HP Select Identity Software

Connector for IBM Resource Access Control Facility (Bidirectional LDAP Based)

Software Version: 1.12

Installation and Configuration Guide

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

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

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

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

Figure 1 Documentation Map

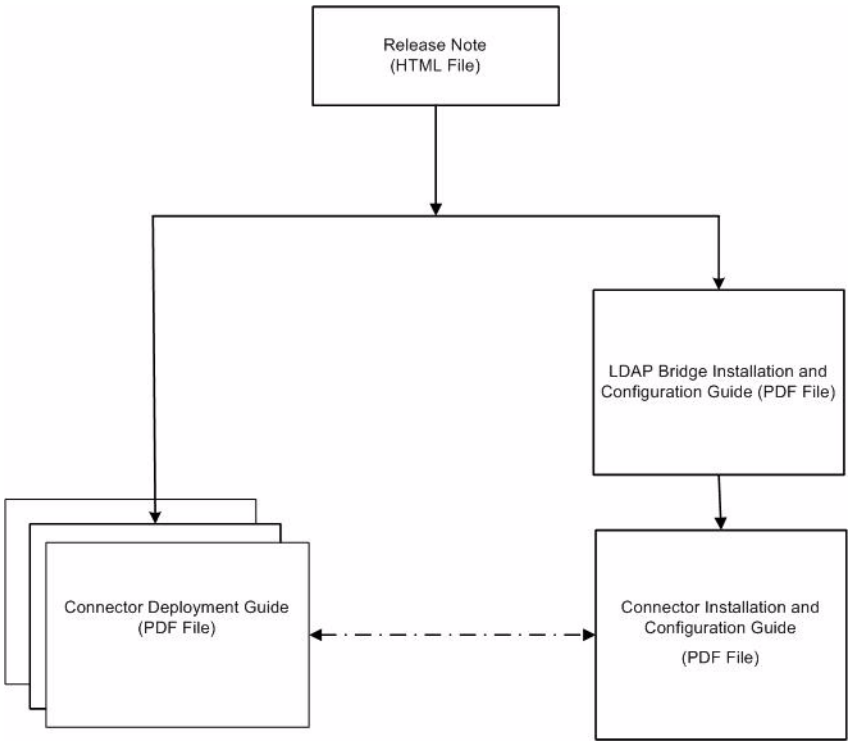


Table 1 Connector Documentation

Document Title and Filename	Contents	Location
Release Note `RACF Connector v1.12 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`		
Connector Deployment Guide (for Select Identity 4.0-4.01) `connector_deploy_SI4.pdf`		
Connector Deployment Guide (for Select Identity 3.3.1) `connector_deploy_SI3.3.1.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 RACF connector.	`/LDAP_Bridge/Docs/` subdirectory under the connector directory.
Connector Installation and Configuration Guide `RACF_guide.pdf`	Connector installation and configuration guide provides installation instructions for the RACF 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 IBM Resource Access Control Facility. An HP Select Identity connector for IBM Resource Access Control Facility enables you to provision users and manage identities on RACF 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 IBM Resource Access Control Facility.

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 RACF Connector

The bidirectional LDAP based connector for IBM Resource Access Control Facility server—hereafter referred to as RACF connector — enables Select Identity to perform the following tasks in RACF server:

- Add, update, and remove users
- Retrieve user attributes

- Enable and disable users
- Verify a user's existence
- Change user passwords
- Reset user passwords
- Expire passwords
- Validate passwords
- Retrieve all entitlements
- Retrieve a list of supported user attributes
- Grant and revoke entitlements to and from users

RACF 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 RACF 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 RACF server.

