SAP Identity Management
Connector Overview

SAP SE
Walldorf, August 2015
Disclaimer

This presentation outlines our general product direction and should not be relied on in making a purchase decision. This presentation is not subject to your license agreement or any other agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or to develop or release any functionality mentioned in this presentation. This presentation and SAP’s strategy and possible future developments are subject to change and may be changed by SAP at any time for any reason without notice. This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. SAP assumes no responsibility for errors or omissions in this document, except if such damages were caused by SAP intentionally or grossly negligent.
Tips: How To Use And Find The Information On The Following Pages…

Make sure to use hyperlinks in order to move around in this presentation.

Hyperlinks…

… are behind every menu item on all agenda slides. Clicking on the menu item will bring you directly to the desired information within this presentation.

… are also working in the PDF-version

Click on the little house-button in the upper right corner to move back to the next upper agenda-level (several sub-agendas exist)

Click on the text-box in the lower right corner in order to return to the highest level main agenda
Index by connector name (alphabetically – all known connectors) → click on the line to find detailed information

Blackberry Ent. Server – by Kogit
CA-ACF2 – by Identity Forge
CA-Top Secret – by Identity Forge
Employee Productivity Excellence (EPE) – by IBSolution GmbH
ENDRA – Enhanced Notes Domino Resource Adapter – by Kogit GmbH
FlexiTrust CA – by FlexSecure
Generic database connector
Generic ASCII Interface
HP NonStop (Tandem) – by Identity Forge
HP OpenVMS – by Identity Forge
HP UX – by Identity Forge
IBM AIX – by Identity Forge
IBM Cognos – by Kogit
IBM iSeries (i5/AS400) – by Identity Forge
IBM RACF – by Identity Forge
IBM RACF – by Kogit
LINUX-RED HAT – by Identity Forge
Lotus Notes/Domino C API
Lotus Notes/Domino Java API for IDM 8.0+
MS Active Directory
MS Exchange
MS ILM (formerly MIIS)
MS SharePoint – by Asconst
MS SharePoint – by Kogit
NetSuite ERP – by Identity Forge
Novell eDirectory
Oracle (SUN) Solaris – by Identity Forge
Oracle Directory (fka. SunOne)
Salesforce CRM – by Identity Forge
SAP Customer Relationship Management
SAP HANA Database
SAP Human Capital Management (using VDS)
SAP ERP Financials (Auditing)
SAP ERP Financials (Accounting)
SAP Extended Warehouse Management
SAP NetWeaver Master Data Management (by IBSolution GmbH)
SAP Portfolio and Project Management
SAP Product Lifecycle Management
SAP Service Parts Planning
SAP Supplier Relationship Management
SAP Supply Network Collaboration
SAP Transportation Management
Service Lifecycle Management Framework – by HP
Service Workflow Visualization Tool – by HP
SuccessFactors Connector (SFSF)

© 2015 SAP SE or an SAP affiliate company. All rights reserved.
1. **Introduction to Identity Management Connectivity and Services**
   A. Connectivity Overview
2. **SAP Identity Management – SAP Application Connectors in Detail**
   I. Standard Bulk Operations with SAP NetWeaver Application Servers
   II. Integration of IDM to SAP components – Special features by component
   III. Central User Administration – Integration and Migration
   IV. Connectors to Non-SAP Applications
   V. 3rd. Party Extension-Products to SAP Identity Management
3. **Database Connectivity and Supported Databases**
4. **The IDM Connector Development Kit for Non-SAP Applications – Overview**
6. **List of Worldwide Implementation Partners**
SAP Identity Management – Connections via Identity Services

Requirements:
- Create a tight integration with SAP applications
- Integrate third-party applications

- Identity services as a standards-based single access point for querying and managing identity information in the complete system landscape
- ‘Tightly aligned, loosely coupled’ integration with SAP and heterogeneous applications based on industry standards
Requirements for Identity Services

The main purpose of Identity Services is to provide web services access to identity data in the Identity Center. Through web services, external clients are able to manage users, privileges (technical roles) and business-roles. The Identity Services accept operations to create and modify users, as well as assigning and removing privilege assignments and role-assignments.

In addition, there are a number of operations for retrieving information about the configuration and the system.

There are several requirements that such a solution has to fulfill:

- **Standard protocols**: In order to make the service available to a variety of applications, it has to be based on standard protocols (like SPML and LDAP). Since access protocols evolve and new protocols gain popularity, it has to be possible to extend the available protocol set.

- **Flexible architecture**: The properties and requirements of the identity service itself may change over time. The solution must be capable of coping with such changes in a way that it removes the burden of changes from Identity Services consumers.

- **Secure**: The number of potential Identity Services consumers is large. Each consumer may have different needs and requirements. Hence, it is crucial that the solution has the means of controlling access to the identity data.
Identity Virtualization

**Virtual Directory Server (VDS) provides**
- Single consistent view and entry point for multiple distributed identity data sources
- Identity information as a service for applications through standard protocols (LDAP, SPML)
- Abstraction layer for underlying data stores

**Consumer only sees one standard interface**
- Transform incoming LDAP requests, and connect directly to the existing data repositories
  - Data stays within original data source
  - Efficient caching

**Properties**
- Real-time access to data; No need to consolidate data sources; No extra data store
  - Quick LDAP deployment
  - Easier and cheaper maintenance
- Attribute manipulation
- Name space modifications
- Complex operations on-the-fly
SAP Identity Management Connectivity – Overview

**Databases**
- SAP HANA Database
- Microsoft SQL Server
- Microsoft Access
- Oracle database
- IBM UDB (DB2)
- MySQL
- Sybase

**On-Prem/Cloud Applications**
- SAP Business Suite
- SuccessFactors
- SAP Access Control (GRC)
- Lotus Domino/Notes (C API)
- Lotus Domino/Notes (Java API) for IDM8.0
- Microsoft Exchange
- RSA ClearTrust
- RSA SecurID

**Directory Servers**
- Microsoft Active Directory
- IBM Tivoli Directory
- Novell eDirectory
- Oracle Directory (fka. SunOne)
- Oracle Internet Directory
- Microsoft Active Directory Application Mode (ADAM)
- Siemens DirX
- OpenLDAP
- eB2Bcom View500 Directory Server
- CA eTrust Directory
- SAP IDM Virtual Directory Server
- Any IDM Virtual Directory Server
- Any LDAP v3 compliant directory server

**Technical**
- SPML
- LDAP
- ODBC / JDBC / OLE-DB
- RFC
- LDIF files
- XML files
- CSV files

**Other + Partner**
- SAP Application Server
- Microsoft Windows
- Unix / Linux
- Shell execute
- Custom Java connector API
- Script-based connector API

... more available and possible...
Availability of More Connectors for Other Applications

Is there a need for a connector that is not mentioned in this presentation?

• SAP continuously evaluates the need for additional connectors and enhances its connector portfolio in response to customer requirements

Alternatives:

• If you are looking for a connector to an application that is not mentioned in this presentation, please contact SAP consulting or one of the SAP implementation partner companies. They will be able to advise on the current planning for your specific application, or custom-create this connector for you

• SAP provides a Connector Development Toolkit (CDK) for partners and customers to develop their own connectors. See the slides about this topic at the end of this presentation
Integration of SAP Business Suite applications
SAP Identity Management –
Standard Bulk Operations with SAP NetWeaver Appl. Servers

Bulk operations from SAP Identity Management to SAP NetWeaver Application Server ABAP and SAP NetWeaver Application Server Java (UME)

- User creation
- User modification
- User deletion
- Disable/enable users
- Assign/De-assign roles
- Assign initial password

All of the above can be done:

- Manually
- Rule based
- Automatically (via batch or scheduled task)
- Workflow based
SAP Identity Management – Standard Functionality with SAP NetWeaver Application Servers

Functional Features

As a result, an identity that is stored in IDM will have a user with assigned roles. That user can logon to a connected SAP system and use the necessary transactions in e.g. an ABAP system or SAP Java Portal.

Certain single roles for e.g. accounts payable and accounts receivable are delivered as examples.

