MEMBER_TASK	<task number for Deprovisioning>
MX_MODIFYTASK	<task number for Modify>
MX_PRIV_GROUPING_ATTRIBUTE	MX_IS_ACCOUNT
MX_PRIV_GROUPING_RULE	P:4 With this value, entries are grouped if they have the same attribute defined in the repository constant MX_PRIV_GROUPING_ATTRIBUTE.
MX_HOOK1_TASK	<task number for AS ABAP PlugIn 1> (1. Create ABAP User)
MX_HOOK2_TASK	<task number for AS ABAP PlugIn 2> (2. Modify ABAP User)
MX_HOOK3_TASK	<task number for AS ABAP PlugIn 3> (3. Delete ABAP User)
MX_HOOK4_TASK	<task number for AS ABAP PlugIn 4> (4. Assign User Membership to ABAP)
MX_HOOK5_TASK	<task number for AS ABAP PlugIn 5> (5. Revoke User Membership to ABAP)
MX_HOOK6_TASK	<task number for AS ABAP PlugIn 6> (6. Enable ABAP User)
MX_HOOK7_TASK	<task number for AS ABAP PlugIn 7> (7. Disable ABAP User)
MX_HOOK8_TASK	<task number for AS ABAP PlugIn 8> (8. Set ABAP User Password)

Repository Constant	Value
MX_HOOK9_TASK	--None--
MX_HOOK10_TASK	<task number for AS ABAP PlugIn 10> (10. Create Group)
MX_HOOK11_TASK	<task number for AS ABAP PlugIn 11> (11. Delete Group)
MX_HOOK12_TASK	<task number for AS ABAP PlugIn 12> (12. Create ABAP Company Address)
MX_HOOK13_TASK	<task number for AS ABAP PlugIn 13> (13. Modify ABAP Company Address)
MX_HOOK14_TASK	<task number for AS ABAP PlugIn 14> (14. Delete ABAP Company Address)
REPOSITORY_SYNC	SYNC
REPOSITORY_TYPE	ABAP

There are additional constants for configuring Secure Network Communications (SNC). For more information, see Appendix D: Configuring the ABAP Connector to use SNC.

Related Information

Appendix D: Configuring the ABAP Connector to Use SNC [page 167]

5.8 Repository Constants for SUN

Repository Constants

Repository Wizard Field	Repository Constant	Value
Host Name	LDAP_HOST	<hostname>
Starting Point	LDAP_STARTING_POINT	<LDAP starting point>
Starting Point, Groups	LDAP_STARTING_POINT_GROUPS	<LDAP starting point for groups>

Repository Wizard Field	Repository Constant	Value
Port number	LDAP_PORT	<LDAP port>
Login user	LDAP_LOGIN	<LDAP user ID>
Password	LDAP_PASSWORD	<password>
System privilege	SYSTEM_PRIVILEGE	PRIV:SYSTEM:<Repository> where <Repository> is the exact name of the repository to which the constants belongs.

The following constants are automatically created and therefore not visible in the wizard.

Additional Repository Constants

Repository Constant	Value
MX_ADD_MEMBER_TASK	<task number for Provisioning>
MX_DEL_MEMBER_TASK	<task number for Deprovisioning>
MX_MODIFYTASK	<task number for Modify>
MX_HOOK1_TASK	<task number for SUN PlugIn 1> (1. Create SUN user)
MX_HOOK2_TASK	<task number for SUN PlugIn 2> (2. Modify SUN user)
MX_HOOK3_TASK	<task number for SUN PlugIn 3> (3. Delete SUN user)
MX_HOOK4_TASK	<task number for SUN PlugIn 4> (4. Assign user membership to SUN Group)
MX_HOOK5_TASK	<task number for SUN PlugIn 5> (5. Revoke user membership from SUN Group)
MX_HOOK6_TASK	<task number for SUN PlugIn 6> (6. Enable SUN User)
MX_HOOK7_TASK	<task number for SUN PlugIn 7> (7. Disable SUN User)
MX_HOOK8_TASK	<task number for SUN PlugIn 8> (8. Set SUN User password)

Repository Constant	Value
MX_HOOK9_TASK	--None--
MX_HOOK10_TASK	<task number for SUN PlugIn 10> (10. Create SUN Group)
MX_HOOK11_TASK	<task number for SUN PlugIn 11> (11. Delete SUN Group)
REPOSITORY_SYNC	SYNC
REPOSITORY_TYPE	SUN

5.9 Repository Constants for Active Directory for Provisioning Framework

Mandatory Repository Constants

Repository Wizard Field	Repository Constant	Value
Host name of ADS	LDAP_HOST	<Host name of ADS>
Starting point users	LDAP_STARTING_POINT	<LDAP starting point>
Starting point groups	LDAP_STARTING_POINT_GROUPS	<LDAP starting point for groups>
Port number	LDAP_PORT	<LDAP port>
SSL Port number	LDAP_PORT_SSL	<LDAP port> An SSL connection is used for password provisioning.[1] For password provisioning SSL must be set up.
Login user	LDAP_LOGIN	<LDAP user ID>
Password	LDAP_PASSWORD	<password>
System privilege	SYSTEM_PRIVILEGE	PRIV:SYSTEM:<Repository> where <Repository> is the exact name of the repository to which the constants belongs.

1

To set up an SSL/TLS secured connection between the Active Directory Server and the Identity Center, you set this constant to the repository value of the Active Directory Server and install the necessary certificates. For more

information, see section *7.4. Identity Center: SSL Security* of the *SAP NetWeaver Identity Management Security Guide*.

To not set a password when creating a user in the Active Directory repository, choose *Provisioning Framework* > *CONNECTORS* > *AD Connector* > *Plugins* > *1 Create AD User* > *Set password*. Uncheck the *Enabled* flag on the *Options* tab.

To not provision a modified password to the Active Directory repository any more, choose *AD Repositories* > *<Active_Directory_Repository>* > *Constants* > *MX_HOOK8_TASK*. Set the value for this constant to *--None--*.

Optional Repository Constants

Repository Constant	Value	Comment
LDAP_MAIL_DOMAIN	<Mail domain>	
LDAP_UPN	<LDAP UPN>	
EXCHANGE_VERSION	<empty> Exchange20 10 or Exchange20 07	By setting any value for this attribute, you define whether existing ADS users are assigned further attributes for using Exchange. That is, you activate the use of Exchange provisioning. You also indicate your Exchange version.
LDAP_TEMPLATE_MAILBOX		The distinguished name of the template mailbox, e.g. CN=Template1,CN=Users,DC=ex2k7 ,DC=dom
LDAP_TEMPLATE_MAILBOX_ATTRIBUTES_2007	<Template mailbox attributes for Exchange 2007>	
LDAP_TEMPLATE_MAILBOX_ATTRIBUTES_2010	<Template mailbox attributes for Exchange 2010>	

The above constants are only necessary if you want to create or change Exchange mailboxes.

The following constants are automatically created and therefore not visible in the wizard.