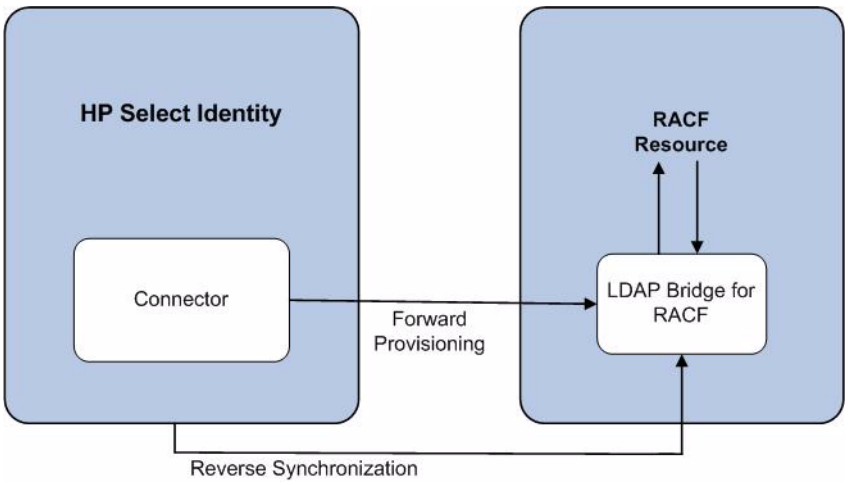
The reverse synchronization feature reconciles user account changes made on the RACF resource with Select Identity. Select Identity periodically polls the RACF resource to retrieve changes through the connector.

This connector can be used with all versions of Select Identity (3.3.1-4.20).

High-Level Architecture

Figure 2 illustrates a high-level architecture of RACF 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 RACF 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 RACF 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 17.

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 19.
	— Add a new connector to Select Identity.	See Add a New Connector on page 19
	— Add a new resource to Select Identity.	See Add a New Resource on page 19.
	— Map the resource attributes to Select Identity attributes.	See Map Attributes on page 23.
	— Create Time Sharing Option Segment in Select Identity.	See Create Time Sharing Option (TSO) Segment on page 25.
	— Configure Workflow External Call.	See Configure Workflow External Call on Select Identity on page 28.
	— Configure Select Identity to support polling based reverse synchronization.	See Configure Select Identity Polling for Reverse Provisioning on page 29.

3 Installing the Connector

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

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

RACF Connector Files

The RACF connector is packaged in the following files in the `Bidirectional LDAP Connector - RACF` directory on the Select Identity Connector CD:

Table 3 RACF Connector Files

Serial Number	File Name	Description
1	• `RACFLdapBridgeConnector_420.rar` for WebSphere • `RACFLdapBridgeConnector_420WL9.rar` for WebLogic	The Resource Adapter Archive (RAR) file contains the connector binaries.
2	`RACF.jar`	The Schema file contains the mapping files that contain attribute information of IBM Resource Access Control Facility.
3	`hpv33r.pax.Z`	This file contains the LDAP Bridge, which has to be installed in resource RACF server. Refer to the *HP Select Identity RACF LDAP Bridge Installation and Configuration Guide* for more information on this.

System Requirements

The RACF connector is supported in the following environment:

Table 4 Platform Matrix for RACF connector

Select Identity Version	Application Server	Database
3.3.1	Websphere 5.1.1.7 on Windows 2003 Server.	Oracle 9i
4.01-4.20	The RACF connector is supported on all the platform configurations of Select Identity 4.01-4.20.	

Installing the LDAP Bridge

Before installing the connector on Select Identity system, you must install LDAP bridge on RACF resource. Refer to the *HP Select Identity RACF LDAP Bridge Installation and Configuration Guide* for more information on installing LDAP bridge on RACF 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 `RACF.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 RACF connector, you must verify some configurable properties in the `LDAPBridgeConfig.properties` file, which is present in the `RACF.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 RACF 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 RACF 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 RACF. 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 RACF, 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 (atrribute 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 RACF 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 RACF is not empty, then the connector will delete the attribute.

- `send_entitlements_as_attrs_in_reverse=false`

  If it is set to true and `multivalue-support` is set to false, then connector sends the entitlement attribute change as the latest value from the resource as a single-valued string separated by a delimiter.

If it is set to true and `multivalue-support` is set to true, then connector sends the entitlement attribute change as the only add/delete sub value.