By assigning corresponding business roles in SAP Identity Management to the appropriate single roles used in the company, it can be controlled which functions can be accessed by a user. Contained within these example roles, among other things, is that a user can execute certain transactions as soon as the data distribution from SAP Identity Management to e.g. SAP ERP Financials or other SAP ERP components has been completed.
Integration of IDM to other SAP components – Applications Overview and Special Features

The next slides will discuss special features that are available for the following different SAP components:

- SAP Human Capital Management (using VDS)
- SuccessFactors Connector
- SAP ERP Financials (Auditing)
- SAP ERP Financials (Accounting)
- SAP Transportation Management
- SAP Extended Warehouse Management
- SAP Supply Network Collaboration
- SAP Service Parts Planning
- SAP Product Lifecycle Management
- SAP Portfolio and Project Management
- SAP Customer Relationship Management
- SAP Supplier Relationship Management
- SAP NetWeaver Master Data Management (by IBSolution GmbH)
- SAP Central User Administration (CUA)
- SAP HANA Database
SAP Human Capital Management (incl. using VDS)
Pre-requisites for SAP HCM and SAP Identity Management Operation

SAP Identity Management Version 7.1 or higher
  • incl. Virtual Directory Server

SAP HCM application component Personnel Administration as of SAP Enhancement Package 4 for SAP ERP 6.0

Note: SAP Identity Management is from a technical point of view an LDAP-enabled directory service, which in particular can process time-dependent employee data. You can use this function to process employee data in the Personnel Administration application component of SAP ERP HCM using a query in order to transfer it to SAP Identity Management.
Bulk operations

– HERE: Sending of employee-related data from SAP ERP HCM to IDM (push from HCM)

Create identities in IDM
Change identities in IDM
Automatic re-formatting of user information from HCM;
- configurable mapping between employee data in HCM and identity data in IDM
Customer specific info types can be replicated from HCM to IDM

SAP HCM special features:
To obtain the employee data, an InfoSet and a corresponding query is used in HCM; Report RPLDAP_EXTRACT_IDM can run regularly as a background job in ‘Delta Download mode’; Sample queries and corresponding BAdI implementations for Delta Download are delivered;

The HR business owner configures which data is replicated when to which Identity center; Regarding “Concurrent employment”, supported by HCM, relate to SAP note 1688791; read more on help.sap.com - Retrieval of Employee-Related Data by SAP ERP HCM
Bulk operations

– HERE: Transfer of identity data from SAP Identity Management to SAP ERP HCM

Automatic modification of employee-related communication data in the component ‘Personnel Administration’ of SAP ERP HCM depending on data in SAP Identity Management

Support of employee related data to be transferred from IDM to HCM

predefined samples:

• Building number
• Office number
• SAP system user name
• First phone number at work center, fax number, mobile phone number
• Email address

SAP HCM special features:
A Business Add-In (BAdI) Implementation BADL_IDM_HR_COMMUNICATION of BAdI definition BADL_EXTEND.IDENTITY is used to update employee data in the SAP ERP HCM system
read more on help.sap.com - Transfer of Employee-Related Data to SAP ERP HCM
SuccessFactors connector (SFSF)
Pre-requisites for Identity propagation if initiated from SuccessFactors

SAP Identity Management Version 8.0 or higher
   • incl. Virtual Directory Server

SuccessFactors
   • SuccessFactors is used as an employee master data system
   • Employee Central is active on SuccessFactors, and Employee Central SOAP API is enabled
   • The SuccessFactors OData API is enabled
   • Role-based permission is enabled
   • You have a technical user on SuccessFactors

Note: The SuccessFactors Connector is shipped as a separate package in SAP Identity Management's Provisioning Framework. The package is called com.sap.idm.connector.sfsf
SuccessFactors Connector (SFSF) 2/3
– Functionality with SAP Identity Management

Bulk operations
– HERE: Sending of employee-related data from SuccessFactors to IDM (push from SFSF)

  o Create / change identities with attributes
    • New since IDM 8.0 SP1: update of username and email attributes
  o Assigning roles to users or removing roles from users

Note: read more in the SAP Identity Management Configuration Guide on
SAP ERP Financials (Auditing)
Pre-requisites for SAP FI and SAP Identity Management Operation

- SAP Identity Management Version 7.1 or higher

Use case:

A user to whom the single role SAP_PLM_AUDITOR is assigned has authorizations for transactions Audit Management and Audit Monitor, as soon as the user and authorization distribution has been completed.
Functional Features

Two cases need to be distinguished when you create auditor-related data:

If you are using SAP ERP HCM and distribute employee-related data to the Audit Management system using Application Link Enabling (ALE), the business partner type EMPLOYEE is assigned to the user.

If you are not using SAP ERP HCM, the user is created as well as a business partner of the type EMPLOYEE and this business partner is assigned to the user.

SAP FI special features:
The function uses BAdI implementation BADI_IDM_PLM_AUDITOR of Business Add-In (BAdI) BADI_EXTEND_IDENTITY. See also the info on help.sap.com – Identity Management for Audit Management.
SAP ERP Financials (Accounting)
Pre-requisites for SAP FI and SAP Identity Management Operation

SAP Identity Management Version 7.1 or higher

FI-AP (account payable) or FI-AR (accounts receivable) of SAP ERP Financials as of SAP Enhancement Package 4 for SAP ERP 6.0

Use case:
A new SAP FI user automatically gets access to all functions in the corresponding company code of the FI system that he needs to do his regular job
SAP Identity Management creates a user for the new employee in the accounting system in the required company code. The system then enters the user under his initials in the company code as an accounting clerk (for example, in company code 0001 with initials PM for user MAJORP).

The user can be assigned to customers or vendors or have them assigned by an administrator, and so be designated as a contact person for correspondence, dunning and checks, for example, or select his work list in processes such as payment proposal processing.

**SAP FI special features:**
The function uses BAdI implementation BADI_IDM_FI_ACCOUNTINGCLERK of Business Add-In (BAdI) BADI_EXTEND_IDENTITY.

see also the info on help.sap.com – Identity Management for accounting clerks
SAP Transportation Management
Pre-requisites for SAP TM and SAP Identity Management Operation

SAP Identity Management Version 7.1 or higher
SAP TM 7.0 or higher

Optional: SAP HCM application component Personnel Administration as of SAP Enhancement Package 4 for SAP ERP 6.0

The organizational structure was transferred from SAP ERP HCM to SAP TM by means of Application Link Enabling (ALE)

– or –

the organizational model was manually created in SAP TM
Functional Features

You transfer data for internal or external identities from SAP Identity Management to SAP TM. Internal identities are users that represent your employees. External identities are users such as business partners that can access your system for specific purposes. In SAP TM, transportation service providers (TSPs) are such external users that can access your system for tendering purposes.

After transfer of the user information, a business partner ID is created for the employee with an Employee business partner role. In addition, the system creates a business partner of the type Central Person and assigns it to the employee's user. If the position of the user is defined in SAP ERP HCM and this position exists in SAP TM, SAP TM assigns the business partner with the Employee BP role to this position.

Certain example roles are delivered which can be assigned to users created in SAP TM from internal identities.

SAP TM special features:
The system uses the /SCMTMS/IDM_TM Business Add-In (BAdI) implementation of the BADI_EXTEND_IDENTITY BAdI definition to create or update the business partner data; - read more on help.sap.com - Identity Management for SAP Transportation Management

© 2015 SAP SE or an SAP affiliate company. All rights reserved.
SAP Extended Warehouse Management (EWM)
Pre-requisites for SAP EWM and SAP Identity Management Operation

SAP Identity Management Version 7.1 or higher

SAP EWM 7.0 or higher with labor management activated

SAP HCM application component Personnel Administration as of SAP Enhancement Package 4 for SAP ERP 6.0
When labor management is activated and you provision identities from IDM to SAP EWM, the system creates a user with a respective SAP EWM role, a business partner (BP) with the Processor BP role, and a Central Person for the BP that manages the user ID, the personnel number, and the BP data.

SAP EWM special features:
The system uses the /SCWM/EL_IDM_EWM Business Add-In (BAdI) implementation of the BADI_EXTEND.IDENTITY BAdI definition in the background to create or update BPs with a Processor BP role.
The system uses the /SCMB/MDL_PARTNER BAdI implementation of the /SCMB/MDL_PARTNER_GEN_ID BAdI definition to influence the ID of the BP with a Processor BP role.
read more on help.sap.com - Identity Management for SAP Extended Warehouse Management
SAP Supply Network Collaboration (SNC)
Pre-requisites for SAP SNC and SAP Identity Management Operation

SAP Identity Management Version 7.1 or higher

SAP SNC 7.0 or higher

SAP HCM application component Personnel Administration as of SAP Enhancement Package 4 for SAP ERP 6.0
Functional Features

Trigger automatic generation of users and business partners for SAP SNC. This is relevant in the following scenarios:

Creation of users and business partners for employees
A user administrator assigns a certain business role to an identity in IDM. As a result, SAP Identity Management triggers automatic user and business partner creation in SAP SNC for the employee.

Creation of users and business partners for external users
If some users of an external business partner, who is maintained as a business partner of type Organization in SAP SNC, require access to the SNC system, the IDM administrator creates the users as new external identities in SAP Identity Management and assigns them to the external business partner. SAP Identity Management triggers automatic user and business partner creation in SAP SNC for the users of the external business partner.

SAP SNC special features:
In order to have your own logic for assigning business partners of type Organization to new users, the BAdI /SCA/IDM_PARTNEROwn needs to be implemented.
read more on help.sap.com - Identity Management for SAP Supply Network Collaboration
SAP Service Parts Planning
Pre-requisites for SAP Service Parts Planning and SAP Identity Management Operation

SAP Identity Management Version 7.1 or higher
SAP SPP 7.0 or higher

For the use case “Creation of users and business partners for new employees”, the Personnel Administration component of the SAP ERP HCM solution (as of enhancement package 4 for SAP ERP 6.0) must be installed.