Additional Repository Constants

Repository Constant	Value
LDAP_FILTER	(objectclass=person)
LDAP_FILTER_GROUPS	(objectclass=group)
MX_ADD_MEMBER_TASK	<task number for Provisioning>
MX_DEL_MEMBER_TASK	<task number for Deprovisioning>
MX_MODIFYTASK	<task number for Modify>

Repository Constant	Value
MX_HOOK1_TASK	<task number for AD PlugIn 1> (1 Create AD User)
MX_HOOK2_TASK	<task number for AD PlugIn 2> (2 Modify AD User)
MX_HOOK3_TASK	<task number for AD PlugIn 3> (3 Delete AD User)
MX_HOOK4_TASK	<task number for AD PlugIn 4> (4 Assign User Membership to AD Group)
MX_HOOK5_TASK	<task number for AD PlugIn 5> (5 Revoke User Membership from AD group)
MX_HOOK6_TASK	<task number for AD PlugIn 6> (6 Enable AD User)
MX_HOOK7_TASK	<task number for AD PlugIn 7> (7 Disable AD User)
MX_HOOK8_TASK	<task number for AD PlugIn 8> (8 Set AD User Password)
MX_HOOK9_TASK	--None--
MX_HOOK10_TASK	<task number for AD PlugIn 10> (10 Create AD Group)
MX_HOOK11_TASK	<task number for AD PlugIn 11> (11 Delete AD Group)
REPOSITORY_SYNC	SYNC
REPOSITORY_TYPE	LDAP

Related Information

SAP NetWeaver Identity Management 7.2 Documentation > *Security Guide*

5.10 Repository Constants for SAP HANA Database

Mandatory Repository Constants

Repository Wizard Field	Repository Constant	Value
Host Name	IMDB_HOSTNAME	< Host name of the SAP HANA database server>
Port	IMDB_PORT	< Port number of the SAP HANA database server> Usually 30015 + instance number * 100, for example, 32015 for instance number 20.>
User Name	IMDB_USER	< User ID> for authentication to the SAP HANA database
Password	IMDB_PASSWORD	<password> for authentication to the SAP HANA database
System privilege	SYSTEM_PRIVILEGE	PRIV:SYSTEM:<Repository> where <Repository> is the exact name of the repository to which the constants belongs.

Optional Repository Constants

Repository Wizard Field	Repository Constant	Value
SSL/TLS Encryption	IMDB_SSL_ENCRYPT	Switch for encryption of the connection to the SAP HANA database. Default: disabled

The following constants are automatically created and therefore not visible in the wizard.

Additional Repository Constants

Repository Constant	Value
IMDB_ADDITIONAL_JDBC_PARAMS	<empty> For experts: You may add special JDBC parameters here if there are no other repository constants that you can use for the required purpose.

Repository Constant	Value
IMDB_JDBC_DRIVER	Class name of the JDBC driver for the SAP HANA database Usually the driver is delivered as part of the SAP HANA database with the `ngdbc.jar` file. Default value: *com.sap.db.jdbc.Driver* **⚠ Caution** Because this file is necessary for the dispatchers, you have to define it as a classpath extension. For example, in the Microsoft Management Console (MMC) choose *Tools* > *Options* > *Java* and add the path to the `ngdbc.jar` file in the *Classpath extensions* field.
IMDB_SSL_KEYSTORE	<empty> Keystore for private keys, used for X.509 client certificate authentication. Keystore name or path to keystore file. Default value: VM default.
IMDB_SSL_KEYSTORE_PASSWORD	<empty> Keystore password, related to IMDB_SSL_KEYSTORE. Default value: VM default
IMDB_SSL_KEYSTORE_TYPE	<empty> Keystore type, related to IMDB_SSL_KEYSTORE. Default value: VM default
IMDB_SSL_TRUSTSTORE	<empty> Keystore for trusted certificates, used for verification of server and CA certificates. Keystore name or path to keystore file. Default value: VM defaul
IMDB_SSL_TRUSTSTORE_PASSWORD	<empty> Keystore password, related to IMDB_SSL_TRUSTSTORE. Default value: VM default
IMDB_SSL_TRUSTSTORE_TYPE	<empty> Keystore type, related to IMDB_SSL_TRUSTSTORE. Default value: VM default
MX_ADD_MEMBER_TASK	<task number for Provisioning>
MX_DEL_MEMBER_TASK	<task number for Deprovisioning>
MX_MODIFYTASK	<task number for Modify>

Repository Constant	Value
MX_PRIV_GROUPING_ATTRIBUTE	MX_PRIVILEGE_TYPE
MX_PRIV_GROUPING_RULE	P:5 With this value, entries are grouped together if they have the same attribute defined in the repository constant MX_PRIV_GROUPING_ATTRIBUTE and if they are of the same operation type, for example, add or remove.
MX_HOOK1_TASK	<task number for SAP HANA database PlugIn 1> (1. Create SAP HANA database User)
MX_HOOK2_TASK	<task number for SAP HANA database PlugIn 2> (2. Modify SAP HANA database User) The SAP HANA database does not support the modify task. Therefore, a dummy task is used to add a log entry detailing that the modify task is not supported.
MX_HOOK3_TASK	<task number for SAP HANA database PlugIn 3> (3. Delete SAP HANA database User)
MX_HOOK4_TASK	<task number for SAP HANA database PlugIn 4> (4. Assign User Membership to SAP HANA database Role)
MX_HOOK5_TASK	<task number for SAP HANA database PlugIn 5> (5. Revoke User Membership to SAP HANA database Role)
MX_HOOK6_TASK	<task number for SAP HANA database PlugIn 6> (6 Enable SAP HANA database User) The SAP HANA database supports this feature as of SAP HANA 1.5 SPS 4.
MX_HOOK7_TASK	<task number for SAP HANA database PlugIn 7> (7 Disable SAP HANA database User) The SAP HANA database supports this feature as of SAP HANA 1.5 SPS 4.
MX_HOOK8_TASK	<task number for SAP HANA database PlugIn 8> (8. Set SAP HANA database User password)
MX_HOOK9_TASK	--None--
MX_HOOK10_TASK	--None--
MX_HOOK11_TASK	--None--

Repository Constant	Value
REPOSITORY_SYNC	SYNC
REPOSITORY_TYPE	SAP_IN_MEMORY_DB

6 Appendix B: Mapping Between Identity Center and AS ABAP Attributes

The following table shows the ABAP attributes that are supported by the ABAP connector and how they are mapped to attributes in the Identity Center.

> **Note**
>
> Attributes that are new to Release 7.1 or 7.2 are indicated accordingly.

Attribute Mapping

IC Attribute	Java (SPML) Attribute	ABAP Connector Attribute	BAPI Parameter	BAPI Field	HR Field	LDAP Mapping to InetOrgPerson
DISPLAYNAME	displayname	Displayname	ADDRESS	FULLNAME	P0001-ENAME	cn
MSKEYVALUE	logonname	logonuid	USERNAME		SYHR_A_P0105_AF_SYS UNAME	
MX_ACADEMIC_TITLE_1		AddressTitleAca1	ADDRESS	TITLE_ACA1	TEXT_P0002-TITEL	title
MX_ACADEMIC_TITLE_2		AddressTitleAca2	ADDRESS	TITLE_ACA2		
MX_ACCESSIBILITYLEVEL		WebAccessibility				
MX_ACCOUNTING_NUMBER		LogondataAccnt	LOGONDATA	ACCNT		
MX_ADDRESS_BUILDING		AddressBuildLong	ADDRESS	BUILD_LONG		
MX_ADDRESS_CHECKSTATUS			ADDRESS	CHCKSTATUS		
MX_ADDRESS_CITY			ADDRESS	CITY	WORKCENTER_CITY	l

IC Attribute	Java (SPML) Attribute	ABAP Connector Attribute	BAPI Parameter	BAPI Field	HR Field	LDAP Mapping to InetOrgPerson
MX_ADDRESS_CITY_NO			ADDRESS	CITY_NO		
MX_ADDRESS_CO_NAME		AddressCOName	ADDRESS	C_O_NAME		
MX_ADDRESS_COMPANY_POSTAL_CODE		AddressPostlCod3	ADDRESS	POSTL_COD3	WORKCENTER_POSTCODE	
MX_ADDRESS_COUNTRY		AddressCountry	ADDRESS	COUNTRY	WORKCENTER_COUNTR Y	
MX_ADDRESS_DIFFERENT_CITY		AddressHomeCity	ADDRESS	HOME_CITY		
MX_ADDRESS_DIFFERENT_CITY_ NO		AddressHomecityno	ADDRESS	HOMECITYNO		
MX_ADDRESS_DISTRICT		AddressDistrict	ADDRESS	DISTRICT		
MX_ADDRESS_DISTRICT_NO		AddressDistrictNo	ADDRESS	DISTRICT_NO		
MX_ADDRESS_FLOOR		AddressFloor	ADDRESS	FLOOR		
MX_ADDRESS_HOUSE_NO		AddressHouseNo	ADDRESS	HOUSE_NO		
MX_ADDRESS_HOUSE_NO_SUPPLEMENT		AddressHouseNo2	ADDRESS	HOUSE_NO2		