If it is set to false, then connector sends the entitlement attribute change as regular entitlements with add/delete entitlements.

Installing RACF Certificate on Select Identity 4.20

Perform the following steps to install the RACF Bidirectional LDAP certificate:

1. Create and configure Select Identity trust store and properties, if not already created.
   a. Create the trustore;
   b. Generate a properties file that is corresponding to the trustore file.

   Refer to *Creating the Trust Store* section of *HP Select Identity Installation Guide* for detailed instructions on creating keystore, trustore, and properties.
2. Import certificate representing RACF resource or issuer of RACF resource to Select Identity trust store:
   a. Get RACF certificate;
   b. Import the certificate into the trustore file you created in the previous step.

   Refer to *Creating the Trust Store* section of *HP Select Identity Installation Guide* for detailed instructions on creating keystore, trustore, and properties.
3. If a resource requires a specific client certificate, you must either generate the client certificate or import the client certificate into the key store:
   a. Create the key store file;
   b. Generate the certificate that represents Select Identity server if no certificate available. Or, import the certificate that represents Select Identity server if a certificate already exists.
   c. Generate the properties file that is corresponding to the keystore.

   For more information, refer to *Creating the Key Store and Key Pairs for Mutual Authentication and/or Secure Object Migration* section of *HP Select Identity Installation Guide*.
4. Register the key store and trust store and select the Select Identity client certificate, if not already done.
   a. Open the security setup tool in Select Identity;
   b. Register the keystore properties to Select Identity;
   c. Register the trustore properties to Select Identity;
   d. Select certificate represent Select Identity server if needed.

   For detailed instructions, refer to *Configure System Security* topic in *HP Select Identity Administration Online Help*.

Rotate Keys

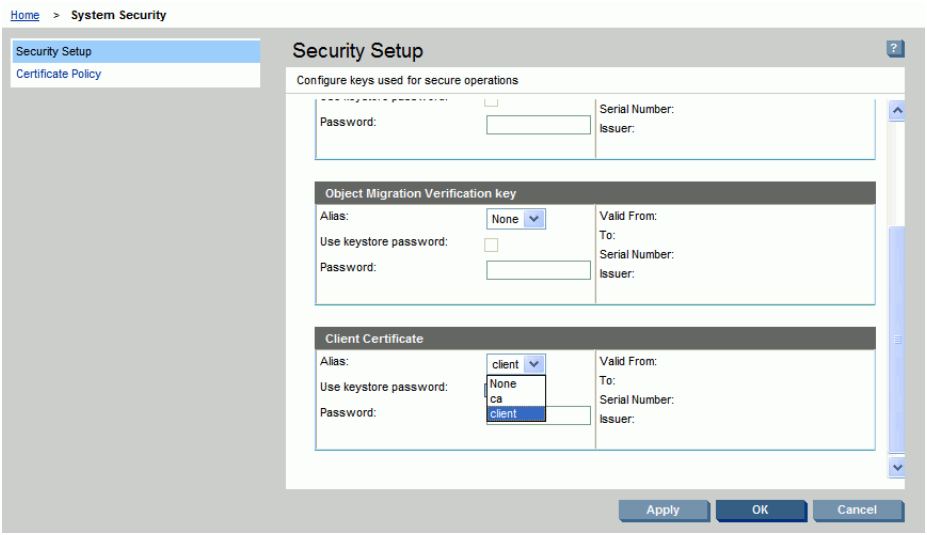
Key rotation is a process that Select Identity can use different keys to connect to a resource. The process is:

1 Generate new key pair in keystore.

For detailed instructions, refer to *Creating the Mutual Authentication Key store* section of *HP Select Identity Installation Guide*.

2 Change key alias in system security setup:

a From the Tools menu, select **System Security** → **Security Setup**. The Security Setup page displays.



b Under Client Certificate section, select the new-generated certificate.