Notes:

* This function in SPP is integrated into the Web user interface in SAP Supply Network Collaboration (SAP SNC). For more information about SAP SNC, see the SAP SNC documentation on the SAP help portal at http://help.sap.com

* For more information about the standard SAP SPP setup, see the relevant sections of the SAP SCM Master Guide at http://service.sap.com/instguides
SAP Service Parts Planning 2/2
– Functionality with SAP Identity Management

Functional Features

With SAP Identity Management, you can trigger automatic generation of users and business partners for SAP Service Parts Planning (SAP SPP). This is relevant in the following use cases:

Creation of users and business partners for new employees

A user administrator creates new employees in the Human Resources (HR) system of the company running SAP SPP. These new employees also need users in SAP SPP, which is solved as follows:

- The user creation in the HR system triggers the automatic creation of a new identity in the SAP Identity Management system.
- If you assign a business role to the identity in SAP Identity Management, then the system triggers automatic user and business partner creation in SAP SPP for these employees

Creation of users and business partners for external users

An external business partner who is maintained as a business partner of type Organization in SAP SPP, requires access to the system
An administrator creates a new external identity in the SAP Identity Management system and assigns it to the external business partner
SAP Identity Management triggers automatic user and business partner creation in SAP SPP for the users of the external business partner

In addition, you can also change and delete such users centrally with SAP Identity Management

read more on help.sap.com - Identity Management for SAP Service Parts Planning
SAP Product Lifecycle Management
SAP Product Lifecycle Management 1/2
– Version Dependencies

Pre-requisites for SAP Product Lifecycle Management and SAP Identity Management Operation

SAP Identity Management Version 7.1 or higher

SAP HCM application component Personnel Administration as of SAP Enhancement Package 4 for SAP ERP 6.0

You have installed Enhancement Package 4 for SAP ERP 6.0 and activated the PLM Web User Interface (PLM Web UI).
### Functional Features

You use this function to manage the data of your employees or external users across different SAP systems, such as SAP Product Lifecycle Management (SAP PLM) and SAP ERP Human Capital Management (SAP HCM), using SAP Identity Management 7.1 or higher. You can use this function, for example, in the detailed design with collaboration scenario. In this use case, you can use employee data from SAP HCM to create users in SAP PLM.

Within SAP PLM, you can have the following systems connected to SAP Identity Management:

- PLM 7.0 Backend System
- Internal Portal
- DMZ System
- External Portal

SAP Identity Management provides user data for the connected SAP systems. SAP Identity Management also provides profiles with information about user-role-assignments and triggers these assignments within the connected SAP systems. The mapping of users and roles takes place in SAP Identity Management without having the content of these roles there. You have to maintain the PCFG roles and portal roles in the connected SAP systems separately.

*read more on [help.sap.com - Identity Management for SAP Product Lifecycle Management]*
SAP Portfolio and Project Management
Pre-requisites for SAP Portfolio and Project Management and SAP Identity Management Operation

SAP Identity Management Version 7.1 or higher

SAP HCM application component Personnel Administration as of SAP Enhancement Package 4 for SAP ERP 6.0

The SAP HCM personnel area or sub-area must be mapped to an SAP portfolio and Project Management-specific location in customizing for SAP RPM, by choosing

- Base System Interfaces
- SAP Human Capital Integration
- Data Distribution from SAP HCM to SAP xRPM
- Map Personnel Areas to Locations

This setting is only required if you want to create business partners

The background user in IDM, which is used for the RFC calls to the Portfolio and Project Management application (when transferring identities) must have the authorization of the PFCG role SAP_XRPM_ADMINISTRATOR. This role can update access control lists for SAP Portfolio and Project Management entities (such as portfolio, or bucket) and create users and business partners in the SAP Portfolio and Project Management application.
Functional Features

This function is used to manage the data of employees across different SAP systems, such as SAP Portfolio and Project Management or SAP ERP Human Capital Management (SAP HCM), using SAP Identity Management 7.1 or higher. Identity Management for SAP Portfolio and Project Management enables efficient and secure management of users and authorizations based on the assignment of roles to an identity which changes over time. This increases administrative efficiency for day-to-day tasks related to Identity Management across the system landscape and helps you to fulfill legal requirements like SAP Governance, Risk, and Compliance tasks, security reviews and audits. The users created from SAP Identity Management have the standard user configuration.

The SAP Identity Management system creates an identity for each employee. When the identity is transferred to SAP Portfolio and Project Management, the system creates a user and a business partner (BP). It also creates a Central Person for the BP that manages the user ID, the personnel number, and the BP data.

Note: BP creation is optional. The /RPM/IDENTITY_MAN BAdI definition is used to create BPs

read more on help.sap.com - Identity Management for SAP Portfolio and Project Management
SAP Customer Relationship Management
Pre-requisites for SAP Customer Relationship Management and SAP Identity Management Operation

SAP Identity Management Version 7.1 or higher

You have installed SAP CRM 7.0

The PFCG roles available for business roles in SAP CRM have been loaded into SAP Identity Management

To ensure that the employee is created in SAP CRM and to avoid the assignment of employees to nonexistent user accounts in SAP CRM, a certain configuration of the ALE inbound process in SAP CRM has to be performed

read more on help.sap.com - Identity Management for SAP Customer Relationship Management
SAP Identity Management is used to automatically create and update identities with corresponding authorizations for employees in SAP Customer Relationship Management (SAP CRM).

If you are using SAP ERP HCM, employee data is sent to SAP CRM using Application Link Enabling (ALE). Corresponding identities are created automatically in SAP Identity Management and are subsequently assigned to the relevant employees (business partners) in SAP CRM.

If you are not using SAP ERP HCM, an administrator creates identities in SAP Identity Management. Based on the identity data, employees are created automatically in SAP CRM. The relevant user accounts for your employees are automatically assigned in SAP CRM.

In SAP CRM, the combination of a user account, a business partner, and a central person is needed so that SAP CRM processes can handle users correctly. The central person is required to establish the relationship between a user account and a business partner, and is assigned to both, the user account and the business partner, to link them together.

The combination of a user account, a business partner, and a central person is created automatically

Note: read more on help.sap.com - Identity Management for SAP Customer Relationship Management
SAP Supplier Relationship Management (SAP SRM)
Pre-requisites for SAP Supplier Relationship Management and SAP Identity Management Operation

- SAP Identity Management Version 7.1 or higher
- SAP SRM 7.0
- SAP ERP HCM as of SAP Enhancement Package 4 for SAP ERP 6.0
- The PFCG roles available for business roles in SAP SRM have been loaded into SAP Identity Management
- The portal roles available for business roles in SAP SRM have been loaded into SAP Identity Management
SAP Supplier Relationship Management 2/2
– Functionality with SAP Identity Management

Functional Features

SAP Identity Management is used to automatically create and update identities with corresponding authorizations for employees in SAP Supplier Relationship Management (SAP SRM). SAP Identity Management can be used with SAP ERP Human Capital Management (SAP ERP HCM) only.

In SAP SRM, the combination of a user account, a business partner, and a central person is needed so that SAP SRM processes can handle users correctly. The central person is required to establish the relationship between a user account and a business partner, and is assigned to both the user account and the business partner to link them together.

The combination of a user account, a business partner, and a central person is created automatically.

Employee data is sent from SAP ERP HCM to SAP SRM using Application Link Enabling (ALE). Corresponding identities are created automatically in SAP Identity Management while the employee data is uploaded from SAP ERP HCM to SAP Identity Management.

read more on help.sap.com - Identity Management for SAP Supplier Relationship Management (SAP SRM)
SAP NetWeaver Master Data Management (by IBSolution GmbH)
Basic Adapter Functionality: User, Role and Password Management in SAP MDM repositories

Provisioning Framework by SAP
- Generic Tasks (Modify Task, etc.)
- Independent from connected system type

IC Tasks provided by IBSolution
- System Specific Tasks
- Hooks into the Provisioning Framework

Java Connector provided by IBSolution

SAP Master Data Management
Repositories to be managed
Adapter Functionality Details

- Retrieval of existing users and roles from SAP MDM repositories
- Add / Modify / Delete user records in the SAP MDM repository’s user store based on the assignment of privileges (derived from imported MDM roles) within SAP Identity Management
- Ready-to-Use Repository Templates, Job Templates and Provisioning Tasks
- Seamless Integration into the SAP Provisioning Framework by adopting its concepts
- Initial Load Jobs / Update Jobs for SAP MDM integration
- System-Specific Provisioning Tasks for SAP MDM integration

Adapter Prerequisites

- SAP Identity Management 7.0 SP02 or higher
- SAP NetWeaver Master Data Management 5.5. SP06 or higher
- Adapter is based on DSE Java Runtime and therefore can be used on all platforms supported by the SAP MDM Java API (see https://support.sap.com/release-upgrade-maintenance/pam.html for more information)
SAP HANA In-Memory Database
Pre-requisites for the SAP HANA Connector and SAP Identity Management Operation

Identity Center v7.2 SP03 (released October 2011) and above

SAP HANA Database version 1.0 and above
  • Connection via the SQL interface

Note: This connector is provided within the SAP IDM provisioning framework
Supported operations:

- Reading of users
- Add / delete users
- Set/change password
- Event based updates
- Add / remove role assignments
- Enables synchronization of users in complex landscapes

Notes: For more information please refer to the document: Identity Management for SAP System Landscapes: Configuration Guide
http://www.sdn.sap.com/irj/sdn/go/portal/prtroot/docs/library/uuid/60efa02c-0532-2e10-d495-f185b1e
SAP HANA Security
Authorization: User setup in different scenarios

Data mart scenario
- Individual users directly access the SAP HANA database, e.g. to consume reports
- Privileges for individual users/roles are assigned on the database level
- Database administrators directly access the SAP HANA database

BW scenario
- Individual users do not have direct access to the SAP HANA database
- Privileges for individual users/roles are assigned in the BW layer
- BW connects to the database via a technical user
- Database administrators directly access the SAP HANA database
Central User Administration (CUA) & SAP Identity Management
What is the relationship between SAP Identity Management and the Central User Administration (CUA)?