IC Attribute	Java (SPML) Attribute	ABAP Connector Attribute	BAPI Parameter	BAPI Field	HR Field	LDAP Mapping to InetOrgPerson
MX_ADDRESS_LANGUAGE		AddresssLangulSO	ADDRESS	LANGUISO		
MX_ADDRESS_NAME_1		AddressName	ADDRESS	NAME		
MX_ADDRESS_NAME_2		AddressName2	ADDRESS	NAME_2		
MX_ADDRESS_NAME_3		AddressName3	ADDRESS	NAME_3		
MX_ADDRESS_NAME_4		AddressName4	ADDRESS	NAME_4		
MX_ADDRESS_NOTES		AddressAdrNotes	ADDRESS	ADR_NOTES		
MX_ADDRESS_POBOX		AddressPoBox	ADDRESS	PO_BOX		postofficebox
MX_ADDRESS_POBOX_CITY		AddressPoBoxCit	ADDRESS	PO_BOX_CIT		
MX_ADDRESS_POBOX_COUNTRY		AddressPoboxCtry	ADDRESS	POBOX_CTRY		
MX_ADDRESS_POBOX_POSTAL_CO DE		AddressPostlCod2	ADDRESS	POSTL_COD2		
MX_ADDRESS_POBOX_REGION		AddressPoBoxReg	ADDRESS	REGION		

IC Attribute	Java (SPML) Attribute	ABAP Connector Attribute	BAPI Parameter	BAPI Field	HR Field	LDAP Mapping to InetOrgPerson
MX_ADDRESS_POBOX_WITHOUT_N UMBER		AddressPoWONo	ADDRESS	PO_W_O_NO		
MX_ADDRESS_POSTAL_CODE		AddressPostlCod1	ADDRESS		postalcode	
MX_ADDRESS_REASON_DONT_USE _POBOX_ADDRESS		AddressDontUseP	ADDRESS	DONT_USE_P		
MX_ADDRESS_REASON_DONT_USE _STREET_ADDRESS		AddressDontUseS	ADDRESS	DONT_USE_S		
MX_ADDRESS_REGION		AddressRegion	ADDRESS	REGION		
MX_ADDRESS_REGION_GROUP		AddressRegiogroup	ADDRESS	REGIOGROUP		
MX_ADDRESS_ROOM_NO		AddressRoomNo	ADDRESS	ROOM_NO		
MX_ADDRESS_STREET_1		AddressStreet	ADDRESS	STREET		
MX_ADDRESS_STREET_2		AddressStrSuppl1	ADDRESS	STR_SUPPL1		
MX_ADDRESS_STREET_3		AddressStrSuppl2	ADDRESS	STR_SUPPL2		

IC Attribute	Java (SPML) Attribute	ABAP Connector Attribute	BAPI Parameter	BAPI Field	HR Field	LDAP Mapping to InetOrgPerson
MX_ADDRESS_STREET_4		AddressStrSuppl3	ADDRESS	STR_SUPPL3		
MX_ADDRESS_STREET_5		AddressLocation	ADDRESS	LOCATION		
MX_ADDRESS_STREET_NO		AddressStreetNo	ADDRESS	STREET_NO		
MX_ADDRESS_STREETADDRESS					WORKCENTER_STREET	street
MX_ADDRESS_TAX_JURISDICTION_CODE		AddressTaxjurcode	ADDRESS	TAXJURCODE		
MX_ADDRESS_TIME_ZONE		AddressTimeZone	ADDRESS	TIME_ZONE		
MX_ADDRESS_TITLE		AddressTitle	ADDRESS	TITLE		
MX_ADDRESS_TRANSPORT_ZONE		AddressTranspzone	ADDRESS	TRANSPZONE		
MX_ADMIN_UNIT		companyid	LOGONDATA	CLASS		
MX_BIRTHNAME		AddressBirthName	ADDRESS	BIRTH_NAME		
MX_CATT_TEST_STATUS		DefaultsCattkennz	DEFAULTS	CATTKENNZ		
MX_CERTIFICATE						usercertificate
MX_COMMUNICATION_LANGUAGE		AddressLanguPISO	ADDRESS	LANGUP_ISO		

IC Attribute	Java (SPML) Attribute	ABAP Connector Attribute	BAPI Parameter	BAPI Field	HR Field	LDAP Mapping to InetOrgPerson
MX_COMMUNICATION_METHOD		AddressCommType	ADDRESS	COMM_TYPE		
MX_COSTCENTER		DefaultCostcenter	DEFAULTS	KOSTL		
MX_DATEFORMAT		dateformat	DEFAULTS	DATFM		
MX_DEPARTMENT		department	ADDRESS	DEPARTMENT	P0001_ORGEH_TL	ou
MX_ENCRYPTED_PASSWORD (7.2)		password				
MX_FAX_ADDITIONAL		additionalFaxes	ADDFAX			
MX_FAX_PRIMARY	fax	primaryFax	ADDFAX		SYHR_A_P0105_AF_FAX	facsimiletelephonenumber
MX_FIRSTNAME	firstname	firstname	ADDRESS	FIRSTNAME	P0002-VORNA	givenname
MX_HCM_SYSUNAME (7.1)					SYHR_A_P0105_AF_SYS UNAME	
MX_IDENTITYUUID (7.2)		identityuuid	IDENTITY	IDENTITY_UUID		
MX_INHOUSE_MAIL		AddressInhouseMl	ADDRESS	INHOUSE_ML		
MX_INITIALS		AddressInitials	ADDRESS	INITIALS		initials
MX_LANGUAGE		locale	DEFAULTS	LANGU	P0002-SPRSL	preferredlanguage
MX_LASTNAME		lastname	ADDRESS	LASTNAME	P0002-NACHN	sn

IC Attribute	Java (SPML) Attribute	ABAP Connector Attribute	BAPI Parameter	BAPI Field	HR Field	LDAP Mapping to InetOrgPerson
MX_LASTMODTIME (7.1 SP 5)			LASTMODIFIED	MODDATE		
MX_LASTMODIFIER (7.1 SP 5)			LASTMODIFIED	MODIFIER		
To be defined		UClassBnameChargeable	UCLASS	BNAME_CHARGEABLE		
To be defined		UClassClient	UCLASS	CLIENT		
To be defined		UClassCountrySurcharge	UCLASS	COUNTRY_SURCHARGE		
To be defined		UClassLicType	UCLASS	LIC_TYPE		
To be defined		UClassSpecVers	UCLASS	SPEC_VERS		
To be defined		UClassSubstituteFrom	UCLASS	SUBSTITUTE_FROM		
To be defined		UClassSubstituteUntil	UCLASS	SYSID		
To be defined		UClassSysid	UCLASS	SYSID		
To be defined			UCLASSSYS	RCVSYSTEM		
To be defined		UClasssysBnameChargeable	UCLASSSYS	BNAME_CHARGEABLE		
To be defined		UClasssysClient	UCLASSSYS	CLIENT		
To be defined		UClasssysCountrySurcharge	UCLASSSYS	COUNTRY_SURCHARGE		
To be defined		UClasssysLicType	UCLASSSYS	LIC_TYPE		
To be defined		UClasssysSpecVers	UCLASSSYS	SPEC_VERS		