For WebSphere, make sure that `sunjce_provider.jar` file is in <*appserver_home*>`/java/jre/lib/ext` directory, and add the following line into `java.securtity` file which is present in <*appserver_home*>`/java/jre/lib/securtiy` directory:

`security.provider.8=com.sun.security.sasl.Provider`.

Installing the Connector RAR

To install the RAR file of the connector (such as `RACFLdapBridgeConnector_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/RACFConnector`**.

After deploying the connector RAR on application server and installing the scripts, you must configure RACF connector with Select Identity. Refer to Configuring the Connector with Select Identity on page 19 for configuration steps.

4 Configuring the Connector with Select Identity

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

1 Add a New Connector

2 Add a New Resource

3 Map Attributes

4 Create Time Sharing Option (TSO) Segment

5 Configure Workflow External Call on Select Identity

6 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/RACFConnector`**.
- 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	Comment
Resource Name	RACF	Name given to the resource.	
Connector Name	RACFResource	The newly deployed connector.	Known as Resource Type in Select Identity 3.3.1.
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.	
Associate to Group	Selected	Whether the system uses the concept of groups. For this connector, select this option.	Applicable only for Select Identity 3.3.1.
Access URL	ldap://rs42.hp.com:2389	URL for connecting to the resource (the format is IP:port).	
Suffix	o=hp.com	Default root suffix.	
Login Name	uid=DMON07, ou=people, o=hp.com	Login name of the administrative user.	*For Non-SSL and one-way SSL connection, this attribute is mandatory for resource creation*; If Authentication Mechanism is `External`, set this attribute null.
Password	DMON07	Password of the specified user.	*For Non-SSL and one-way SSL connection, this attribute is mandatory for resource creation;* If Authentication Mechanism is `External`, set this attribute null.
Default User Suffix	ou=people	Suffix where all users exist.	
passPluginSuffix	ou=no plugin sufffix	Password Plug-in Suffix, not applicable to RACF.	

Table 5 Resource Configuration Parameters (cont'd)

Field Name	Sample Values	Description	Comment
Default Group Suffix	ou=Groups	Suffix where all groups exist.	
Mapping File	`RACF.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.	

Table 5 Resource Configuration Parameters (cont'd)

Field Name	Sample Values	Description	Comment
CRL Flag	false	Indicates if the resource performs CRL check. This flag works with CRL check flag in **Tools → System Security → Security Setup → Certificate Policy** page. If these two flags are both true, the connector will perform CRL check.	
Usage Flag	false	Indicates if the connector performs usage check. This flag works with usage check flag in **Tools → System Security → Security Setup → Certificate Policy** page. If these two flags are both true, the connector will perform Usage check.	
Authentication Mechanism	simple/ external	This is for SSL connections only. If you are connecting to non-SSL connection, leave it blank. `Simple` indicates that the connector uses `username/ password` as authentication credential. `External` is only effective when connect to two-way-SSL. `External` indicates that the connector uses External SASL merchanism to authenticate user credential, which means LDAP bridge will check certification provided by the connector to determine which user is connecting in ldap bridge.	

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 section, 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 RACF 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 RACF Mapping Information

Select Identity Resource Attribute	Connector Attribute	Attribute on RACF LDAP Bridge	Attribute in RACF	Description	Typical Value
UserName	uid	uid	User-ID	The ACID. This must be less than or equal to seven characters. This attribute is mandatory for user creation.	DMU1000
Password	Password	racfPassword	PASSWORD	Password for this ACID, which must be less than or equal to eight characters. This attribute is mandatory for user creation.	PASSWORD For ldap bridge v3.5 or above, the mapping field on LDAP Bridge is *racfPassword* for password sync instead of *userPassword*.
cn	cn	cn	NAME	Username in RACF; all racf ACIDs require a name. This attribute is mandatory for user creation.	TEST NAME
DN	DN	DN		Distinguished Name of the entry	No value to be provided.

