HP Select Identity Software

Connector for SAP Central User Administration (CUA)

Connector Version: 1.02

Installation and Configuration Guide

hp

i n v e n t

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

© Copyright 2006-2007 Hewlett-Packard Development Company, L.P.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/). Portions Copyright © 1999-2003 The Apache Software Foundation. All rights reserved.

Select Identity uses software from the Apache Jakarta Project including:

- Commons-beanutils
- Commons-collections
- Commons-logging
- Commons-digester
- Commons-httpclient
- Element Construction Set (ecs)
- Jakarta-poi
- Jakarta-regexp
- Logging Services (log4j)

Additional third party software used by Select Identity includes:

- JasperReports developed by SourceForge
- iText (for JasperReports) developed by SourceForge
- BeanShell
- Xalan from the Apache XML Project
- Xerces from the Apache XML Project
- Java API for XML Processing from the Apache XML Project
- SOAP developed by the Apache Software Foundation
- JavaMail from SUN Reference Implementation
- Java Secure Socket Extension (JSSE) from SUN Reference Implementation
- Java Cryptography Extension (JCE) from SUN Reference Implementation
- JavaBeans Activation Framework (JAF) from SUN Reference Implementation

- OpenSPML Toolkit from OpenSPML.org

- JGraph developed by JGraph

- Hibernate from Hibernate.org

- BouncyCastle engine for keystore management, bouncycastle.org

This product includes software developed by Teodor Danciu (http://jasperreports.sourceforge.net). Portions Copyright © 2001-2004 Teodor Danciu (teodord@users.sourceforge.net). All rights reserved.

Portions Copyright © 1994-2004 Sun Microsystems, Inc. All Rights Reserved.

This product includes software developed by the Waveset Technologies, Inc. (www.waveset.com). Portions Copyright © 2003 Waveset Technologies, Inc. 6034 West Courtyard Drive, Suite 210, Austin, Texas 78730. All rights reserved.

Portions Copyright © 2001-2004, Gaudenz Alder. All rights reserved.

Trademark Notices

AMD and the AMD logo are trademarks of Advanced Micro Devices, Inc.

Intel and Pentium are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.

JAVA™ is a US trademark of Sun Microsystems, Inc.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California

UNIX® is a registered trademark of The Open Group.

Support

You can visit the HP software support web site at:

http://www.hp.com/go/hpsoftwaresupport

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require an active support contract.

To find more information about support access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

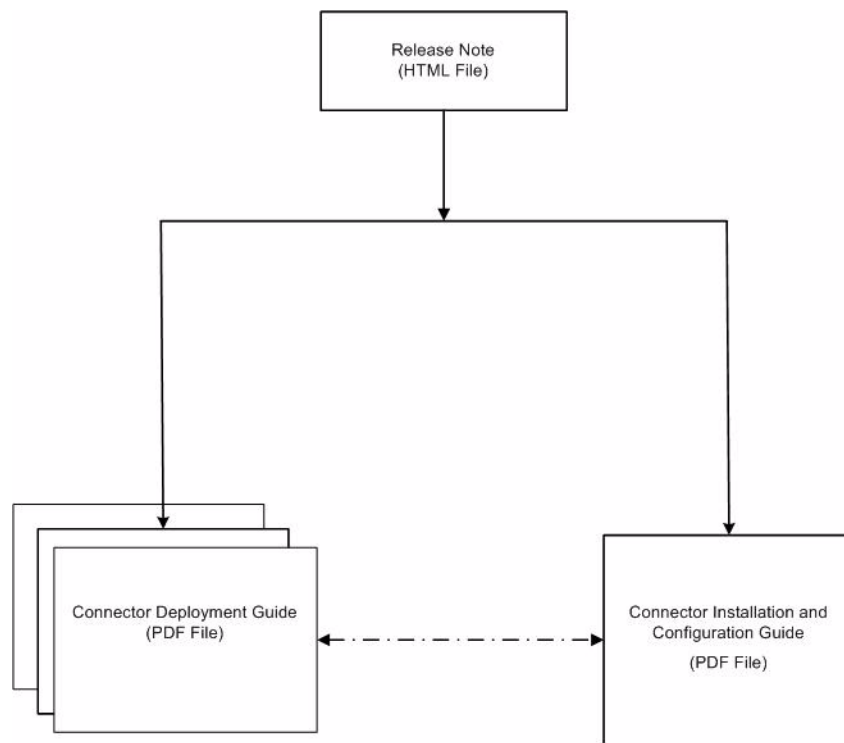# 1 Documentation Map

This chapter describes the organization of HP Select Identity connector documentation and provides necessary information on how to use the documentation set to install and configure the connectors.