IC Attribute	Java (SPML) Attribute	ABAP Connector Attribute	BAPI Parameter	BAPI Field	HR Field	LDAP Mapping to InetOrgPerson
To be defined		UClasssysSubstituteFrom	UCLASSSYS	SUBSTITUTE_FROM		
To be defined		UClasssysSubstituteUntil	UCLASSSYS	SUBSTITUTE_UNTIL		
To be defined		UClasssysSysid	UCLASSSYS	SYSID		
MX_LOCKED	islocked	islocked	ISLOCKED	LOCAL_LOCK		
MX_LOGONALIAS		useralias	ALIAS	USERALIAS		
MX_MAIL_ADDITIONAL		additionalMails	ADDSMTP		SYHR_A_P0105_AF_EMAIL	
MX_MAIL_PRIMARY	email	primaryMail	ADDSMTP		SYHR_A_P0105_AF_EMAIL	mail
MX_MIDDLENAME		AddressMiddlename	ADDRESS	MIDDLENAME	P0002-MIDNM	
MX_MOBILE_ADDITIONAL		additionalMobiles	ADDTEL			
MX_MOBILE_PRIMARY	mobile	primaryMobile	ADDTEL		SYHR_A_P0105_AF_CEL L	mobile
MX_NAMCOUNTRY (7.1)		AddressNamCountry	ADDRESS	NAMCOUNTRY		
MX_NAME_ABBREVIATION		AddressInitsSig	ADDRESS	NITS_SIG		
MX_NAME_PREFIX_1		AddressPrefix1	ADDRESS	PREFIX1		
MX_NAME_PREFIX_2		AddressPrefix2	ADDRESS	PREFIX2		
MX_NAMEFORMAT (7.1)			ADDRESS	NAMEFORMAT		
MX_NICKNAME		AddressNickname	ADDRESS	NICKNAME		

IC Attribute	Java (SPML) Attribute	ABAP Connector Attribute	BAPI Parameter	BAPI Field	HR Field	LDAP Mapping to InetOrgPerson
MX_NUMBERFORMAT		Numberformat	DEFAULTS	DCPFM		
MX_PAGER_ADDITIONAL		additionalPagers	ADDRESS			pager
MX_PAGER_PRIMARY		primaryPager	ADDPAG			
MX_PARAMETER (7.1)			PARAMETER1	PARID, PARVA		
MX_PASSWORD	password	password	PASSWORD	BAPIPWD		userpassword
MX_PASSWORD_DISABLED Mapping only applies to Initial Load and other usages of FromSAP/FromSAPIdentity passes (BAPI_USER_GET_LIST).	ispassworddisabled	Ispassworddisabled	ISLOCKED	NO_USER_PW		
MX_PERSONUUID (7.2)		personuuid	IDENTITY	BPPERSON		
MX_PHONE_ADDITIONAL		additionalPhones	ADDTEL			homephone
MX_PHONE_PRIMARY	telephone	primaryPhone	ADDTEL		SYHR_A_P0105_AF_TEL_NR + SYHR_A_P0105_AF_TEL _EXT	telephonenumber
MX_PRINTERSETTINGS_SPDA		DefaultsSpda	DEFAULTS	SPDA		
MX_PRINTERSETTINGS_SPDB		DefaultsSpdb	DEFAULTS	SPDB		

IC Attribute	Java (SPML) Attribute	ABAP Connector Attribute	BAPI Parameter	BAPI Field	HR Field	LDAP Mapping to InetOrgPerson
MX_PRINTER-SET-TINGS_SPLD		DefaultsSpld	DEFAULTS	SPLD		
MX_PRINTER-SET-TINGS_SPLG		DefaultsSplg	DEFAULTS	SPLG		
MX_PRT_ADDI-TIONAL (7.2)		additionalPRT	ADDPRT			
MX_REFER-ENCE_USER		ReferenceUser	REF_USER	REF_USER		
MX_RML_ADDI-TIONAL (7.1 SP 5)			ADDRML			
MX_RML_PRI-MARY (7.2)		primaryRML	ADDRML			
MX_SALUTA-TION		salutation	ADDRESS	TITLE_P	T522T-ANRLT	
MX_SEARCH_T ERM_1		AddressSort1P	ADDRESS	SORT1_P		
MX_SEARCH_T ERM_2		AddressSort2P	ADDRESS	SORT2_P		
MX_SECOND-NAME		AddressSe-condname	ADDRESS	SECONDNAME		
MX_SNC_FLAG		SNCFlag	SNC	GUIFLAG		
MX_SNC_NAME		SNCName	SNC	PNAME		
MX_SSF_ADDI-TIONAL (7.2)		additionISSF	ADDSSF			
MX_SSF_PRI-MARY (7.2)		primarySSF		ADDSSF		

IC Attribute	Java (SPML) Attribute	ABAP Connector Attribute	BAPI Parameter	BAPI Field	HR Field	LDAP Mapping to InetOrgPerson
MX_START_MENU (7.1)		DefaultsStartMenu	DEFAULTS	START_MENU		
MX_TIMEFORMAT (7.1 SP 5)			DEFAULTS	TIMEFM		
MX_TIMEFORMAT (7.2)		timeformat	DEFAULTS	TIMEFM		
MX_TIMEZONE	timezone	timezone	LOGONDATA	TZONE		
MX_TITLE_SUPPLEMENT		AddressTitleSppl	ADDRESS	TITLE_SPPL		
MX_TLX_ADDITIONAL (7.2)		additionalTLX	ADDTLZ			
MX_TLX_PRIMARY (7.2)		primaryTLX	ADDTLX			
MX_TTX_PRIMARY (7.2)		primaryTTX	ADDTTX			
MX_TTX_ADDITIONAL (7.2)		additionalTTX	ADDTTX			
MX_URI_ADDITIONAL (7.1 SP 5)		additionalURI	ADDURI			
MX_URI_PRIMARY (7.2)		primaryURI	ADDURI			
MX_USER_CATEGORY (7.1)		groups	GROUPS	USERGROUP		
MX_USERTYPE		securitypolicy	LOGONDATA	USTYP		
MX_VALIDFROM	validfrom	validfrom	LOGONDATA	GLTGV		
MX_VALIDTO	validto	validto	LOGONDATA	GLTGB		
MX_WORKPLACE_BUILDING		AddressBuildingP	ADDRESS	BUILDING_P	TEXT_P8001_BUILD	

IC Attribute	Java (SPML) Attribute	ABAP Connector Attribute	BAPI Parameter	BAPI Field	HR Field	LDAP Mapping to InetOrgPerson
MX_WORKPLACE_FLOOR		AddressFloorP	ADDRESS	FLOOR_P		
MX_WORKPLACE_FUNCTION		jobfunction	ADDRESS	FUNCTION	P0001_PLANS_TL	
MX_WORKPLACE_ROOM		AddressRoomNoP	ADDRESS	ROOM_NO_P	WORKCENTER_ROOM	
MX_X400_ADDITIONAL (7.2)		additionalX400	ADDX400			
MX_X400_PRIMARY (7.2)		primaryX400	ADDX400			
MXREF_MX_COMPANY_ADDRESS		Company	COMPANY	COMPANY		
MXREF_MX_PRIVILEGE		roles	ACTIVITYGROUPS	AGR_NAME		
MXREF_MX_PRIVILEGE		profiles	profiles	BAPIPROF		

6.1 Additional Mapping Attributes for Enhanced SAP Business Suite Integration

The following table shows additional attributes that are used for the enhanced SAP Business Suite integration use case. These attributes are used as parameters for the Business Add-In (BAdI) implementations that apply to the specific integration scenario, for example, Customer Relationship Management (CRM). Attributes that are explicitly used for the SAP Business Suite applications are indicated as such in the Identity Center schema using the prefix MX_FS so that they can be recognized and provisioned accordingly.

For example, the SAP HCM attribute PERNR is mapped to MX_FS_PERSONNEL_NUMBER in the Identity Center schema.