Table 6 RACF Mapping Information (cont'd)

Select Identity Resource Attribute	Connector Attribute	Attribute on RACF LDAP Bridge	Attribute in RACF	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|racfUser` For Group: `groupOfNames|racfGroup|top`
racfGroup	racfGroup	racfGroup	GROUP	*A group added to this ACID.*	DMG0020
racfAdsp	racfAdsp	racfAdsp	ADSP		TRUE / FALSE
racfGrpacc	racfGrpacc	racfGrpacc	Group Access		TRUE / FALSE
racfRestricted	racfRestricted	racfRestricted	Restricted		TRUE / FALSE
racfClauth	racfClauth	racfClauth	Class Auths	multi valued attribute	ACCTNUM;TSOAUTH;TSOPROC;USE
racfAuthority	racfAuthority	racfAuthority	Group Authority	single valued attribute	USE, CREATE, CONNECT, and JOIN
racfUacc	racfUacc	racfUacc	Universal	single valued attribute	ALTER, CONTROL, UPDATE, READ, and NONE
racfPasswordInterval	racfPasswordInterval	racfPasswordInterval	Password Interval		180 (days)
racfResumeDate	racfResumeDate	racfResumeDate	Resume Date		mm/dd/yy
racfRevokeDate	racfRevokeDate	racfRevokeDate	Revoke Date		mm/dd/yy
racfRevoke	racfRevoke	racfRevoke	Revoke	Attribute used for Enable/ disable User	For User Enable:FALSE For User Disable:TRUE

Table 6 RACF Mapping Information (cont'd)

Select Identity Resource Attribute	Connector Attribute	Attribute on RACF LDAP Bridge	Attribute in RACF	Description	Typical Value
racfAuditor	racfAuditor	racfAuditor	Auditor		TRUE / FALSE
racfSpecial	racfSpecial	racfSpecial	Security Level		TRUE / FALSE
racfUaudit	racfUaudit	racfUaudit	User Audit		TRUE / FALSE
racfModifyDate	racfModifyDate	racfModifyDate	Last Modified Date		2006-03-24 (any date) mm/dd/yy
racfNopassword	racfNopassword	racfNopassword	No Password		TRUE / FALSE
racfModifierGroup	racfModifierGroup	racfModifierGroup	Last Modifier Group		DMUSER1 (group name)
racfModifierUser	racfModifierUser	racfModifierUser	Last Modifier User		DMON06 (user name)

Create Time Sharing Option (TSO) Segment

RACF supports creation of Time Sharing Option (TSO) segments. In the LDAP Bridge the segments are represented as sub entry for the user and the bridge will create the segment in the RACF server.For example, a user named 'testUser' having distinguished name (DN) as uid=testUser,ou=people,o=hp.com can have the segment racfSegment=TSO with DN as racfSegment=TSO,uid=testUser,ou=people,o=hp.com.

To add a user from Select Identity in RACF with TSO segment we have to create an additional RACF resource in Select Identity. Perform the following steps to create an additional RACF resource in Select Identity.

1 Add a new resource – You must add a new resource to Select Identity that uses the newly added connector. While entering the resource parameters for RACF connector, refer to the table below.

Table 5A Resource Configuration Parameters for TSO Resource

Field Name	Sample Values	Description	Comment
Resource Name	RACF_TSO	Name given to the resource.	
Connector Name	RACFResource	The newly created connector.	Known as Resource Type in Select Identity 3.3.1.
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.	
Associate to Group	Selected	Whether the system uses the concept of groups. For this connector, select this option.	Applicable only on Select Identity 3.3.1.
Access URL	ldap:// rs42.hp.com:2389	URL for connecting to the resource (the format is IP:port).	
Suffix	o=hp.com	Default root suffix.	
Login Name	uid=DMON07, ou=people, o=hp.com	Login name of the administrative user.	
Password	DMON07	Password of the specified user.	
Default User Suffix	ou=people	Suffix where all users exist.	
passPluginSuffix	ou=no plugin sufffix	Password Plug-in Suffix, not applicable to RACF.	
Default Group Suffix	ou=Groups	Suffix where all groups exist.	