Figure 1 illustrates the documentation map for Select Identity connector. For a list of available product documentation, refer to the Table 1.

Figure 1   Documentation Map

Table 1   Connector Documentation

Document Title and Filename	Contents	Location
Release Note `SAP CUA Connector v1.02 Release Note.htm`	This file contains necessary information on new features of the connector, enhancements, known problems or limitations, and support information.	`/Docs/` subdirectory under the connector directory.

Connector Deployment Guide (for Select Identity 4.20)
 	
`connector_deploy_SI4.20.pdf`
 	
Connector Deployment Guide (for Select Identity 4.10-4.13)
 	
`connector_deploy_SI4.13.pdf`
	Connector deployment guides provide detailed information on:
	
	• Deploying a connector on an application server.
	• Configuring a connector with Select Identity.
	
	Refer to these guides when you need generic information on connector installation.
		`/Docs/` root directory on the product's CD media.

Connector Installation and Configuration Guide `SAP CUA_guide.pdf`	Connector installation and configuration guide provides installation instructions for a specific connector. It contains resource specific configuration details.	`/Docs/` subdirectory under the connector directory.

2 Introduction

This chapter gives an overview of the HP Select Identity connector for SAP Central User Administration (CUA). A Select Identity connector for SAP CUA enables you to provision users and manage identities on SAP CUA system. At the end of this chapter, you will be able to know about:

- The benefits of HP Select Identity.
- The role of a connector.
- The connector for SAP CUA.

About HP Select Identity

HP Select Identity provides a new approach to identity management. Select Identity helps you automate the process of provisioning and managing user accounts and access privileges across platforms, applications, and corporate boundaries. Select Identity communicates with the enterprise information system through connectors, and automates the tasks of identity management. The enterprise information system, which is also referred to as **resource**, can be a database, a directory service, or an ERP package, among many others.

About Connectors

You can establish a connection between a resource and Select Identity by using a connector. A connector is resource specific. The combination of Select Identity and connector helps you perform a set of tasks on the resource to manage identity. A connector can be **unidirectional** or **bidirectional**. A unidirectional connector helps you manage identities from Select Identity, but if any change takes place in resource, it cannot communicate that back to Select Identity. On the other hand, a bidirectional connector can reflect the changes made on resource back to Select Identity. This property of bidirectional connectors is known as **reverse synchronization**.

About SAP CUA Connector

The connector for SAP Central User Administration (CUA)— hereafter referred to as SAP CUA connector — communicates with the CUA/non-CUA system of the SAP deployment to provision users. The SAP CUA connector is a unidirectional connector and can perform the following tasks from Select Identity to SAP:

- Add, update, and remove users

- Retrieve user attributes

- Enable and disable users

- Verify a user's existence

- Change user passwords

- Reset user passwords

- Retrieve all entitlements (profiles and roles)

- Grant and revoke entitlements (profiles and roles) to users

➤ This connector can be used with all Select Identity versions.

Overview of Installation Tasks

Before you start installing the connector, you must ensure that system requirements and all the installation prerequisites are met. Refer to the Table 2 for an overview of installation tasks

Table 2   Overview of Installation Tasks

Task Number	Task Name	Reference
1	Install the connector on the Select Identity server.	See Installing the Connector on page 11.
	— Meet the system requirements.	See System Requirements on page 12.
	— Ensure all the prerequisites are met.	See Prerequisite on page 12.
	— Extract contents of the Schema file.	SeeExtracting Contents of the Schema File on page 12.
	— Install the Resource Adapter Archive (RAR) file of the connector.	See Installing the Connector RAR on page 14.
2	Configure the connector with Select Identity.	See Configuring the Connector with Select Identity on page 15.