SAP Identity Management is the strategic solution for managing identities in SAP and non-SAP environments.

SAP will continue to support CUA in its current functionality according to SAP maintenance rules.

SAP Identity Management can be connected and used in combination with an existing CUA.

Should I install a new CUA?

It depends on the scope of your project and your current stage:
You can quickly and easily connect ABAP-based systems to a new CUA. This enables you to manage several thousand users and their individual role assignments.

However, if you require automatic cross-system rule-based access management, workflow support, or connectivity for a heterogeneous system landscape, you should consider using SAP Identity Management.
Central User Administration (CUA) – Migration to SAP Identity Management

Requirement:
Extend support of identity management to non-SAP environments and greater level of functionality

• Supports SAP and heterogeneous environments
• Self-service and delegated admin
• Workflow and approvals
• Business role management

Manage CUA from SAP Identity Management
Migrate ABAP systems from CUA to IDM
Shut down CUA when all systems are migrated

Requirement:
Extend support of identity management to non-SAP environments and greater level of functionality

• Supports SAP and heterogeneous environments
• Self-service and delegated admin
• Workflow and approvals
• Business role management

Manage CUA from SAP Identity Management
Migrate ABAP systems from CUA to IDM
Shut down CUA when all systems are migrated

© 2015 SAP SE or an SAP affiliate company. All rights reserved.
Connectors to Non-SAP Applications

**The next slides will discuss connectors that are available to Non-SAP application:**

Blackberry Ent. Server – by Kogit
CA-ACF2 – by Identity Forge
CA-Top Secret – by Identity Forge
FlexiTrust CA – by FlexSecure
Generic database connector
Generic ASCII Interface
HP NonStop (Tandem) – by Identity Forge
HP OpenVMS – by Identity Forge
HP UX – by Identity Forge
IBM AIX – by Identity Forge
IBM Cognos – by Kogit
IBM iSeries (i5/AS400) – by Identity Forge
IBM RACF – by Identity Forge
IBM RACF – by Kogit

Linux RED HAT – by Identity Forge
Lotus Notes/Domino C API
Lotus Notes/Domino Java API for IDM 8.0+
MS Active Directory
MS Exchange
MS ILM (formerly MIIS)
MS SharePoint – by Asconsit
MS SharePoint – by Kogit
Novell eDirectory
NetSuite ERP – by Identity Forge
Oracle (SUN) Solaris – by Identity Forge
Oracle Directory (fka. SunOne)
Salesforce CRM – by Identity Forge

**Notes:** Click on one line to jump immediately to the adapter information

The above list will constantly be subject for updates
Blackberry Enterprise Server - by KOGIT GmbH
Pre-requisites for Blackberry and SAP Identity Management Operation

Identity Center and VDS v7.1 and above

Blackberry Enterprise Server 5.0
- For Domino Server
- For MS Exchange Server

Platform: Windows
Blackberry Ent. Server - by KOGIT GmbH 2/2
– Functionality with SAP Identity Management

Supported operations:

Account actions:
- Creation of accounts
- Reading of accounts
- Modify and delete accounts
- Enable/Disable accounts

Password related:
- Set initial passwords
- Set productive password
- Retrieve passwords

Group actions:
- Add group
- Modify Group
- Delete Group
- Add and remove members

Roles and policy actions:
- Reading of roles
- Creating of roles
- Modify and delete of roles
CA-ACF2 – Advanced Connector by Identity Forge
CA-ACF2 – Advanced Connector by IdF 1/2
– Version Dependencies

Integration Overview
Provide automatic provisioning, reconciliation, password management and monitoring for z/OS ACF2 target systems:
Uses SAP Virtual Directory LDAPv3 Integration for "out-of-the-box" integrations that provide lower risk, simplified implementation and proven industry integration.
Enhanced functionality for z/OS ACF2 implementations, such as:
- Custom Attribute Support
- Alias/Catalog Management
- High-Availability and Enhanced Performance

Pre-requisites
Identity Center v7.0 SP2 (released June 2008) and above
Uses Standard, out-of-the-box SAP LDAP Adapter
Security Manager: ACF2 on z/OS [ACF2 R8 to R15]
Supported Platform: IBM z/OS 1.4 – 1.13
### Supported CA-ACF2 Operations:

- **User Supported Operations:**
  - Retrieve all users and all user profile attributes
  - Add, modify, suspend (Disable) delete, nosuspend (Enable) users
  - Assign/Un-Assign Access Rules
  - Assign/Un-Assign Resource Rules
  - Custom Attribute Support

- **User Password Operations:**
  - Self Service Change Password
  - Admin Reset Password (w/Password Policy Verification)
  - Password Synchronizations

- **Access Rule Supported Operations:**
  - Retrieve all Access Rules and all profile data
  - Add, Modify and Delete Access Rules
  - Assign or Un-Assign User Membership (Multiple Users)

- **Resource Rule Supported Operations:**
  - Retrieve All Resource Rules and data
  - Add, Modify and Delete Resource Rules
  - Assign or Un-Assign User Membership (Multiple Users)

- **ALIAS Supported Operations:**
  - Retrieve All Master Catalog Alias For A User
  - Retrieve All Catalog Alias For A User
  - Define Alias / Delete Alias

### Enhanced Functionality:

- **Complete Reconciliation of all data for the following:** users, access rules, resources, catalogs

- **Legacy Integration or Custom Application Support [Post-Processing]:**
  - Submit REXX, JCL scripts post ACF2 command, passing relevant data

- **Real-Time User Audit Tracking (Real-Time tracking of user/event changes on z/OS):**
  - Record and Report Date and Time of User Event
  - Record and Report Issued Commands (Including Complete Data)
  - Record and Report Issuing IP Address
  - Record and Report Issuing User (Who Made Change)
  - Record and Report Affected User (User Changed)

### Notes:

The Identity Forge (IdF) Advanced Connector for ACF2 has additional functionality specifically related to ACF2 Target systems. Please refer to [http://identityforge.com/index.php/products/mainframe-midrange/advanced-adapter-for-ca-acf2](http://identityforge.com/index.php/products/mainframe-midrange/advanced-adapter-for-ca-acf2) for more information.
CA-Top Secret – Advanced Connector by Identity Forge
Integration Overview

Uses SAP Virtual Directory LDAPv3 Integration for “out-of-the-box” integrations that provide lower risk, simplified implementation and proven industry integration
Provides automatic provisioning, reconciliation
Enhanced functionality for z/OS CA-Top Secret implementations, such as:
  • Custom Attribute Support (CSDATA)
  • Alias/Catalog Management
  • High-Availability and Enhanced Performance

Pre-requisites for Top Secret and SAP Identity Management Operation

- Identity Center v7.0 SP2 (released June 2008) and above
- Uses Standard, out-of-the-box SAP LDAP Adapter
- Security Manager: CA-Top Secret R9 and Above
- Supported Platform: IBM z/OS 1.4 – 1.13
CA-Top Secret – Advanced Connector by IdF 2/2
– Functionality with SAP Identity Management

**Supported Operations:**

**User Supported Operations:**
- Retrieve all users and all user profile attributes
- Add, modify, suspend (Disable) delete, no-suspend (Enable) users
- Assign/Un-Assign Access Rules
- Assign/Un-Assign Resource Rules
- Custom Attribute Support

**User Password Operations:**
- Self Service Change Password
- Admin Reset Password (w/Password Policy Verification)
- Password Synchronizations

**Profile Supported Operations:**
- Retrieve all Access Rules and all profile data
- Add, Modify and Delete Profiles
- Assign or Un-Assign User Membership (Multiple Users) to Profiles

**Resource Supported Operations:**
- Retrieve All Resources and all Dataset data
- Add, Modify and Delete
- Permit Access

**Facilities Supported Operations:**
- Retrieve All Facilities and All Facility Data
- Add, Modify and Delete Facilities
- Assign or Un-Assign User Membership (Multiple Users) to Facilities

**Enhanced Functionality:**
- Complete Reconciliation (Full Import) of all data for the following (users, profiles, groups, resources (facilities), datasets)
- Legacy Integration or Custom Application Support [Post-Processing]
  - Submit REXX, JCL scripts post TOP SECRET command, passing relevant data
- Real-Time User Audit Tracking (Real-Time tracking of user/event changes on z/OS)
  - Record and Report Date and Time of User Event
  - Record and Report Issued Commands (Including Complete Data)
  - Record and Report Issuing IP Address
  - Record and Report Issuing User (Who Made Change)
  - Record and Report Affected User (User Changed)
- Real-Time (Push) Reconciliation
  - Native Password Capture
  - Detect Native User Event
  - Detect Native Event Capture
- Alias/Catalog Management
  - Define, Delete Alias
  - Retrieve All Catalog Alias and All Master Catalog Alias for a User