Additional Attributes

IC Attribute	Short Description	Source System	Source Attribute Name (for example, DDIC Data Element)	BAdI Parameter Name
DISPLAYNAME	Formatted Name of Employee or Applicant	SAP HCM	P0001-ENAME	ADDRESS-FULLNAME
MX_ACADEMIC_TITLE_1	Academic Title Text	SAP HCM	TEXT_P0002_TITLE	ADDRESS-TITLE_ACA1
MX_ADDRESS_STREETADDRESS	Street	SAP HCM	P8001-STRAS	ADDRESS-STREET (AD_STREET)
MX_ADDRESS_CITY	City	SAP HCM	P8001-ORT01	ADDRESS-CITY (AD_CITY1)
MX_ADDRESS_COUNTRY	Country	SAP HCM		ADDRESS-COUNTRYISO
MX_FIRSTNAME	First Name	SAP HCM	P0002-VORN	ADDRESS-FIRSTNAME
MX_FS__POSITION_ID	Position	SAP HCM	P0001-PLANS	POSITION_ID
MX_FS_ACADEMIC_TITLE_1_ID	Academic Title	SAP HCM	P0002-TITLE	ACADEMIC_TITLE_1_ID
MX_FS_BP_PERSON_ID	Business Partner (Person)		SYSUUID	BP_PERSON_ID
MX_FS_BUSINESS_AREA	Business Area Text	SAP HCM	TEXT_P0001_GSBER	BUSINESS_AREA
MX_FS_BUSINESS_AREA_ID	Business Area	SAP HCM	P0001-GSBER	BUSINESS_AREA_ID
MX_FS_CENTRALPERSON_ID	Central Person (CP)	SAP HCM	OBJID (char 10)	CENTRALPERSON_ID
MX_FS_COMPANY_CODE	Company Code Text	SAP HCM	TEXT_P0001-BUKRS	COMPANY_CODE
MX_FS_COMPANY_CODE_ID	Company Code	SAP HCM	P0001-BUKRS	COMPANY_CODE_ID
MX_FS_COST_CENTER	Text Cost Center	SAP HCM	TEXT_P0001-KOSTL	COST_CENTER
MX_FS_COST_CENTER_ID	Cost Center	SAP HCM / SAP NetWeaver	P0001-KOSTL	COST_CENTER_ID
MX_FS_EMPLOYEE_GROUP	Employee Group Text	SAP HCM	TEXT_P0001_PERSG	EMPLOYEE_GROUP

IC Attribute	Short Description	Source System	Source Attribute Name (for example, DDIC Data Element)	BAdI Parameter Name
MX_FS_EM-PLOYEE_GROUP_ID	Employee Group	SAP HCM	P0001-PERSG	EMPLOYEE_GROUP_ID
MX_FS_EM-PLOYEE_SUBGROUP	Employee Sub-group_Text	SAP HCM	TEXT_P0001_PERSK	EMPLOYEE_SUB-GROUP
MX_FS_EM-PLOYEE_SUBGROUP _ID	Employee Subgroup	SAP HCM	P0001-PERSK	EMPLOYEE_SUB-GROUP_ID
MX_FS_EMPLOY-MENT_STATUS _ID	Employment Status	SAP HCM	P0000-STAT2	EMPLOYMENT_STA-TUS_ID
MX_FS_EMPLOY-MENT_STATUS	Employment Status Text	SAP HCM	TEXT_P0000_STAT2	EMPLOYMENT_STA-TUS
MX_FS_IDEN-TITY_TYPE	Type of Identity			IDENTITY _TYPE
MX_FS_JOB	Job Text	SAP HCM	P0001_STELL_TL	JOB
MX_FS_JOB_ID	Job	SAP HCM	P0001-STELL	JOB_ID
MX_FS_ORGANIZA-TIONAL_UN IT	Organizational Unit Text	SAP HCM	P0001_ORGEH_TL	ORGANIZA-TIONAL_UNIT
MX_FS_ORGANIZA-TIONAL_UN IT_ID	Organizational Unit	SAP HCM	P0001-ORGEH	ORGANIZA-TIONAL_UNIT_ID
MX_FS_PERNR_IS_MA NAGER	PERNR_IS_MAN AGER	SAP HCM		PERNR_IS_MANAGER
MX_FS_PERSON-NEL_AREA	Personnel Area Text	SAP HCM	TEXT_P0001_WERKS	PERSONNEL_AREA
MX_FS_PERSON-NEL_AREA_ID	Personnel Area	SAP HCM	P0001-WERKS	PERSONNEL_AREA_ID
MX_FS_PERSON-NEL_NUMBER	Personnel number	SAP HCM	PERNR	PERSONNEL_NUMBER
MX_FS_PERSON-NEL_NUMBER_ OF_MANAGER	Personnel Number of nextlevel manager	SAP HCM	PERNR_OF_MANAGER	PERSONNEL_NUM-BER_OF_M ANAGER
MX_FS_PERSON-NEL_SUBAREA	Personnel Subarea Text	SAP HCM	TEXT_P0001_BTRTL	PERSONNEL_SUB-AREA

IC Attribute	Short Description	Source System	Source Attribute Name (for example, DDIC Data Element)	BAdI Parameter Name
MX_FS_PERSON-NEL_SUBAREA _ID	Personnel Subarea	SAP HCM	P0001-BTRTL	PERSONNEL_SUB-AREA_ID
MX_FS_POSITION	Position Text	SAP HCM	P0001_PLANS_TL	POSITION
MX_FS_POSITION_ID (7.2)	Position	SAP HCM	P0001-PLANS	
MX_FS_SALUTA-TION_ID	Form-of-Address Key	SAP HCM	P0002-ANRED	SALUTATION_ID
MX_FS_SCMEWM_PRR _ID	EWM Processor	EWM	/SCMB/DE_PRR	SCMEWM_PRR_ID
MX_FS_SCMSNC_BP_ ORG_ID	SNC Business Partner (Organization)	SCM, SNC	SYSUUID	SCMSNC_BP_ORG_ID
MX_FS_SCMSNC_VISI-BILITY _PROFILE	SNC Visibility Profile	IDM		SCMSNC_VISIBIL-ITY_PROFILE
MX_FS_SCMTMS_BP_ ORG_ID	TM TSP (Organization Business Partner)	SCM TM	SYSUUID or BP Num-ber	SCMTMS_BP_ORG_ID
MX_FS_SOURCE_SYS-TEM	SourceSystem	SAP NetWeaver	SY-SYSID+ SY-MANDT	SOURCE_SYSTEM
MX_FS_WORK_CON-TRACT	Contract Text	SAP HCM	TEXT_P0001_ANSVH	WORK_CONTRACT
MX_FS_WORK_CON-TRACT_ID	Contract (in CE mode, should be renamed to Personnel Assignment)	SAP HCM	P0001-ANSVH	WORK_CONTRACT_ID
MX_HCM_SYSUNAME	System user	SAP HCM	P0105_AF-SYSUNAME	
MX_LANGUAGE	Language	SAP HCM	P0002-SPRSL	DEFAULTS-LANGU
MX_LASTNAME	Last Name	SAP HCM	P0002-NACHN	ADDRESS-LASTNAME
MX_MAIL_PRIMARY or MX_MAIL_ADDI-TIONAL	E-Mail	SAP HCM or IDM	P0105_AF-EMAIL	ADDRESS-E_MAIL or table ADDSMTP
MX_MOBILE_PRIMARY	Cell Phone	SAP HCM	P0105_AF-CELL	List of numbers in table ADDTEL

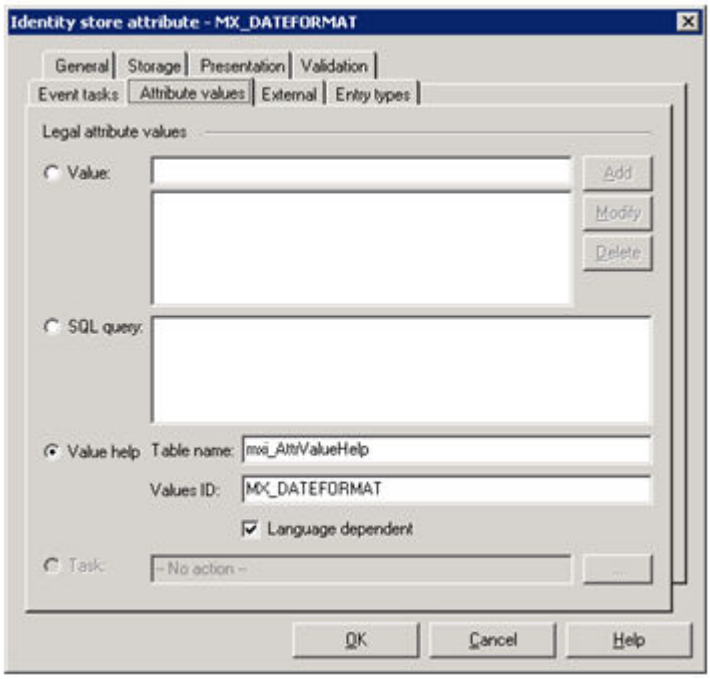
IC Attribute	Short Description	Source System	Source Attribute Name (for example, DDIC Data Element)	BAdI Parameter Name
MX_PHONE_PRIMARY or MX_PHONE_ADDITIONAL	Phone	SAP HCM	P0105_AF-TEL_NR + P0105_AF-TEL_EXT	ADDRESS-TEL1_NUMBR (First telephone no.: dialing code+number) ADDRESS-TEL1_EXT (First Telephone No.: Extension) or list of numbers in table ADDTEL
MX_WORKPLACE_ROOM	Room Number	SAP HCM	P1028-ROOM1 (P8001-ROOM1)	ADDRESS-ROOM_NO_P
MX_SALUTATION	Form-of-Address Text	SAP HCM	TEXT_P0002_ANRED	ADDRESS-TITLE_P
MX_WORKPLACE_BUILDING	Building Number	SAP HCM	P1028-BUILDING (P8001-BUILDING)	ADDRESS-BUILDING_P