3 Installing the Connector

This chapter elaborates the procedure to install the SAP CUA connector on the Select Identity server. At the end of this chapter, you will know about

- Software requirements to install the SAP CUA connector.
- Pre-installation tasks.
- Procedure to install the SAP CUA connector.

SAP CUA Connector Files

The SAP CUA connector is packaged in the following files, which are located in the `SAP CUA` directory of the Select Identity Connector CD:

Table 3   SAP CUA Connector Files

Serial Number	File Name	Description
1	`SAPR3CUAConnector_420.rar` for WebSphere `SAPR3CUAConnector_420WL9.rar` for WebLogic	This is the Resource Adapter Archive (RAR) file of the connector. It contains a collection of binary files.
2	`SAPR3CUASchema.zip`	This JAR file contains of the following file: `SAPCUA.xml` – the mapping file to map attributes from SAP to Select Identity. `SAPParamResources.properties` – the properties file to configure password related settings.

System Requirements

The SAP CUA connector is supported in the following environment:

Table 4   Platform Matrix for SAP CUA connector

Select Identity Version	Application Server	Database
4.10-4.20	The SAP CUA connector is supported on all platform configurations of Select Identity 4.10-4.20.	

The SAP CUA connector supports the following SAP versions:

Table 5   SAP CUA Connector Supported SAP Versions

SAP CUA connector	SAP Version and Operating System
SAP CUA Connector 1.01	SAP R/3 4.6c and 4.7 on Microsoft Windows Server 2003 and HP-UX 11.11
	SAP ECC (ERP Central Component) version 6.0 on NetWeaver 04s on Microsoft Windows Server 2003 with Service Pack 2 and AIX 5.3

Prerequisite

Before you start installing the connector, you must download the SAP Java Connector (JCo) API (version 2.1.8) from **http://service.sap.com** and install the API on the application server.

Also, add `<sapjco-install-path>\sapjco.jar` to the `CLASSPATH` environment variable where `<sapjco-install-path>` is the installation directory of the SAP Java Connector (JCo) API.

Extracting Contents of the Schema File

The Schema file of the connector contains necessary mapping information to map resource attributes to Select Identity. Extract contents of the `SAPR3CUASchema.zip` file to a directory that is in the application server `CLASSPATH`. Refer to the *HP Select Identity Connector Deployment Guide* for detailed instruction to extract contents of the schema file.

Modifying the Properties File

After finish extracting contents of the `SAPR3CUASchema.zip` file, you can directly modify properties file (`SAPParamResources.properties`). There are two parameters included:

*   `pwdCaseSensitive=`

This parameter determines whether the connector supports case-sensitive or case-insensitive password. It is available for connector version 1.01 only:

> If `true`, the connector supports case-sensitive password.

> If `false`, the connector supports case-insensitive password.

When you install the connector (version 1.01) for use with SAP R/3 4.6c and 4.7 or SAP ECC 6.0 which is set to case-insensitive, it is recommended to set `pwdCaseSensitive` to `false`, so that the connector setting is consistent with the password policy of SAP.

If the password policy of SAP ECC 6.0 is set to case-sensitive, it is recommended to set `pwdCaseSensitive` to `true`.

> ➤ It is highly recommended to keep the password policy of Select Identity consistent with that of SAP.

- `adminResetPwdAfterFail=`

This parameter determines which one of the two workarounds below the connector will follow when user change password fails.

Both SAP system and Select Identity have their own password policies. When users attempt to change their passwords to SAP through Select Identity, it is possible that the password policy of Select Identity does not comply with that of SAP. In order to solve this conflict, two workarounds are available with connector version v1.01 to implement user password reset/self-change. You can modify the value of parameter `adminResetPwdAfterFail` to choose one of the two workarounds:

> If `false`, the connector will follow Workaround 1 to prompt password change fail.

> If `true`, the connector will follow Workaround 2 to force change password to SAP.

— Workaround 1

When a user sets a password to SAP in Select Identity, if the new password the user provides does not comply with SAP password policy (for example, same as one of the previously used five passwords), Select Identity will prompt the user password reset failure. And, the user account in SAP is locked, the user will not be able to log in. The user shall contact the SAP administrator for password policy details in order to provide a password that complies with the SAP password policy.