**Notes:** The Identity Forge (IdF) Advanced Connector for TOP SECRET has additional functionality specifically related to TOP SECRET target systems. For more information please refer to [http://identityforge.com/index.php/products/mainframe-midrange/advanced-adapter-for-ca-topsecret](http://identityforge.com/index.php/products/mainframe-midrange/advanced-adapter-for-ca-topsecret)
FlexiTrust Certification Authority (CA) by FlexSecure
Pre-requisites for the FlexSecure FlexiTrust B Certification Authority and SAP Identity Management Operation

Identity Center v7.1 SP2 (released June 2009) and above

FlexiTrust B v3.5.5 and above

Platform:

- RedHat Enterprise Linux V4 and above,
- SUSE Linux Enterprise V10 and above,
- Debian V4.0 and above
- Sun Solaris V9 and above

Note:

This connector provides SAP Identity Management with the ability to connect to the FlexiTrust Certification Authority by FlexSecure

The templates use the VDS to allow IDM the remote control of the FlexiTrust CA
FlexiTrust Certification Authority 2/2
– Functionality with SAP Identity Management

**Supported operations:**

- Trigger user certificate generation, receive certificate
- Revoke user certificate
- Receive certificate revocation list (CRL)
- It is possible to hand over the passwords for certificate activation

**Notes:**
Certificates and CRLs can be passed on to a productive directory service by SAP Identity Management
More information about FlexiTrust can be found here: [http://www.flexsecure.de/de/loesungen/flexitrust-b-trustcenter](http://www.flexsecure.de/de/loesungen/flexitrust-b-trustcenter)
Generic Database Connector
Generic Database Connector 1/2 – Version Dependencies

Pre-requisites for the Generic Database Connector and SAP Identity Management Operation

Identity Center v7.0 SP2 and above

Any database

Platform: Any platform supported by the respective database

Note:

This connector provides generic means of communicating with any type of database, using generic SQL statements.
Generic Database Connector 2/2
– Functionality with SAP Identity Management

Supported operations:

• Reading of users
• Reading of groups
• Add, modify, delete users
• Use of any SQL statement
• Event based updates

Group actions:

➤ Group operations in this context means updating other tables, which of course is possible

Notes:

This is a low level connector in the Identity Center, which connects to any database using the JDBC protocol.

Any SQL statement (including stored procedures) can be executed to retrieve data from the database. Updating can either update rows directly, using a unique identifier, or by issuing any SQL statements. Event based updating depends on the database, and may require adding a timestamp column to a table or writing a stored procedure;

It is possible to add passwords encrypted or in clear text (not recommended) to any database table.
Generic ASCII Interface
Generic ASCII Interface 1/2
– Version Dependencies

Pre-requisites for the generic ASCII interface and SAP Identity Management Operation

Identity Center v7.0 SP2 and above

Any ASCII text file

Platform: Any platform supported ASCII text files

Note:
This connector provides identity management with the ability to read and write ASCII files. It can handle CSV files (with and without headers) and fixed record length files.
Generic ASCII Interface 2/2
– Functionality with SAP Identity Management

**Supported operations:**

Reading of users

Reading of groups

Add, modify, delete users

Event based updates are NOT supported

It is possible (although not advisable) to write passwords to the ASCII file, both in clear text or encrypted

**Notes:**

A template exists for the Core Identity Center connector for reading and writing files. This can be used for interfacing with any application that can export/import certain formatted ASCII files. It is possible to write only changes, as well as reading only changes (delta handling);

Data can optionally be encrypted in the file.
HP NonStop (Tandem) – Advanced Connector by Identity Forge
HP NonStop – Advanced Connector by IdF 1/2
– Version Dependencies & Architecture

Integration Overview
Provide automatic provisioning, reconciliation, password management and monitoring for HP NonStop target systems
Use SAP Virtual Directory LDAPv3 Integration for “out-of-the-box” that provide lower risk, simplified implementation and proven industry integration

Pre-requisites for HP NonStop and SAP Identity Management
Identity Center v7.0 SP2 (released June 2008) and above
Security Manager: Any HP NonStop OS
HP NonStop – Advanced Connector by IdF 2/2  
– Functionality for SAP Identity Management

**Supported Operations:**

**User Guardian Supported Operations:**
- Retrieve all users and all user profile attributes
- Add, alter, freeze, thaw and delete
- Assign or Un-Assign User to Groups
- Self Service Change Password
- Admin Reset Password

**User ALIAS Supported Operations:**
- Retrieve all users and all user profile attributes
- Add, alter, freeze, thaw and delete
- Assign or Un-Assign User to Groups
- Self Service Change Password
- Admin Reset Password

**Group Supported Operations:**
- Retrieve all groups and attribute data
- Add, Alter and Delete groups
- Assign or Un-Assign User Membership

**Enhanced functionality for NonStop implementations, such as:**
- Guardian ID & Alias group assignments
- Remote Password
- High-Availability and Enhanced Performance

**Notes:**
HP OpenVMS – Advanced Connector by Identity Forge
Pre-requisites for HP OpenVMS and SAP Identity Management

- Identity Center v7.0 SP2 (released June 2008) and above
- OpenVMS version support: Any version of VAX, Alpha, Integrity

Integration Overview

- Use SAP Virtual Directory LDAPv3 Integration for "out-of-the-box" integrations that provide lower risk, simplified implementation and proven industry integration
- Enhanced functionality for OpenVMS implementations:
  - Rule Management
  - High-Availability and Enhanced Performance
Supported Open VMS Operations:

ROLE (UAF) Supported Operations:
- Search & Extract ALL UAF Rights
- Create New UAF Rights
- Modify/Update UAF Attributes
- Assign Users
- Un-Assign Users

Password Management:
- Admin Password Resets

User Management:
- Search & Extract All Users
- Create New Users
- Modify/Update User Attributes
- Disable Users
- Enable Users
- Delete Users
- Assign UAF Rights Membership
- Un-Assign UAF Rights Membership

Notes:
HP UX – Advanced Connector by Identity Forge
Integration Overview

Provide automatic provisioning, reconciliation, password management and monitoring for HP-UX target systems:

Use SAP Virtual Directory LDAPv3 Integration for “out-of-the-box” integrations that provide lower risk, simplified implementation and proven industry integration.

Enhanced functionality for HP-UX implementations, such as:

- SSH or Agent Based
- High-Availability and Enhanced Performance

Pre-requisites

- Identity Center v7.0 SP2 (released June 2008) and above
- Uses Standard, out-of-the-box SAP LDAP Adapter
- Platform: HP-UX (Enterprise) any version
Supported HP-UX Operations:

User Supported Operations:
- List all users and all user profile attributes
- Create User
- Modify User Attributes (uid/gid)
- Delete User
- Add or Append User to Group
- Change User’s Supplemental/Auxiliary Groups

User Password Operations:
- Admin Reset Password

Group Supported Operations:
- Create Group
- Modify Group
- Delete Group
- List all groups and all group data
- List all groups a user is a member of

Notes:
The Identity Forge (IdF) Advanced Connector for HP-UX has additional functionality specifically related to HP-UX. Please refer to http://identityforge.com/index.php/products/enterprise-unix-os/advanced-adapter-for-hpux for more information.
IBM AIX – Advanced Connector by Identity Forge
Integration Overview

Provides automatic provisioning, reconciliation, password management and monitoring for IBM AIX target systems:
Use SAP Virtual Directory LDAPv3 Integration for “out-of-the-box” integrations that provide lower risk, simplified implementation and proven industry integration.
Enhanced functionality for AIX implementations:
• Support for standard and custom attributes
• High-Availability and Enhanced Performance

Pre-requisites Overview

• Identity Center v7.0 SP2 (released June 2008) and above
• Uses Standard, out-of-the-box SAP LDAP Adapter
• Security Manager: IBM-AIX [v5.x, v6.x, v7.x and above]
IBM AIX – Advanced Connector by IdF 2/2
– Functionality with SAP Identity Management

User Management Features:
- Authenticate user with ID & Password
- Create, update & delete user/login ID
- Reset user password
- Enable / disable user
- Assign / un-assign user to group
- Assign / un-assign user to role

Reconciliation & Data Mining Features
- Retrieve all users
- List user attribute information
- Retrieve all groups
- List group attribute information

Notes:
The Identity Forge (IdF) Advanced Connector for IBM-AIX has additional functionality specifically related to IBM-AIX. Please refer to http://identityforge.com/index.php/products/enterprise-unix-os/advanced-adapter-for-ibm-aix for more information.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.
IBM Cognos – by Kogit GmbH
Pre-requisites for COGNOS and SAP Identity Management Operation

Identity Center and VDS v7.1 and above

IBM COGNOS 8

Platform: Windows 2000 and above
Supported operations:

Account Actions
- Creating of accounts
- Reading of accounts
- Modify and delete accounts
- Enable/Disable accounts

Password related:
- Set initial passwords
- Set productive password
- Retrieve passwords

Group actions:
- Add group
- Modify Group
- Delete Group
- Add and remove members

Roles and policy actions:
- Reading of roles
- Creating of roles
- Modify and delete of roles
IBM iSeries (i5/AS400) – Advanced Connector by Identity Forge
Integration Overview

Provide automatic provisioning, reconciliation, password management and monitoring for z/OS IBM iSeries target systems:

