HP Select Identity Software

Connector for eTrust CA- ACF2 (Bidirectional LDAP Based)

Software Version: 1.02

Installation and Configuration Guide

Document Release Date: September 2007
Software Release Date: September 2007

Legal Notices

Warranty

Restricted Rights Legend

Copyright Notices

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

Trademark Notices

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 HP Select Identity connector. For a list of available product documentation, refer to the Table 1.

Figure 1 Documentation Map

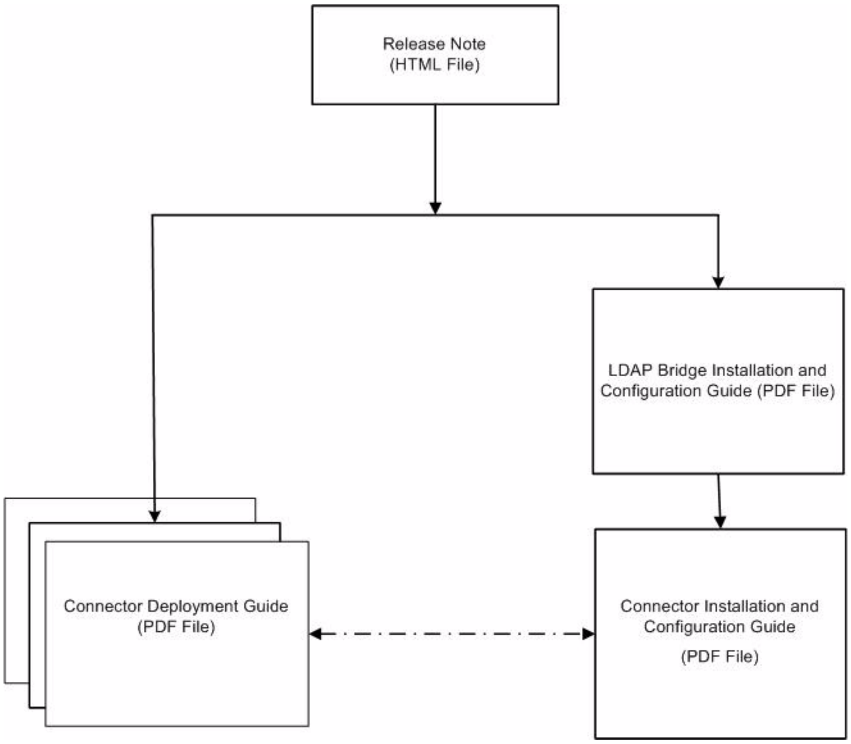

Release Note
(HTML File)
LDAP Bridge Installation and Configuration Guide (PDF File)
Connector Deployment Guide
(PDF File)
Connector Installation and Configuration Guide
(PDF File)

Table 1 Connector Documentation

Document Title and Filename	Contents	Location
Release Note `ACF2 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 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 Deployment Guide (for Select Identity 4.10-4.13) `connector_deploy_SI4.13.pdf`		
LDAP Bridge Installation and Configuration Guide `LDAP_Bridge_guide.pdf`	LDAP Bridge installation and configuration guide provides installation instructions for the LDAP Bridge for the ACF2 connector.	`/LDAP_Bridge/Docs/` subdirectory under the connector directory.
Connector Installation and Configuration Guide `ACF2_guide.pdf`	Connector installation and configuration guide provides installation instructions for the ACF2 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 eTrust CA- ACF2. An HP Select Identity connector for eTrust CA- ACF2 enables you to provision users and manage identities on ACF2 server. 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 eTrust CA- ACF2.

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 ACF2 Connector

The bidirectional LDAP based connector for eTrust CA- ACF2— hereafter referred to as ACF2 connector — enables Select Identity to perform the following tasks on ACF2 server:

- Add, update, and remove users
- Retrieve user attributes
- Verify a user’s existence

- Change user passwords
- Reset user passwords
- Expire passwords
- Validate passwords
- Retrieve all entitlements (the LDAP Bridge for ACF2 currently does not support entitlements)
- Retrieve a list of supported user attributes

ACF2 is a bidirectional Lightweight Directory Access Protocol Version 3 (LDAPv3) compliant connector that pushes changes made to user data in Select Identity database to a target ACF2 server. The connector uses the Java LDAP Application Program Interfaces (APIs) to provision users and their entitlements in the LDAP server, which in turn pushes the data to the ACF2 server.