Table 5A Resource Configuration Parameters for TSO Resource (cont'd)

Field Name	Sample Values	Description	Comment
Mapping File	`RACF_subAccount.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.	
segmentPrefix	racfSegment=Tso		

2 Map attributes – You must map the Select Identity attributes to the attributes of the time sharing resource. While mapping the attributes, refer to the following table for resource specific mapping information.

Table 6A RACF Mapping Information for TSO

Select Identity Resource Attribute	Connector Attribute	Attribute on RACF LDAP Bridge	Attribute in RACF	Description	Typical Value
DN	DN	DN			DN: racfSegment =Tso, uid= ,ou=, o=
TSOObjectClass	TSOObjectClass	TSOObjectClass			
UserName	uid	uid	User-ID	The ACID. This must be less than or equal to seven characters. This attribute is mandatory for user creation.	DMU1000
racfTsoAcctnum	racfTsoAcctnum	racfTsoAcctnum	Account Number	Account Number	ACCT#

Table 6A RACF Mapping Information for TSO

Select Identity Resource Attribute	Connector Attribute	Attribute on RACF LDAP Bridge	Attribute in RACF	Description	Typical Value
racfTsoMaxsize	racfTsoMaxsize	racfTsoMaxsize	Region Size Max	Region Size Max	600
racfTsoProc	racfTsoProc	racfTsoProc	Logon Procedure	Logon Procedure	ROCPROC
racfTsoSize	racfTsoSize	racfTsoSize	Region Size Default	Region Size Default	4096

For adding a TSO User, specify TSO objectclass value equal to `top|racfUserSegTso` and give value of any one of the TSO attributes as specified in Table 4A.

3 Add a user that is linked to the two types of resources.

After the User creation request is successful in Select Identity, verify in the RACF server that the user testUser is created with TSO segment. Verify this using the following command in the emulator

```
listuser <username> TSO
```

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 RACF 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 RACF Connector

Serial Number	Parameter Name	Parameter Value
1	AttributeName	racfRevoke
2	EnableValue	FALSE
3	DisableValue	TRUE
4	UserName	Select Identity admin user name. For example, sisa.
5	Password	Select Identity admin password. For example, abc123.
6	Url	http://localhost:9080/lmz/webservice

Configure Select Identity Polling for Reverse Provisioning

Reverse synchronization in RACF 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.

Attribute Names on Select Identity should be same as on RACF LDAP Server, if they are different, reverse requests will be rejected by saying that the specified attribute does not exist on the Select Identity.

For example: For `racfOwner` attribute that comes from RACF LDAP server, there should be a same attribute `racfOwner` on Select Identity also.

To configure polling, you must perform the following additional configuration on Select Identity (on Select Identity 3.3.1 or Select Identity 4.01-4.20).

Select Identity 3.3.1

Perform the following procedures to enable polling mechanism on Select Identity 3.3.1 for the RACF connector.

Modify the Truaccess.properties File

You need to add the following properties in the `TruAccess.properties` file to enable polling from Select Identity:

- A new entry "si.reconciliation.resync.polling" is used to point out the resource name for RESYNC or for reconciliation. The resource must be non-authoritative, otherwise no action will be taken for resync. For a regular reconciliation, the resource may be authoritative.

  si.reconciliation.resync.polling= <Resource Name on SI>

- To enable the RESYNC for reconciliation, following entries are also necessary.

  # The recon provisioning back feature is enabled for the specified resource.
  si.reconciliation.resync.<Resource Name on SI>=true

  # Workflow used for recon provisioning back feature of specified resource.
  truaccess.fixedtemplate.recon.resync.<Resource Name on SI>=SI\ Recon\ User\ Enable\ Disable\ Workflow

  # Default Workflow used for recon provisioning back feature.
  truaccess.fixedtemplate.recon.resync= SI\ Recon\ User\ Enable\ Disable\ Workflow

  # Another property is required to specify the keyfield name in the operational attributes of the spml request.
  si.reconciliation.polling.keyfield.<Resource Name on SI>= uid