- Uses SAP Virtual Directory LDAPv3 Integration for “out-of-the-box” integrations that provide lower risk, simplified implementation and proven industry integration.
- Enhanced functionality for iSeries implementations, such as:
  - Custom COMMANDCALL Support
  - High-Availability and Enhanced Performance

Pre-requisites Overview

- Identity Center v7.0 SP2 (released June 2008) and above
- Uses Standard, out-of-the-box SAP LDAP Adapter
- Security Manager: i5 SERIES [i5/AS400 v5.2 and above]
Supported iSeries Operations:

User Supported Operations:
- Retrieve all users and all user profile attributes
- Add, modify, disable, delete, enable users
- Directory Entry Support

User Password Operations:
- Self Service Change Password
- Admin Reset Password (w/Password Policy Verification)
- Password Synchronizations

Group Supported Operations:
- Retrieve All Groups and all profile data
- Add, Modify and Delete Profiles
- Assign or Un-Assign User Membership (Multiple Users) to Profiles

Enhanced Functionality:

Complete Reconciliation of all data for the following (users, groups, files)

Real-Time (Push) Reconciliation
- Native Password Capture
- Detect Native User Event
- Detect Native Event Capture

Custom Command Call Support
- Configurable support for processing custom i5 Command Calls

Note:
IBM RACF – Advanced Connector by Identity Forge
IBM RACF – Advanced Connector by IdF 1/2
– Version Dependencies & Architecture

Pre-requisites for z/OS IBM-RACF and SAP Identity Management

- Identity Center v7.0 SP2 (released June 2008) and above
- Security Manager: RACF on z/OS - Platform: IBM z/OS 1.4 – 1.13

Integration Overview

Provide automatic provisioning, reconciliation, password management and monitoring for z/OS IBM RACF target systems

Uses SAP Virtual Directory LDAPv3 Integration for “out-of-the-box” integrations that provide lower risk, simplified implementation and proven industry integration

Enhanced functionality for z/OS RACF implementations, such as:
- Custom Attribute Support (CSDATA)
- Alias/Catalog Management
- High-Availability and Enhanced Performance

Diagram:

- PROVIDER
- STANDARD LDAP REQUEST & RESPONSE
- z/OS IBM-RACF
- VOYAGER
- PIONEER AGENT
- LDAP GATEWAY
IBM RACF – Advanced Connector by IdF 2/2
– Functionality with SAP Identity Management

Supported RACF Operations:

User Supported Operations:
- Retrieve all users and all user profile attributes
- Add, alter, revoke/disable, resume/enable delete
- Assign or Un-Assign User to Group
- Permit Users to Datasets & Resources
- Self Service Change Password
- Admin Reset Password
- Password Interval Operations
- Password Capture Synchronizations

Group Supported Operations:
- Retrieve all groups and attribute data
- Add, Alter and Delete groups
- Assign or Un-Assign User Membership (CONNECT/REMOVE)

Dataset Supported Operations:
- Retrieve All Datasets and all dataset profile attributes
- Add, Modify and Delete Datasets

Resource Supported Operations:
- Retrieve all facility and custom resources
- Create, Alter and Delete resource

Enhanced Functionality:

Complete Reconciliation of all data for the following (users, groups, datasets, resources (facilities))

Legacy Integration or Custom Application Support [Post-Processing]
- Submit REXX, JCL scripts post RACF command, passing relevant data

Real-Time User Audit Tracking (Real-Time tracking of user/event changes on z/OS)
- Record and Report Date and Time of User Event
- Record and Report Issued Commands (Including Complete Data)
- Record and Report Issuing IP Address
- Record and Report Issuing User (Who Made Change)
- Record and Report Affected User (User Changed)

Real-Time (Push) Reconciliation
- Native Password Capture
- Detect Native User Event
- Detect Native Event Capture

Alias/Catalog Management
- Define, Delete Alias
- List Master Catalog Entries

Digital Certificate Management

Notes: The Identity Forge (IdF) Advanced Connector for IBM-RACF has additional functionality specifically related to IBM-RACF and z/OS. Please refer to http://identityforge.com/index.php/products/mainframe-midrange/advanced-adapter-for-ibm-racf for more information.
IBM RACF Connector by Kogit
Pre-requisites for RACF and SAP Identity Management Operation

Identity Center v7.0 SP2 and above

Secure Way Security Server for z/OS 1.4 or newer

Platform: z/OS 1.4 or newer
IBM RACF – Connector by Kogit GmbH 2/2
– Functionality with SAP Identity Management

Supported operations:

Account actions
- Reading of accounts
- Reading of groups
- Add, modify, delete accounts
- Enable/Disable accounts

Event based updates are supported

Group actions:
- Add group
- Modify Group
- Delete Group
- Add and remove members

Password related:

Set initial passwords
Set productive password
Retrieve passwords

Manage different user types / attributes

Note: for more information visit www.kogit.de
Linux-RED HAT – Advanced Connector by Identity Forge
Integration Overview

Provide automatic provisioning, reconciliation, password management for Red Hat Linux target systems:

- Uses SAP Virtual Directory LDAPv3 Integration for "out-of-the-box" integrations that provide lower risk, simplified implementation and proven industry integration.
- Enhanced functionality for Red Hat Linux implementations, such as:
  - SSH or Agent Based
  - High-Availability and Enhanced Performance

Pre-requisites

- Identity Center v7.0 SP2 (released June 2008) and above
- Uses Standard, out-of-the-box SAP LDAP Adapter
- Platform: Enterprise Linux RED HAT Any version 4.x – 5.x
Linux RED HAT – Advanced Connector by IdF 2/2
– Functionality with SAP Identity Management

Supported Operations:

User Supported Operations:

- List all users and all user profile attributes
- Create User
- Modify User Attributes (uid/gid)
- Delete User
- Add or Append User to Group
- Change User’s Supplemental/Auxiliary Groups

User Password Operations:

- Admin Reset Password

Group Supported Operations:

- Create Group
- Modify Group
- Delete Group
- List all groups and all group data
- List all groups a user is a member of

Notes:

The Identity Forge (IdF) Advanced Connector for RED HAT Enterprise Linux has additional functionality specifically related to RED HAT. Please refer to http://identityforge.com/index.php/products/enterprise-linux-os/advanced-adapter-for-linux-redhat for more information.
IBM Lotus Notes/Domino Server Connector – C API
Pre-requisites for Lotus Notes and SAP Identity Management Operation

- Identity Center v7.1 (7.2 starting Q3/12)
- Lotus Notes client 7.0 up to 8.0
- Lotus Domino server 7.0 up to 8.0
- Platform: MS Windows 2008 server, MS Windows XP

Note: The connector is based upon Lotus Notes C API for Windows platform
Lotus Notes / Domino 2/3 – Functionality with SAP Identity Management

**Bulk operations:**
- Reading of users
- Reading of groups

**Admin process:**
- User creation with certificate generation
- Admin rename request
- Admin delete user request

**Non-admin process:**
- User modification
- User deletion

**Managed groups:**

**Group actions:**
- Add group
- Modify Group
- Delete Group
- Add and remove members

**Supported group types**
- Multi purpose group
- ACL Only
- Mail only
- Server only
- Deny only

**Lotus Notes Limitations:**

Groups in Lotus Notes have their own limitation (32 K limit of the list of all user names within a group). In general this is solved by subdividing the members into subgroups. However this is not part of the connector as this largely depends on the customer system.

Group assignment allows for bulk assignment/removal of users. For performance reasons a centralized solution with Identity Center running scheduled bulk updates are recommended, as the Identity Center ensures uniqueness and saves the costs for checking for user existence within a group/(and sub-groups).

Bulk operations also allows for add and remove member operation to be combined in one operation.
Provisioning and bulk operational tasks in Identity Center – Example

Provisioning tasks defined for Lotus Notes

Bulk tasks for Lotus Notes
IBM Lotus Notes/Domino Server Connector - Java API (new since IDM 8.0)
IBM Lotus Notes/Domino Connector for IDM 8.0+ – Version Dependencies

Pre-requisites for Lotus Notes and SAP Identity Management Operation

- Identity Center v8.0 or above
- Lotus Domino server Lotus Domino server at least 8.5.3
- ID Vault to be set for the organization which IdM will manage
- DIIOP processes to be running on the server
- Platform: Any platform where Java runs

Note:

- The Lotus Notes/Domino Connector for IDM 8.0+ is based upon Lotus Notes Java API
- The old connector is still valid for the older releases
IBM Lotus Notes/Domino Connector for IDM 8.0+
– Functionality with SAP Identity Management

Bulk operations:
- Reading of users
- Reading of groups

Admin process:
- User creation with certificate generation
- Admin rename request
- Admin delete user request
- Delete Group

Non-admin process:
- User modification
- User deletion

Managed groups:
Group actions:
- Create group
- Delete Group
- Add and remove members

Supported default group types
- Multi purpose group
- ACL Only
- Mail only
- Server only
- Deny only

Password reset
Invoked from a Domino Agent and we provide example code.

Lotus Notes Limitations:
Groups in Lotus Notes have their own limitation (32 K limit of the list of all user names within a group). In general this is solved by subdividing the members into subgroups. However this is not part of the connector as this largely depends on the customer system.

Group assignment allows for bulk assignment/removal of users. For performance reasons a centralized solution with Identity Center running scheduled bulk updates are recommended, as the Identity Center ensures uniqueness and saves the costs for checking for user existence within a group/(and sub-groups).