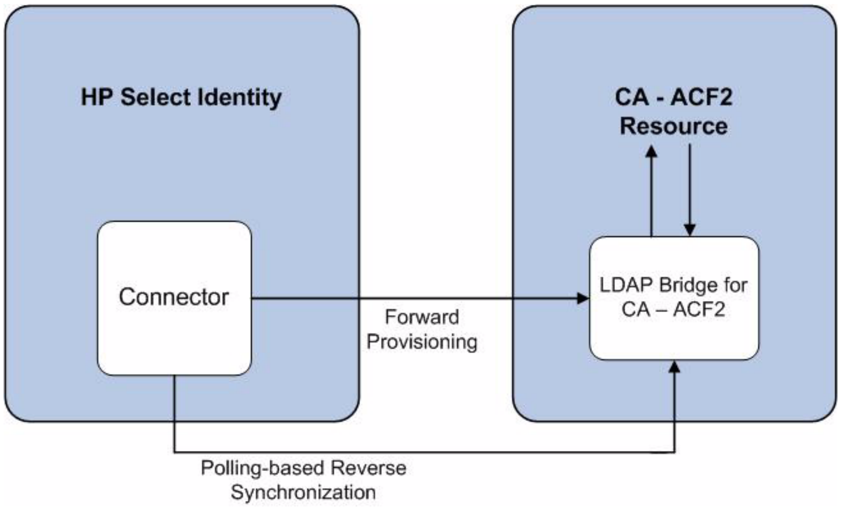
The reverse synchronization feature reconciles user account changes made on the ACF2 resource with Select Identity. Select Identity periodically polls the ACF2 resource to retrieve changes through the connector.

➤ This connector can be used with Select Identity 4.10-4.20.

High-Level Architecture

Figure 2 illustrates a high-level architecture of ACF2 connector. You must install the connector on Select Identity server and the agent on resource system. The LDAP Bridge helps synchronizing the changes made on ACF2 server with Select Identity.

Figure 2 High-Level Architecture of the Connector



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 Organization of Tasks

Task Number	Task Name	Reference
1	Install the connector on the Select Identity server.	See Installing the Connector on page 13
	— Meet the system requirements.	See System Requirements on page 14.
	— Install the LDAP Bridge.	Refer to the *HP Select Identity CA ACF2 LDAP Bridge Installation and Configuration Guide*.
	— Extract contents of the Schema file (file that contains the mapping files for the connector) to location on the Select Identity server.	See Extracting Contents of the Schema File on page 14.
	— Verify the configurable parameters in the `LDAPBridgeConfig.properties` file.	See Verifying Configurable Parameters on page 14.
	— Install the Resource Adapter Archive (RAR) of the connector on an application server.	See Installing the Connector RAR on page 16.

Table 2 Organization of Tasks (cont’d)

Task Number	Task Name	Reference
2	Configure the connector with the Select Identity server.	See Configuring the Connector with Select Identity on page 17.
	— Add a new connector to Select Identity.	See Add a New Connector on page 17
	— Add a new resource to Select Identity.	See Add a New Resource on page 17.
	— Map the resource attributes to Select Identity attributes.	See Map Attributes on page 19.
	— Configure Workflow External Call.	See Configure Workflow External Call on Select Identity on page 20.
	— Configure Select Identity to support polling based reverse synchronization.	See Configure Select Identity Polling for Reverse Provisioning on page 21.

3 Installing the Connector

This chapter elaborates the procedure to install ACF2 connector on Select Identity server. At the end of this chapter, you will know about

- Software requirements to install the ACF2 connector.
- Prerequisite conditions to install ACF2 connector.
- Procedure to install ACF2 connector.

ACF2 Connector Files

The ACF2 connector is packaged in the following files in the `ACF2` directory on the Select Identity Connector CD:

Table 3 ACF2 Connector Files

Serial Number	File Name	Description
1	• `ACF2LDAPConnector_420.rar` for WebSphere • `ACF2LDAPConnector_420WL9.rar` for WebLogic	The Resource Adapter Archive (RAR) file contains the connector binaries.
2	`ACF2.jar`	The Schema file contains the mapping files that contain attribute information of eTrust CA- ACF2.
3	`hpv33a.pax.Z`	This file contains the LDAP Bridge, which has to be installed in resource ACF2 server. Refer to the *HP Select Identity CA ACF2 LDAP Bridge Installation and Configuration Guide* for more information on this.

System Requirements

The ACF2 connector is supported in the following environment:

Table 4 Platform Matrix for ACF2 connector

Select Identity Version	Application Server	Database
4.10-4.20	The ACF2 connector is supported on all the platform configurations of Select Identity 4.10-4.20.	

Installing the LDAP Bridge

Before installing the connector on Select Identity system, you must install LDAP bridge on ACF2 resource. Refer to the *HP Select Identity CA ACF2 LDAP Bridge Installation and Configuration Guide* for more information on installing LDAP bridge on ACF2 server.

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 `ACF2.jar` 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.