7 Appendix C: Attributes that Support Value Help

Attributes

Identity Center Attribute	Value Help Content	Modifiable / To be Read from AS ABAP	Language Dependency
MX_DATEFORMAT	Fixed (Delivered with the provisioning framework)	N	Y
MX_LANGUAGE	Fixed (Delivered with the provisioning framework)	N	Y
MX_LANGUAGE_COUNTRY	Fixed (Delivered with the provisioning framework)	N	Y
MX_NUMBERFORMAT	Fixed (Delivered with the provisioning framework)	N	Y
MX_TIMEZONE	Fixed (Delivered with the provisioning framework)	N	Y
MX_USERTYPE	Fixed (Delivered with the provisioning framework)	N	Y
MX_ACADEMIC_TITLE_1	Tables TSAD2 and TSAD2T	Y	N
MX_ACADEMIC_TITLE_2	Tables TSAD2 and TSAD2T	Y	N
MX_ADMIN_UNIT	Tables USGRP and USGRPT	Y	N
MX_NAME_PREFIX_1	Table TSAD4	Y	N
MX_NAME_PREFIX_2	Table TSAD4	Y	N
MX_PRINTERSET-TINGS_SPLD	Table TSP03	Y	N
MX_SALUTATION	Tables TSAD3 and TSAD3T	Y	N
MX_TITLE_SUPPLEMENT	Tables TSAD5 and TSAD5T	Y	N
MX_USER_CATEGORY	Tables USGRP and USGRPT	Y	N

The value help content is stored in the `mxi_AttrValueHelp` database table, which is specified in the attribute value properties. See the example below for the MX_DATEFORMAT attribute.



See also *Reading Value Help Content*.

Related Information

Reading Value Help Content [page 47]

8 Appendix D: Configuring the ABAP Connector to Use SNC

Prerequisites

- You have access to the SAP Cryptographic Library.

  > **Note**
  >
  > The distribution of the SAP Cryptographic Library is subject to and controlled by German export regulations and is not available to all customers. In addition, the library may be subject to local regulations of your own country that may further restrict the import, use and (re-)export of cryptographic software. If you have any further questions on this issue, contact your local SAP subsidiary.

- The AS ABAP is configured to use SNC.
  For more information, see the SNC documentation on the Help Portal.

  > **Note**
  >
  > In the procedure below you exchange the public-key certificates.

Context

You can use Secure Network Communications (SNC) to secure the connection between the Identity Center and the ABAP system.

SNC requires the use of an external security product to perform the security functions. For this purpose, you can use the SAP Cryptographic Library or any SNC-certified product. The following description shows how to configure SNC when using the SAP Cryptographic Library. If you are using a different SNC-certified product, then see the documentation provided by the vendor for information about how to establish the security context for the Identity Center.

Procedure

1. Download and install the SAP Cryptographic Library.
2. Create a Personal Security Environment for the Identity Center.
3. Create credentials for the Identity Center.

4. Exchange the public-key certificates belonging to the Identity Center and the AS ABAP.
5. Set the SNC parameters for the AS ABAP connector.
6. Maintain the extended user access control lists (ACL) on the AS ABAP to allow the service user to connect to the AS ABAP using the SNC connection.
7. Test the connection.

Related Information

Secure Network Communications (SNC)

8.1 Creating a Personal Security Environment

Context

Use the command line tool's command `get_pse` to generate the server's PSE, which includes the public and private key pair and a public-key certificate. If you are using a trusted CA, then you can also use the `get_pse` command to generate a certificate request. Per default, all of the items are generated, however, you can use the options `-noreq` or `- onlyreq` to explicitly include or omit the certificate request.

> **Tip**
>
> For easier administration, we recommend using self-signed certificates that are not signed by a trusted CA.

> **Note**
>
> As an alternative to creating a PSE, you can use the same PSE as the AS ABAP server. If this is the case, and you have already created the PSE on the AS ABAP, then copy the AS ABAP's PSE to the appropriate location instead of creating a new one.

Procedure

1. Start a command line interface.
2. Navigate to the location of the sapgenpse command line tool.
3. Use the following command line to generate a PSE. Create the server's PSE in the SECUDIR directory.

```
sapgenpse get_pse [-p <PSE_name>] [-x <PIN>] [DN]
```

Where:

Command Line Options

Option	Parameter	Description	Allowed Values	Default
-p	<PSE_name>	Path and file name for the server's PSE	Path description (in quotation marks, if spaces exist)	None
-x	<PIN>	PIN that protects the PSE	Character string	None
None	DN	Distinguished Name for the server The Distinguished Name is used to build the server's SNC name.	Character string (in quotation marks, if spaces exist)	None

> **Note**
>
> The Distinguished Name consists of the following elements:
>
> - CN = <Common_Name>
> - OU = <Organizational_Unit>
> - O = <Organization>
> - C = <Country>

The following examples show possible Distinguished Names for the Identity Center:

- CN=IC, OU=MyDept, O=MyCompany, C=DE
- CN=IC, OU=IdM, O=MyCompany, C=US

There are also additional command line options that you can use to specify further details. See the table below.

Additional Command Line Options

Option	Parameter	Description	Allowed Values	Default
-r	<file_name>	File name for a certificate request	Path description (in quotation marks, if spaces exist)	stdout
-s	<key_len>	Key length	512, 1024, 2048	1024
-a	<algorithm>	Algorithm used	RSA, DSA	RSA

Option	Parameter	Description	Allowed Values	Default
-noreq	None	Only generate a key pair and PSE. Do not generate a certificate request.	Not applicable Not	Not set
-onlyreq	None	Generate a certificate request for the public key stored in the PSE specified by the -p parameter.	Not applicable Not	Not set

Results

The server's PSE is created in the directory you specified.

> **Note**
>
> Check the contents of the directory at the operating system level to make sure the PSE was created in the correct location before proceeding with the next step.

> **Example**
>
> The following command line generates a PSE for the Identity Center where a self-signed certificate is used.
>
> ```
> sapgenpse get_pse -p IC.pse -noreq -x abcpin "CN=IC, O=MyCompany, C=DE"
> ```

8.2 Creating Credentials

Context

The server must have active credentials at runtime. Therefore, to produce active credentials, use the configuration tool's command `seclogin` to "open" the server's PSE.

> **Note**
>
> The credentials are located in the `cred_v2` file in the directory specified in the `<SECUDIR>` environment variable. Make sure that only the user under which the server runs has access to this file (including read access).

> ⚠ Caution
>
> It is very important to create the credentials for the user who runs the Identity Center's processes. In a default installation, this user is SYSTEM.