Bulk operations also allows for add and remove member operation to be combined in one operation.
Provisioning and other tasks in Identity Center – Example

Repository

Create Repository

Enter Name and Description of New Repository

Name: [Input]

Description: [Input]

Type: [Input]

Details of Repository "LDBP0"

Edit constants of repository "LDBP0"

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DESTINATION_SERVER_HOSTNAME</td>
<td>[Input]</td>
</tr>
<tr>
<td>IS_IMMEDIATE</td>
<td>[Input]</td>
</tr>
<tr>
<td>NAME_FILE_ACTION</td>
<td>[Input]</td>
</tr>
<tr>
<td>NAMES_DATABASE</td>
<td>[Input]</td>
</tr>
<tr>
<td>PASSWORD_RESET_AGENT_DATABASE</td>
<td>[Input]</td>
</tr>
<tr>
<td>PASSWORD_RESET_AGENT_NAME</td>
<td>[Input]</td>
</tr>
<tr>
<td>REGISTRATION_SERVER_HOSTNAME</td>
<td>[Input]</td>
</tr>
<tr>
<td>REGISTRATION_SERVER_IP_PORT</td>
<td>[Input]</td>
</tr>
<tr>
<td>REGISTRATION_SERVER_PASSWORD</td>
<td>[Input]</td>
</tr>
<tr>
<td>REGISTRATION_SERVER_USERNAME</td>
<td>[Input]</td>
</tr>
</tbody>
</table>

© 2015 SAP SE or an SAP affiliate company. All rights reserved.
MS Active Directory
Pre-requisites for MS Active Directory and SAP Identity Management Operation

Identity Center v7.0 SP2 and above


Supported operations:
- Reading of users
- Reading of groups
- Add, modify, delete users
- Event based updates are supported

Password related:
- Set initial passwords
- Set productive password
- Retrieve passwords

Group actions:
- Add group
- Modify Group
- Delete Group
- Add and remove members

Create, modify, delete and move AD security group, and any other objects within AD

Notes:
In general, SAP Identity Management supports heterogeneous landscapes when connecting to LDAP directories using a general LDAP API, which has to be adapted on a project base during implementation due to directory vendors' deviation or extension of standard LDAP schemata or attribute usage, as well as customer specific schema extensions and attributes.

SAP's support of the integration between SAP Identity Management and a third-party directory contains the standard LDAP definition described by the common standards' bodies.

A template for MS ADS is available: The template uses the built-in LDAP connector to update AD, with the exception of setting passwords, which requires the Windows runtime, and VB script, and must run on a domain connected windows-server.

Setting of password must be done by executing the job on the domain server. Retrieving passwords requires the AD password hook, which will capture any password changes.
MS Exchange
Pre-requisites for MS Exchange and SAP Identity Management Operation

Identity Center v7.0 SP2 and above

MS Exchange 2000 and above

MS Exchange 2/2 – Functionality with SAP Identity Management

Supported operations:

- Reading of users
- Reading of groups
- Add, modify, delete users
- Event based updates are supported

Group actions:

- Add group
- Modify Group
- Delete Group
- Add and remove members

Mail-enabled security-groups and distribution-lists can be handled

Note:

A template is available; If the LDAP-connector is used, a MAPI-Client has to connect to the mailbox before the physical mailbox is created. A workaround for this will be to use the client-library in combination with VB-scripts to create the mailbox.
MIIS / ILM (Microsoft Identity Integration Server, now called MS-ILM)
MIIS – Microsoft Identity Integration Server
MS-ILM = the New Name

MIIS / ILM – Microsoft Identity Integration Server

→ Now Called MS-ILM – Microsoft Identity Lifecycle Manager

The MIIS / ILM connector relies on a standard SQL database connector. It has to be connected on a project based configuration

Opportunity for a 3rd. party out-of-the-box connector
Microsoft SharePoint Connector by ASCONSIT
Pre-requisites for MS SharePoint and SAP Identity Management Operation

Identity Center v7.1 SP2 and above

MS SharePoint 2007 or higher

MS Active Directory (AD) set-up and configuration

Platform: MS Windows Server 2003 or higher
MS SharePoint – by ASCONSIT 2/2
– Functionality with SAP Identity Management

Supported operations:

AD related user actions:
- Reading of users
- Create user
- Modify user
- Delete user
- Enable/Disable user
- Rename user
- Move user

SharePoint group actions:
- Reading of groups
- Create and delete groups
- Add and remove users

SharePoint role actions:
- Reading roles
- Add and remove users

Special functions:
- Reconciliation
- Extended authentication options

Event based updates are supported

Password Management

Note: Technology is already proven and tested in existing customer projects. By default Windows Server 2008 and IIS supports stronger authentication mechanism. Connectivity via standard Web Service integration. Additional functions on demand.

Website: http://www.asconsit.com Contact: info@asconsit.com
MS SharePoint – by Kogit GmbH
Pre-requisites for MS SharePoint and SAP Identity Management Operation

Identity Center and VDS v7.1 and above

Microsoft SharePoint Server 2007 and above

Microsoft Active Directory

Platform: Windows
Supported operations:

Account actions (connected with MS AD)
- Creating of accounts
- Reading of accounts
- Modify and delete accounts
- Enable/Disable accounts

Password related:
- Set initial passwords
- Set productive password
- Retrieve passwords

Group actions:
- Add group
- Modify Group
- Delete Group
- Add and remove members

Roles and permissions actions
- Reading of roles and permissions
- Creating of roles and permissions
- Modify and delete of roles and permissions
NetSuite ERP – Advanced Connector by Identity Forge
NetSuite ERP – Advanced Connector by IdF 1/2
– Version Dependencies & Architecture

Integration Overview
Provide automatic provisioning, reconciliation, password management and monitoring for NetSuite ERP target systems:
Use SAP Virtual Directory LDAPv3 Integration for "out-of-the-box" integrations that provide lower risk, simplified implementation and proven industry integration.
Enhanced functionality for NetSuite ERP implementations, such as:
- Uses Standard NetSuite WSDL
- High-Availability and Enhanced Performance

Pre-requisites
- Identity Center v7.0 SP2 (released June 2008) and above
- Uses Standard, out-of-the-box SAP LDAP Adapter
- Platform: NetSuite ERP Web License

© 2015 SAP SE or an SAP affiliate company. All rights reserved.
Supported NetSuite Operations:

Employee/Customer Supported Operations:

- Search All Employees/Customers
- Create Employee
- Modify Employee Attributes
- Delete Employee
- Add or Append User Access Rights

User Password Operations:

- Admin Reset Password

Notes:

Novell eDirectory
Pre-requisites for Novell eDirectory and SAP Identity Management Operation

Identity Center v7.0 SP2 and above

Any Novell eDirectory

Platform: Any platform supported by Novell eDirectory
**Novell eDirectory 2/2**  
– Functionality with SAP Identity Management

**Supported operations:**

- Reading of users
- Reading of groups
- Add, modify, delete users
- Event based updates are supported

**Group actions:**

- Add group
- Modify Group
- Delete Group
- Add and remove members

**Password related:**

- Set initial passwords
- Set productive password
- Retrieve password is NOT supported

---

**Notes:**

In general, SAP Identity Management supports heterogeneous landscapes when connecting to LDAP directories using a general LDAP API, which has to be adapted on a project base during implementation due to directory vendors’ deviation or extension of standard LDAP schemata or attribute usage, as well as customer specific schema extensions and attributes. SAP’s support of the integration between SAP Identity Management and a third-party directory contains the standard LDAP definition described by the common standards’ bodies.

The framework with templates for the Novell eDirectory is currently not generally released as part of the product but can be retrieved on request from SAP.
Oracle (SUN) Solaris – Advanced Connector by Identity Forge
Oracle (SUN) Solaris – Advanced Connector by IdF 1/2
– Version Dependencies

Integration Overview

Use SAP Virtual Directory LDAPv3 Integration for "out-of-the-box", certified integrations that provides lower risk, simplified implementation and proven industry integration
Provides automatic provisioning, reconciliation and password management
Enhanced functionality for Oracle (SUN) Solaris implementations:
- SSH or Agent Based
- High-Availability and Enhanced Performance

Pre-requisites for Oracle (SUN) Solaris and SAP Identity Management Operation

- Identity Center v7.0 SP2 (released June 2008) and above
- Uses Standard, out-of-the-box SAP LDAP Adapter
- Platform: Oracle (SUN) Solaris (Any Version)
Supported Solaris Operations:

User Supported Operations:
- List all users and all user profile attributes
- Create User
- Modify User Attributes (uid/gid)
- Delete User
- Add or Append User to Group
- Change User’s Supplemental/Auxiliary Groups

User Password Operations:
- Admin Reset Password

Group Supported Operations:
- Create Group
- Modify Group
- Delete Group
- List all groups and all group data
- List all groups a user is a member of

Notes:
The Identity Forge (IdF) Advanced Connector for Solaris has additional functionality specifically related to Solaris OS. Please refer to http://identityforge.com/index.php/products/enterprise-unix-os/advanced-adapter-for-solaris for more information
Oracle Directory (fka. SunOne)
Oracle Directory (fka. SunOne) 1/2
– Version Dependencies

Pre-requisites for Oracle Directory (fka. SunOne) and SAP Identity Management Operation

Identity Center v7.0 SP2 and above

Any Oracle Directory (fka. SunOne)

Platform: Any platform supported by Oracle Directory (fka. SunOne)
Oracle Directory (fka. SunOne) 2/2
– Functionality with SAP Identity Management

Supported operations:

- Reading of users
- Reading of groups
- Add, modify, delete users
- Event based updates are NOT supported

Group actions:

- Add group
- Modify Group
- Delete Group
- Add and remove members

Password related:

- Set initial passwords
- Set productive password
- Retrieve password is NOT supported

Notes:

In general, SAP Identity Management supports heterogeneous landscapes when connecting to LDAP directories using a general LDAP API, which has to be adapted on a project base during implementation due to directory vendors’ deviation or extension of standard LDAP schemata or attribute usage, as well as customer specific schema extensions and attributes. SAP’s support of the integration between SAP Identity Management and a third-party directory contains the standard LDAP definition described by the common standards’ bodies.