Modify the following already existing entries as below
Initially their values will be ReconciliationDefaultProcess, change it to
Select Identity Recon User Enable Disable Workflow

truaccess.fixedtemplate.recon_enable=SI\ Recon\ User\ Enable\ Disable\ Workflow truaccess.fixedtemplate.recon_disable=SI\ Recon\ User\ Enable\ Disable\ Workflow

A sample of modified `TruAccess.properties` file:

```
truaccess.fixedtemplate.recon_enable=SI\ Recon\ User\ Enable\ Disable\
Workflow truaccess.fixedtemplate.recon_disable=SI\ Recon\ User\ Enable\
Disable\ Workflow

si.reconciliation.resync.polling=RACF

si.reconciliation.resync.RACF=true

truaccess.fixedtemplate.recon.resync.RACF=SI\ Recon\ User\ Enable\ Disable\
Workflow

truaccess.fixedtemplate.recon.resync=SI\ Recon\ User\ Enable\ Disable\
Workflow

si.reconciliation.polling.keyfield.RACF=uid
```

Modify the Select Identity database

You must add a row for a periodic polling task to the Batch table manually.

The xml text of the batch is:

```
<?xml version="1.0" encoding="UTF-8"?><Batch at="00:00:00" enabled="true"
handlerClass="
com.trulogica.truaccess.reconciliation.util.ReconPollingTaskHandler"
name="ReconPollingTask"
taskid="0"><RecurringSchedule><BySecond><RepeatInterval value="300"></
RepeatInterval></BySecond></RecurringSchedule></Batch>
```

You must run the following SQL command on the Select Identity database to add the batch task:

```
INSERT INTO BATCH (ID, ENABLED, STATE, REPEATCOUNT, NEXTSCHEDULED,
LASTSCHEDULED, JOBID, XMLTEXT, OWNER, STATECHANGETIME)
VALUES (-105, 1, 2, 1, '1/1/1975', null, null, '<?xml version="1.0"
encoding="UTF-8"?><Batch at="00:00:00" enabled="true"
handlerClass="com.trulogica.truaccess.reconciliation.util.ReconPollingTa
skHandler" name="ReconPollingTask"
taskid="0"><RecurringSchedule><BySecond><RepeatInterval value="300"></
RepeatInterval></BySecond></RecurringSchedule></Batch>', 0, null);
```

You have to add a new table(PollingJob), RESOURCECHANGELOG, to Select Identity database to store the lastChangeNumber as the parameter for calling the method `getChangeLog`.

To give the initial value of `lastChangeNumber` of the RESYNC resource, this PollingJob should be added before the first execution of polling batch with correct value of lastChangeNumber to prevent retrieve all users from the resource.

The SQL command that has to be run on Select Identity database to create & initialize this table is:

```
CREATE TABLE RESOURCECHANGELOG
(
ResourceId int PRIMARY KEY NOT NULL,
lastChangeNumber int,
maxChangeLogCount int);

INSERT INTO RESOURCECHANGELOG  VALUES(<resourceId>, <lastChangeNumber>,
<maxChangeLogCount>);
```

Where **<resourceId>** is the primary key (ID column) of the Top Secret Resource from the APPLICATION table (There will be an entry for each Select Identity resource in APPLICATION table.)

<lastChangeNumber> is generated based on current date and time to a number. All changelogs generated on the resource after this time should be considered for Reconciliation. If **<lastChangeNumber>** is set to zero, then it indicates all changelogs are to be considered. After each polling execution, the lastChangeNumber will be updated.

<maxChangeLogCount> indicates the maximum number of changelogs that will be retrieved in one polling action from one resource.

Once these changes are done in database, Select Identity will start polling for the change logs every 5 mins. If you want to change the next poll time, you can modify the NEXTSCHEDULED column of the row with ID=-105 under BATCH table. Then next poll will be done when you have specified in this column.

Select Identity 4.01-4.20

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. Refer to the *Service Studio* chapter of the *HP Select Identity Administration Online Help* for information on Select Identity services.