Verifying Configurable Parameters

Before you start installing the ACF2 connector, you must verify some configurable properties in the `LDAPBridgeConfig.properties` file, which is present in the `ACF2.jar` file. Verify the parameters and change the values if they do not match with the values as mentioned below.

- `entitlement-delimiter=|`

  It contains the string delimiter that is displayed between an entitlement type and its name.

- `modify_replace=false`

  This parameter that can be set to true or false. When it is set to false, the ACF2 Connector uses modify/add and modify/delete operations to support multi-value attribute. When it is set to true, the connector uses modify/replace operation to support multi-value attribute.

- `attributeValue-delimiter=|`

  It contains the string delimiter that is used to separate attribute values for multi valued attribute.

- `attribute-begins=[[`

  `attribute-ends=]]`

These parameters wrap the special base64 encoded attribute values while sending to connector from Select Identity.

- `checkModValues=true`

  If this is set to true, the ACF2 connector compares each attribute values with the values in the resource during user modify operation. If user modifies an attribute that does not support modify operation, then the connector can detect it and throws an exception to the user. If the `checkModValues` parameter is set to false, attribute values are not compared. If you modify an attribute that does not support modify operation, the change will still be sent to ACF2. You must not change an attribute value that does not support modify operation, when `checkModValues` is set to false.

- `dualLink-support=1`

  This parameter specifies whether a Link is a User Link or a Group Link. If it is 1, then it is a User Link. For ACF2, you must set this parameter to 1.

- `multivalue-support=false`

  This parameter specifies whether Select Identity supports multi-value attributes or not. This property is used in the reverse provisioning. When a multi-value attribute is detected in the `replog` during polling, all the values of the multi-value attribute are combined as single-value string.

  If true - Select Identity supports multi-value attributes.
  If false - Select Identity does not support multi-value attributes.

- `mergeChangeLog=true`

  If this is set to true, multiple add/modify change-log entries for a user in the `replog` file are merged into a single change-log entry.

- `unlink-before-terminate=true`

  If you do not want to unlink an entitlements while performing a `terminate user` operation, set this flag to true.

- `ignore-non-updateable-attr-values=true`

  If it is set to true, and from Select Identity if you change the value an attribute that cannot be updated (attribute that does not support `UPDATE` operation), the connector logs a warning message in a log file, but does not throw any exception. If it is set to true, then connector logs warning message as well as throws an exception, when a non-updatable attribute value is changed from Select Identity.

- `ignore-deleteable-attr-values=true`

  If true and the attribute supports UPDATE operation and the value of an attribute is sent as empty from Select Identity to connector but its value on ACF2 is not empty, then the connector will not delete the attribute.

  If false and the attribute supports UPDATE operation and the value of an attribute is sent as empty from Select Identity to connector but its value on ACF2 is not empty, then the connector will delete the attribute.

Installing the Connector RAR

To install the RAR file of the connector (such as `ACF2LDAPConnector_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/ACF2Connector`**.

After deploying the connector RAR on application server and installing the scripts, you must configure ACF2 connector with Select Identity. Refer to Configuring the Connector with Select Identity on page 17 for configuration steps.

4 Configuring the Connector with Select Identity

This chapter describes the procedure to configure the ACF2 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 ACF2 connector with Select Identity.

1. Add a New Connector
2. Add a New Resource
3. Map Attributes
4. Configure Workflow External Call on Select Identity
5. Configure Select Identity Polling for Reverse Provisioning

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/ACF2Connector`**.
- 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 5 Resource Configuration Parameters

Field Name	Sample Values	Description
Resource Name	ACF2	Name given to the resource.
Connector Name	ACF2Connector	The newly created connector.
Authoritative Source	Yes	Whether this resource is a system that is considered to be the authoritative source for user data in your environment. You must specify **Yes** because the connector can synchronize account data with the Select Identity server.
Associate to Group	Selected	Whether the system uses the concept of groups. For this connector, select this option.
Access URL	ldap:// 216.140.203.112:2389	URL for connecting to the resource (the format is IP:port).
Suffix	o=hp.com	Default root suffix.

Login Name	uid=secint2,
	ou=people,
	o=hp.com
		Login name of the administrative user.

Password	PASWD	Password of the specified user.
Default User Suffix	ou=people	Suffix where all users exist.
Default Group Suffix	ou=people	Suffix where all groups exist.
Mapping File	`ACF2.xml`	Name of the file that specifies the attribute mappings. This file should exist in the classpath of the application server. Click **View** to open the file in a browser. If this file cannot be viewed, Select Identity could not locate it.
Select Identity Locale	en_US	Locale-specific information. If Country = US and Language = English, current locale string is en_US.