Procedure

Use the following command line to open the server's PSE and create credentials:

```
sapgenpse seclogin [-p <PSE_name>] [-x <PIN>] [-O [<NT_Domain>\]<user_ID>]
```

Where:

Command Line Options

Option	Parameter	Description	Allowed Values	Default
-p	<PSE_name>	Path and file name for the server's PSE	Path description (in quotation marks, if spaces exist)	None
-x	<PIN>	PIN that protects the PSE	Character string	None
-o	[<NT_Domain>] \<user_ID>	User for which the credentials are created. (The user that runs the dispatcher service.)	Valid operating system user	The current user

With the additional options, you can also use the seclogin command to delete the server's credentials, change the PIN that protects a PSE, or to list the available credentials for a user. See the table below.

Additional Command Line Options

Option	Parameter	Description	Allowed Values	Default
-l	None	List all available credentials for the current user.	Not applicable	Not set
-d	None	Delete PSE	Not applicable	Not set
-chpin	None	Specifies that you want to change the PIN	Not applicable	Not set

Results

The credentials file (`cred_v2`) for the user provided with the `-O` option is created in the SECUDIR directory.

> **Note**
>
> Check the contents of the directory at the operating system level to make sure the credentials were created in the correct location before proceeding with the next step.

> **Example**
>
> The following command line opens the Identity Center's PSE and creates credentials for the MXDispatcher_Service_User user.
>
> ```
> sapgenpse seclogin -p IC.pse -x abcpin -O MXDispatcher_Service_User
> ```

8.3 Exchanging the Public-Key Certificates

Context

This procedure assumes that you are using different PSEs for the AS ABAP server and the Identity Center.

If you are using the same PSE, then you can skip this step. In this step, you establish a trust relationship between the two servers by exchanging their public-key certificates. This procedure consists of the following steps.

Procedure

1. Export the Identity Center's public-key certificate from the Identity Center's PSE.
2. Import the Identity Center's public-key certificate into the AS ABAP's SNC PSE.
3. Export the AS ABAP's public-key certificate from the AS ABAP's SNC PSE.
4. Import the AS ABAP's public-key certificate into the Identity Center's PSE.

8.3.1 Exporting the Identity Center's Public-Key Certificate

Context

Procedure

Use the tool's command `export_own_cert` to export the server's certificate:

```
sapgenpse export_own_cert -o <output_file> -p <PSE_name> [- x <PIN>]
```

Where:

Command Line Options

Option	Parameter	Description	Allowed Values	Default
-o	<output_file>	Exports the certificate to the named file	Path description (in quotation marks, if spaces exist)	stdout
-p	<PSE_name>	Path and file name for the server's PSE	Path description (in quotation marks, if spaces exist)	None
-x	<PIN>	PIN that protects the PSE	Character string	None

Example

The following command line exports the Identity Center's public-key certificate to the `IC.crt` file.

```
sapgenpse export_own_cert -o IC.crt -p IC.pse -x abcpin
```

8.3.2 Importing the Identity Center's Public-Key Certificate Into the AS ABAP's SNC PSE

Prerequisites

- You know the PIN that protects access to the AS ABAP's SNC PSE.
- You have access to the Identity Center's public-key certificate that you exported in the last step.

Context

If the AS ABAP uses the SAP Cryptographic Library as its security provider for SNC, then you can use the trust manager to maintain the AS ABAP's SNC PSE.

Procedure

1. Using the trust manager on the AS ABAP (transaction `STRUST`), select the *SNC PSE* with a double-click.
2. Enter the PIN that protects access to the PSE.

   Information about the SNC PSE appears in the upper section of the trust manager's screen.
3. Choose *Certificate* > *Import* from the menu or the symbol for *Import certificate*.
4. In the dialog that follows, enter the path and file name of the Identity Center's public-key certificate file, select the *Base64* format, and choose *Enter*.

   The certificate appears in the *Certificate* section of the trust manager's screen.
5. Choose *Add to Certificate List* to add the certificate to the AS ABAP's SNC PSE.
6. Save the data.

> ⚠ Caution
>
> Do not forget to save the data. Otherwise, changes made to the PSE are lost.

8.3.3 Exporting the AS ABAP's Public-Key Certificate

Context

Continue with exporting the AS ABAP's public-key certificate.

Procedure

1. Make sure the SNC PSE is still the selected PSE.
2. Select the certificate shown in the *Owner* field with a double-click.

   Information about the certificate appears in the *Certificate* section.
3. Choose *Certificate* > *Export* from the menu or the symbol for *Export certificate*.
4. In the dialog that follows, enter the path and file name where you want to save the file, select the *Base64* format and choose *Enter*.

   The file is saved to the file system.
5.

Results

You can now import this file into the Identity Center's PSEs.

8.3.4 Importing the AS ABAP's Public-Key Certificate Into the Identity Center's PSE

Return to the Identity Center server and import the AS ABAP's public-key certificate into the Identity Center's PSE.

Prerequisites

- You have access to the AS ABAP's public-key certificate that you exported in the last step.

Context

Procedure

Use the tool's command `maintain_pk` to import the AS ABAP's public-key certificate into the Identity Center PSE's certificate list.

```
sapgenpse maintain_pk [-a <cert_file>] -p <PSE_name> [-x <PIN>]
```

Where:

Command Line Options

Option	Parameter	Description	Allowed Values	Default
-a	<cert_file>	Add certificate from file `<cert_file>` to the certificate list.	Path description (in quotation marks, if spaces exist)	None
-p	<PSE_name>	Path and file name for the server's PSE	Path description (in quotation marks, if spaces exist)	None
-x	<PIN>	PIN that protects the PSE	Character string	None

Additional Command Line Options

Option	Parameter	Description	Allowed Values	Default
`-m`	`<cert_file>`	Add multiple certificates from `<cert_file>` to the certificate list.	Not applicable	None
`-M`	`<store>`	Add multiple certificates from the CryptoAPI certificate store to the certificate list.	ROOT, CA, MY, SPC	None
`-d`	`<number>`	Delete certificate number <number> from certificate list.	Numerical value	None
`-l`	None	List existing certificate list.	Not applicable	None
`-y`	None	Automatic YES-mode for `-m` or `-M` options.	Not applicable	None

Example

The following command line imports the AS ABAP's certificate from the `<AS ABAP_DIR_INSTANCE>\sec \ABC.crt` file into the Identity Center's PSE.

```
sapgenpse maintain_pk -a <AS_ABAP_DIR_INSTANCE>\sec\ABC.crt -p <Install_folder>\sec
\IC.pse
```

8.4 Setting the SNC Parameters

Context

You then have to set the connection-specific SNC parameters in the repository constants for the AS ABAP system that you are connecting to.

Procedure

Set the parameters as shown in the table below.

Repository Constants for SNC

Parameter	Description	Permitted Values	Example
`JCO_CLIENT_ SNC_LIB`	Path and file name of the SAP Cryptographic Library	String value	<Install_folder>\ sap-crypto.dll
`JCO_CLIENT_ SNC_MODE`	SNC activation indicator	0, 1 0 = SNC disabled 1= SNC activated	1
`JCO_CLIENT_ SNC_MYNAME`	The Identity Center's SNC name.	String value	p:CN=IC, O=MyCompany, C=DE
`JCO_CLIENT_ SNC_PARTNERNAME`	SNC name of the communication partner (AS ABAP)	String value	p:CN=ABC, O=MyCompany, C=DE
`JCO_CLIENT_ SNC_QOP`	Quality of protection level	1: Secure authentication only 2: Data integrity protection 3: Data privacy protection 9: Use the value from `snc/ data_prote ction/max`.	3

For more information about setting repository constants, see *Creating Repositories*. For more information about transporting repository definitions, see the *Transport Guide* on the SAP Community Network. For more information about the SNC parameters, see the SAP Help Portal.