On Select Identity, if RACF service view has some attributes as mandatory, all of them should exist on RACF 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.

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.

A Pre-Provisioning and Post-Provisioning Operations

The RACF connector supports pre-provisioning and post-provisioning operations. Before/after a user is created / modified / deleted, the RACF connector can do other changes on the mainframe such as:

- Creating dataset aliases in SMS
- Adding users to other mainframe repositories
- Notifying mainframe personnel
- Executing any TSO CLIST or REXX exec commands.

To perform pre/post provision operations in RACF, a hook implementation class is used. This hook implementation class can send RACF commands on the resource through the LDAP Bridge. To send the commands to RACF, the hook implementation class can execute an LDAP search on the LDAP Bridge by passing the special search filter (RACF commands) and the LDAP Bridge executes the RACF commands..

- In `LDAPBridgeConfig.properties` file, the hook class name should be provided under the property `hook-provisioning-class`. The connector uses the class name and invokes it by using java reflection. For example, `hook-provisioning-class=com.hp.ovsi.racf.postprovision.class`.
- The scope of the post provision hook is limited to one. That is, for all the operations (add, modify, delete), there can be only one hook class.

The hook implementation class should implement the following `ProvisioningHookInterface` interface:

```
package com.hp.ovsi.connector;
public interface ProvisioningHookInterface {
    void preProvision(ProvisionContext p) throws
javax.naming.NamingException;
    void postProvision(ProvisionContext p) throws
javax.naming.NamingException;
}
```

A sample implementation of the hook class is available in the connetor CD.

The post provision hook is invoked only when the provision is successful. If the provision is not successful, the connector will throw an exception, and the post provision hook will not be invoked.

Sample Special Search filters:

Some of the sample special Search filters, which execute against LDAP Bridge containing RACF Commads are listed below.

```
tsoProcess=ADDUSER:testuser1:Name('test user')
tsoProcess=LU:testuser1
```

— **`ADDUSER:testuser1:Name('test user')`** is the TSO command to add a user with user name testuser1.

— **`LU:testuser1`** is the TSO command to to list the user.

Special Attributes

In the schema mapping file, the property `attrFunction` is used to identify if an attribute is special. This special attribute can have multiple values delimited by | (configurable in the properties file). If an attribute needs to be passed to provisioning operation and to the pre-provisioning hook, then it should have the value like `attrFunction=pre|provision`.

The default value for the attrFunction is `Provision`, that is, if that attribute is not specified or has an improper value in the definition, then it will take the default value `Provision`.

B Troubleshooting

- While creating and trying to save a resource, you get an error saying

  `Unable to find valid certification path to requested target.`

  Solution:

  Verify if the certificate of Sun ONE resource or issuer of Sun ONE resource has been imported into the truststore of Select Identity.

- While creating and trying to save a resource, you get an error saying

  `No trusted certificate found`

  Solution:

  Check the truststore managed by Select Identity, it seems that there is no trust key entry in the truststrore.

- While creating and trying to save a resource, you get an error saying

  `Bad certificate`

  Solution:

  Check the keystore managed by Select Identity to see if the certificate representing Select Identity is correct and trusted by the server.

- While creating and trying to save a resource, you get an error saying
  `error.securityfw.provider.cert.cn.not.found{16.157.133.80}`

  Cause:

  The cn field of server certificate does not equal to ldap URL in access information. For example, cn of certificate is machine name but using IP address in access information.

- While creating and trying to save a resource, you get an error saying

  `Cannot access key :null, maybe the password is incorrect or there is no private key.`

  Cause:

  The keystore managed by Select Identity is corrupt, or no key in it, or the password is incorrect.

- While creating and trying to save a resource, you get an error saying
  `error.securityfw.provider.certificate.revoked{CN=sicf-dev-2.asiapacific.hpqcorp.net, OU=TISU, O=CarlTao.HP.com, ST=Shanghai, C=CN}`

  Cause:

  The certificate from Sun ONE server can not pass CRL (certificate revoke list) check.