After entering the resource access information, User Reconciliation Policy page appears. On the User Reconciliation Policy page, perform the following:

1. Select the Polling Enable checkbox.
2. Set the polling interval as one day.
3. Under Add and Modify sections, set Reconciliation Workflow as Select Identity Recon User Enable Disable Workflow from the drop-down box.

Map Attributes

After successfully adding a resource for the ACF2 connector, you must map the resource attributes to Select Identity attributes. Refer to the *HP Select Identity Connector Deployment Guide* for information on mapping and creating attributes. While mapping attributes, refer to the following table for resource specific mapping information.

Table 6 ACF2 Mapping Information

Select Identity Resource Attribute	Connector Attribute	Attribute on ACF2 LDAP Server	Attribute in ACF2	Description	Typical Value
User Name	uid	uid	LID	The ACID, which must be less than or equal to seven characters. *This attribute is mandatory for user creation*.	QAHP1000
Password	Password	userPassword	PASSWORD	Password for this ACID, which must be less than or equal to eight characters. *This attribute is mandatory for user creation.* (length 5 - 8 characters)	PASSWORD
cn	cn	cn	NAME	Username in ACF2; all ACF2 ACIDs require a name.	TEST NAME
DN	DN	DN		Distinguished Name of the entry	No value to be provided.

Table 6 ACF2 Mapping Information (cont'd)

Select Identity Resource Attribute	Connector Attribute	Attribute on ACF2 LDAP Server	Attribute in ACF2	Description	Typical Value
objectclass	objectclass	objectclass		LDAP object classes used for user creation. *This attribute is mandatory for user creation*	For User: top;person;organizationalPerson;inetOrgPerson;acf2Person
Acf2Priv	Acf2Priv	Acf2Priv	Privilege		Add value TSO to enable TSO for this user, add NOTSO to disable access.
acfTsoPriv	acfTsoPriv	acfTsoPriv			Multi-valued, defines various TSO privileges. To add a privilege, specify the appropriate value in the acf2Priv attribute. To remove a privilege (LDAP modify only), specify the value prefixed by NO.

Configure Workflow External Call on Select Identity

To enable reverse synchronization, you must configure the workflow external call for user enable/ disable operation on Select Identity for ACF2 connector. Refer to *HP Select Identity Deployment Guide* for information on configuring user enable/disable workflow external call. While configuring, enter the parameters as given in the table below.

Table 7 User Enable/Disable Parameters for ACF2 Connector

Serial Number	Parameter Name	Parameter Value
1	AttributeName	acf2Priv
2	EnableValue	SUSPEND
3	DisableValue	SUSPEND

Table 7 User Enable/Disable Parameters for ACF2 Connector (cont'd)

Serial Number	Parameter Name	Parameter Value
4	UserName	Select Identity administrative user name, for example, sisa.
5	Password	Select Identity administrative password. For example, abc123.
6	Url	http://localhost:7001/lmz/webservice

Configure Select Identity Polling for Reverse Provisioning

Reverse synchronization in ACF2 connector is achieved by polling.

Each time the polling is invoked, the following sequences take place in the background:

1. The polling batch task is invoked
2. The polling batch gets the resource name from the `TruAccess.properties` property file and get the ChangeLogs made from the last polling via the connector.
3. The polling batch task converts all the ChangeLogs into an SPML file, and the SPML file will be converted to a Request using the SPML parser and submitted to the Select Identity Reconciliation engine. Then ReconcilationHelper is called to execute all the Modify Requests.
4. In the provisioning stage of request execution, Select Identity will be updated with the changes in the resource.

To configure polling, you must perform the following additional configuration on Select Identity 4.10-4.20.

You must add the a new property to `TruAccess.properties` file to enable polling. To the existing file, add c`om.hp.ovsi.connector.changeLog.maxCount=`*`<maxChangeLogCount>`*

where *<maxChangeLogCount>* is a positive number.

For example, you can set c`om.hp.ovsi.connector.changeLog.maxCount=500`

This property indicates the maximum number of changelogs that will be retrieved in one polling action from one resource.

After configuring the connector with Select Identity, you can use the connector to create a service, or you can associate the connector with an existing service.

- On Select Identity, if ACF2 service view has some attributes as mandatory, all of them should exist on ACF2 LDAP server and they should be sent when reverse add request comes from connector. That is, the only attributes that are coming in reverse add request can be mandatory in Select Identity Service view, if it is mandatory in view and it does not come in reverse add request, request will be rejected by Select Identity.
- In Select Identity service view, Password attribute should not be a mandatory attribute.This is because, at present, ACF2 reverse provisioning does not support Password attribute. If it is made as mandatory, all reverse add requests will be rejected.

5 Uninstalling the Connector

If you want 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 Deployment Guide* to for information on deleting a connector from Select Identity and application server.