Related Information

Creating Repositories [page 44]
SAP Identity Management Implementation Guide - Transport
SAP Help Portal

8.5 Maintaining the Extended User ACL

Context

When setting up the SNC-protected connection, the two systems are authenticated within the SNC layer, but not the actual user that is to log on to the AS ABAP using the connection. Therefore, to allow the service user to connect to the AS ABAP using the secure connection, you must maintain the extended user ACL. Proceed as follows:

Procedure

1. Using table maintenance (for example, transaction `SM30`), maintain the `USRACLEXT` table.
2. Choose *New Entries*.
3. Enter the following data in the corresponding fields:

   Required Data

Field	Value	Example
User	`<IC_service_user>`	**`IC_SERV_USER`**
Sequence Number	`<seqential number>`	**`000`**
SNC Name	`<IC_SNC_Name>`	**`p:CN=IC, O=MyCompany, C=DE`**

4. Save the data.

8.6 Testing the Connection

Context

Procedure

1. Set up a job that reads data from the AS ABAP and run it.
2. If the job returns errors, set the following system environment variables:
   - RFC_TRACE = 1
   - CPIC_TRACE = 3
3. Run the job again.
4. Check the CPIC trace file.

   This file has the name `CPICTRC<number>` and, by default, is located in the Identity Center's install folder.

   The file contains the SNC initialization information. A correct initialization appears as follows.

```
[Thr 3560] <<- SncSetParam()==SAP_O_K
[Thr 3560] ->> SncInit(prg=5, ini_fname=(NULL),
      &sec_avail=000784D3)
[Thr 3560] SncInit(): Initializing Secure Network Communication
      (SNC)
[Thr 3560] PC with Windows NT
      (mt,ascii,SAP_UC/size_t/void* = 8/32/32)
[Thr 3560] SncInit(): Trying user/application supplied as a
      gssapi library name: "C:\Program Files\SAP\IdM\Identity
      Center\sapcrypto.dll".
[Thr 3560] load shared library (C:\Program
      Files\SAP\IdM\Identity
      Center\sapcrypto.dll), hdl 0
[Thr 3560] using "C:\Program Files\SAP\IdM\Identity
      Center\sapcrypto.dll"
      ...
[Thr 3560] File "C:\Program Files\SAP\IdM\Identity
      Center\sapcrypto.dll" dynamically loaded as GSS-API v2
      library.
[Thr 3560] The internal Adapter for the loaded GSS-API
      mechanism identifies as:
      Internal SNC-Adapter (Rev 1.0) to SECUDE 5/GSS-API v2
[Thr 3560] <<- SncPDLInit()==SAP_O_K
[Thr 3560] SncInit(): Initiating Credentials available,
      lifetime=263246h 32m 39s
[Thr 3560] <<- SncInit()==SAP_O_K
[Thr 3560] sec_avail = "true"
[Thr 3560] ->> SncSessionInit(&snc_hdl=000784D4)
[Thr 3560] <<- SncSessionInit()==SAP_O_K
[Thr 3560] out: &snc_hdl = 0D753FC8
[Thr 3560] ->> SncSetMyName(snc_hdl=0D753FC8, myname="p:CN=IC,
      O=MyCompany, C=DE")
[Thr 3560] <<- SncSetMyName()==SAP_O_K
[Thr 3560] in: myname = "p:CN=IC, O=MyCompany, C=DE"
[Thr 3560] ->> SncSessionInitiator(snc_hdl=0D753FC8,
      auth_type=1, buf_size_hint=0,target='p:CN=ABC,
      O=MyCompany, C=DE')
[Thr 3560] <<- SncSessionInitiator()==SAP_O_K
[Thr 3560] in: target = "p:CN=ABC, O=MyCompany, C=DE"
[Thr 3560] parses to = "p:CN=ABC, O=MyCompany, C=DE"
[Thr 3560] ->> SncSetQOP(snc_hdl=0D753FC8, min=max default,
      max=max default, qop=max default)
[Thr 3560] <<- SncSetQOP()==SAP_O_K
[Thr 3560] in: qop values = "min=9 (max default), max=9
      (max default), use=9 (max default)"
[Thr 3560] resulting = "min=3 (old:2), max=3 (old:3),
      use=3 (old:3)"
[Thr 3560] STISncInit: set snc state to SNC_ENABLED
```

Any errors will be indicated in this initialization block. The table below shows typical error conditions.

Typical Errors

Error	Description	Solution
GSS-API(maj): No credentials were supplied GSS-API(min): Can't read file Couldn't acquire DEFAULT INITIATING credentials	Either credentials were not created, or they were created for the wrong user.	Make sure the Identity Center's SNC is correct. Use the sapgenpse command get_my_name to obtain the Distinguished Name being used. Make sure this coincides with the repository constant JCO_CLIENT_SNC_MYNAME. Also make sure the credentials exist for the correct user. To make sure, delete the cred_v2 file (if it exists) and create credentials for the correct user. (The user ID is also indicated in the error message.) Use the sapgenpse seclogin command with the –O option to set the user for which the credentials apply.
SncSetMyName()== SNCERR_BAD_NT_PREFIX in: myname in: target	The message in: myname indicates that the Identity Center's SNC name is not correct. The message in: target indicates that the AS ABAP's SNC name is not correct.	
GSS-API(maj): A token had an invalid signature GSS-API(min):The name is wrong	The connection could not be established.	Check the value of the repository constant JCO_CLIENT_SNC_MYNAME or JCO_CLIENT_SNC_PARTNERNAME depending on the corresponding message. Make sure the SNC name contains the prefix p:.
GSS-API(maj): A token had an invalid signature GSS-API(min): Certification path ends at wrong CA	The connection could not be established.	Check the SNC name for the AS ABAP in the repository constant JCO_CLIENT_SNC_PARTNERNAME. Make sure it corresponds to the SNC name specified in the profile parameter snc/identity/as on the AS ABAP.

Error	Description	Solution
no conversation found with id <ID> In addition, the error SNC name and specified user/client do not match appears in the job log.	The connection could not be established with the given parameter values.	The certification path could not be verified. Check the trust relationships. Make sure the Identity Center's publickey certificate is contained in the SNC PSE's certificate list on the AS ABAP. Also make sure the AS ABAP's publickey certificate is contained in the Identity Center's certificate list. You can use the sapgenpse maintain_pk – l option to check the Identity Center's certificate list.
SNC disabled, reject request from host=<host> TP=java	SNC is not active on target system.	Activate SNC and check the configuration on the target system.

8.7 Downloading and Installing the SAP Cryptographic Library

Prerequisites

- You know the user under which the dispatcher runs. You can find this user by checking the user that runs the Windows service `MXDispatcher_<dispatcher_name>`.

Context

The SAP Cryptographic Library installation package is available for authorized customers on the SAP Service Marketplace at service.sap.com/swdc.

The installation package sapcrypto.car contains the following files:

- The SAP Cryptographic Library (`sapcrypto.dll` for Windows NT or `libsapcrypto.<ext>` for UNIX).
- A corresponding license ticket (ticket).
- The configuration tool `sapgenpse.exe`.

Procedure

1. Download the file from the SAP Service Marketplace and extract it to a local directory.

   If you are not authorized to download the file, then contact your local subsidiary to clarify whether you are allowed to receive the installation package.
2. Copy the library (`sapcrypto.dll`) and the command line tool (`sapgenpse.exe`) to a local directory, for example, the Identity Center's install directory.

   ```
   <Install_folder>\sapcrypto.dll
   ```

   ```
   <Install_folder>\sapgenpse.exe
   ```
3. Copy the license ticket (ticket) to a local directory.

   > **Tip**
   >
   > We recommend creating a subdirectory sec and copying the ticket to this directory.

   ```
   <Install_folder>\sec\ticket
   ```

   This will also be the location for the Identity Center's Personal Security Environment (PSE) that contains the key pair used for securing the connections.
4. Set the SECUDIR environment variable to this directory.

   ```
   SECUDIR=<Install_folder>\sec
   ```
5. Make sure you set SECUDIR for the user that runs the corresponding dispatcher (or as a system variable, if the user is the SYSTEM user).

   > **Note**
   >
   > Default SECUDIR
   >
   > If SECUDIR is not set, then the server searches for the license ticket in the sec subdirectory of the server's home directory:
   >
   > On Windows NT: `$HOMEDRIVE$HOMEPATH\sec\`
6. If the user running the dispatcher is different from the logged on user, set the system environment variable USER to the dispatcher's user.

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.

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: https://help.sap.com/viewer/disclaimer).

go.sap.com/registration/contact.html