A template exists. It uses the built-in LDAP connector to update Oracle directory server.
Salesforce CRM – Advanced Connector by Identity Forge
Integration Overview

Provide automatic provisioning, reconciliation, password management and monitoring for Salesforce CRM target systems:
Uses SAP Virtual Directory LDAPv3 Integration for “out-of-the-box” integrations that provide lower risk, simplified implementation and proven industry integration.
Enhanced functionality for Salesforce CRM implementations, such as:
  • Roles and Permission Sets
  • Standard v7 ‘13 WSDL Integration
  • High-Availability and Enhanced Performance

Pre-requisites

- Identity Center v7.0 SP2 (released June 2008) and above
- Uses Standard, out-of-the-box SAP LDAP Adapter
- Platform: Salesforce CRM up to ‘13 v7
Supported Salesforce Operations:

Product Features:

- Authentication
- User Security Management
- Password Management
- Role Assignment
- Permission Set Assignment
- Public Group Management
- Lead | Contract | Account | Opportunity Management
- Full Reconciliation of CRM Objects

**Notes:**

The next slides will discuss connections to Non-SAP applications that are using certain software extensions which were developed by the SAP partner network:

- **Employee Productivity Excellence (EPE)** – by IBSolution GmbH
- **ENDRA – Enhanced Notes Domino Resource Adapter** – by Kogit GmbH
- **Service Lifecycle Management Framework** – by HP
- **Service Workflow Visualization Tool** – by HP

Note: The above list will constantly be subject for updates
Employee Productivity Excellence (EPE) by IBSolution GmbH
IBSolution’s EPE is an Add-On solution, built upon SAP Identity Management, which combines SAP IDM's powerful functions with easy to use UI’s and pre-build scenarios and content

By using identity services, EPE is tightly integrated into the SAP Identity Management solution and comes up with …

- easy to use UI’s
- a wizard based workflow construction kit
- huge functionality to allow decentralized administration (incl. decentralized workflow definition + centralized approval)
- HR integration (display of organizational model plus easy assignment of roles to org. units / positions)
- html email notifications
- person-centric task list
- usage of open standards such as SPML, BPEL, …
- a lot more …

IBSolution EPE is available for SAP Identity Management 7.0 SP2 and later releases
Seamless integration of SAP Identity Management and IBSolution EPE User Interfaces

Visualization of the HR Org.Model to assign roles to Org.Units and Positions

Interested in more information? Please visit http://www.ibsolution.de
ENDRA
Enhanced Notes Domino Resource Adapter
by Kogit
ENDRA Add-On – by Kogit GmbH 1/2
– Version Dependencies

Pre-requisites for Lotus Notes and SAP Identity Management Operation

- Identity Center v7.0 SP2 and above
- Lotus Notes client 7.0 or higher
- Lotus Domino server 7.0 or higher
- Platform: based on Domino Server

**ENDRA:**

ENDRA stands for Enhanced Notes Domino Resource Adapter and is a highly functional solution to administrate Domino users. You can use ENDRA as a stand-alone solution or in combination with SAP Identity Management.

The solution supports all default standard administration functions from Lotus Domino. Further, it offers a Domino Administration tool combined with the integration in company processes.

You can find more information on the website: [www.kogit.de](http://www.kogit.de)
Supported operations:

- Reading of user
- Reading of groups
- Add, modify, delete and rename user
- Enable/Disable user

Password related:

- Set productive password
- Reset passwords

Group actions:

- Add group
- Modify Group
- Delete Group
- Assign and de-assign users

Special operations:

- Archiving the group membership and the Id-data
- Change User data in the Domino directory
- Recover deleted user
- Create/Delete Mailing databases
- Extend ID Data
Service Lifecycle Management Framework by HP
HP's Service Lifecycle Management (SLcM) Framework enables managing hardware, software, permissions and other IT services during their complete lifecycle using SAP Identity Management.

Advantages:

- Innovative solution that extends the functionality of SAP Identity Management and allows for the management of any IT services
- Improved user experience by offering a central Service Request Management Portal for all kinds of IT services
- Cost-efficient solution
  - Reduced license and maintenance cost due to the usage of a single tool
  - Reduced complexity by using a single workflow engine
- Utilization of software products of a strategic partner instead of a boutique vendor
Service Lifecycle Management Framework – by HP (2/2)

Features:

- Self-services portal for all required IT-Services
- Order processes for all IT services including approvals can be implemented using SAP Identity Management
- "Service bundles" can simplify ordering commonly used IT services (e.g. the service bundle "sales employee" can contain the hardware, software, devices and permissions that typical sales employees need)
- Flexibility to implement management of additional IT services (e.g. ordering of office supplies)
- Internal cost allocation based on IT services actual usage
- Flexible reporting (e.g. based on cost location, IT services or account usage)

The HP SLcM Framework is available for SAP Identity Management 7.1 and higher. – Interested? Please contact Udo Fink or Holger Flocken
Service Workflow Visualization Tool – by HP
HP's Workflow Visualization Tool (WV Tool) simplifies the life of workflow administrators. It completes the hierarchical view on workflows provided by SAP Identity Management using a process-oriented view.

Features:

- visualizes workflows using an intuitive notation based on UML
- provides workflow administrators with all important information at one glance
  - simplifies troubleshooting
  - helps with quickly creating high-quality workflow documentation
- provides a configurable amount of detailed task information on demand
- makes workflows transparent for users
- based on Web Dynpro, thus easy to integrate into the SAP Identity Management environment

The WV Tool is available for SAP Identity Management 7.1 and above.
Workflow Visualization Tool – by HP (2/2)

Screen Samples

SAP Identity Management

Interested? Please contact Udo Fink or Holger Flocken
Database Connectivity
Database Connectivity

Supported database standards

- ODBC (general standard for database connectivity)
- JDBC (JAVA standard for database connectivity)
- OLE DB (Microsoft standard for database connectivity)

The above standards are supported through the DB vendor client software which is accessed by the different modules in SAP Identity Management

Note: ODBC has in general a lower performance and OLE DB and JDBC is preferred

Supported databases / database types using the above standards:

- Microsoft SQL Server
- IBM UDB (DB2)
- SAP HANA Database
- Microsoft Access
- MySQL
- Oracle database
- Sybase
The Connector Development Kit for Non-SAP Applications – Overview
Purpose
To provide a development toolkit and guidelines for customers and third party vendors to create an SAP Identity Management connector for non-SAP applications.

Components
Identity Center
• Main functionality used here: Identity provisioning

Virtual Directory Server
• Single access point for data updates in multiple repositories
Identity Center Integration
- The connector tasks integrate into the existing (common) provisioning framework in the Identity Center
  - One set of tasks has to be customized to work together with the target application utilizing VDS

Virtual Directory Server Integration
- The generic VDS core functionality has to be extended
  - Source code has to be developed which will be used by VDS to connect to the target application.
Connectivity Architecture

Provisioning Framework
- Independent of repositories and back-ends
- Hooks into the partner’s set of IC connector tasks

IC Tasks (Set From Partner)
- Hooked into the provisioning framework

Virtual Directory Server (VDS)

Connectors from Partners
- Multiple connectors in a virtual tree

Back-Ends (Third-Party Applications)
3rd. Party Connector Certification – Requirements and Process
General information about third party certifications with SAP products is available here: http://www.sdn.sap.com/irj/sdn/interface-certifications

You may contact the SAP Integration and Certification Center (ICC) directly using this mail address: icc@sap.com

The integration scenario offered by the SAP Integration and Certification Center (ICC) is called NW-IDM-CON and it is listed on the Integration Scenario/Interface reference table of the ICC on the SDN (direct link)

Partners of SAP as well as potential partners and independent software vendors (ISVs) are invited to use the Connector Development Kit (CDK) to create an Identity Management connector for their application and to integrate the application in the Identity Management landscape. This connector can then be certified by the SAP ICC.
Questions and Answers

Questions?

For technical questions about identity management please use the SAP Identity Management forum on SCN (try the "Search"):
http://scn.sap.com/community/idm/content

If you are looking for general information about SAP Identity Management, please refer to the public information on the SCN:
http://scn.sap.com/community/idm

For software issues concerning the product "SAP Identity Management" please open a support ticket using component "BC-IDM"