The positive point of this approach is that the new password provided by the user will always comply with SAP password policy; negative point is the increase in admin workload resulting from users frequently seeking for admin support due to password change failure.

— Workaround 2

Similar to Workaround 1, the difference is that if the user sets the password to an improper one, Select Identity will force change SAP password to the user-specified one and return success message to the user. But when logging in to SAP next time, the user will be prompted to change password again.

The negative point of this approach is that a password that does not comply with SAP password policy will exist in SAP for a short period of time; the positive point is that user account will not be locked, and no increase in admin workload.

Installing the Connector RAR

To install the RAR file of the connector (such as `SAPR3CUAConnector_420.rar`) on the Select Identity server, you must copy the file to a local subdirectory on the Select Identity server, and then deploy on the application server. Refer to the *HP Select Identity Connector Deployment Guide* for detailed information on deploying a RAR file on an application server.

☛ While deploying the RAR on WebSphere, enter the JNDI Pool Name as **eis/SAPCUAConnector**.

4 Configuring the Connector with Select Identity

This chapter describes the procedure to configure the SAP CUA connector with Select Identity and the connector specific parameters that you must provide while configuring the connector with Select Identity.

Configuration Procedure

After you deploy the connector RAR on application server, you must configure the connector with Select Identity. Perform the following steps to configure the SAP CUA connector with Select Identity.

1   Add a New Connector

2   Add a New Resource

3   Map Attributes

Add a New Connector

Add a new connector in Select Identity by using the user interface. While adding the connector, do the following:

*   In the Connector Name text box, specify a name for the connector.

*   In the Pool Name text box, enter **eis/SAPCUAConnector**.

*   Select **No** for the Mapper Available section.

Refer to the *HP Select Identity Connector Deployment Guide* for detailed information on adding a new connector in Select Identity.

Add a New Resource

Add a new resource in Select Identity that uses the newly added connector. Refer to the *HP Select Identity Connector Deployment Guide* for detailed instructions on adding a resource in Select Identity.

Refer to the following table while entering the parameters in the Basic Information and the Access Information pages:

Table 6   Resource Configuration Parameters

Field Name	Sample Values	Description
Resource Name	sap_server	Name given to the resource.
Connector Name	SAP_CUA	
Authoritative Source	No	Whether this resource is a system that is considered to be the authoritative source for user data in your environment. You must specify **No** because the connector cannot synchronize account data with the Select Identity server.
User Name	admin	User name of an SAP user with privileges to add other users, and also execute Remote Function Calls (RFCs). If this user does not have RFC authorization, the connector will throw exceptions.
Password	password123	Password of the above user.
Client ID	00	Server client ID.
Language	EN	Language for the system.
Host Address	server.company.com	The address of the server.
System Number	00	The system number.
Mapping File	SAPCUA.xml	Name of the resource mapping file.
IsEmployee	Yes — if the resource being created for SAP HR No — if the resource is being created for SAP users.	
IsCUA	Yes - If the resource is SAP CUA system. No - If the resource is SAP non-CUA System	

Map Attributes

After successfully adding a resource for SAP CUA connector, you must map the resource attributes to Select Identity attributes. Add new attributes to Select Identity if necessary. Refer to the *HP Select Identity Connector Deployment Guide* for more information on mapping and creating attributes.

While mapping the attributes, refer to the following table for resource specific mapping information.

Table 7   SAP Mapping Information

Select Identity Resource Attribute	SAP Attribute	Description
Username	Username	Key field on the resource.
Password	Password	This is a mandatory attribute.
Firstname	Firstname	
Lastname	Lastname	This is a mandatory attribute.
Email	E_Mail	
Costcenter	Kostl	

After mapping the attributes, you can use the connector to create a service, or you can associate the connector with an existing service. Refer to the *Service Studio* chapter of the *HP Select Identity Administration Online Help* for information on Select Identity services.

5 Uninstalling the Connector

To uninstall a connector from Select Identity, perform the following steps:

* Remove all resource dependencies.

* Delete the connector from Select Identity.

* Delete the connector from application server.

See *HP Select Identity Connector Deployment Guide* for more information on deleting the connector from application server and Select Identity.