HP OpenView Select Identity

3270 Emulation Connector for RACF

Connector Version: 3.3

Installation and Configuration Guide

Document Release Date: November 2006
Software Release Date: November 2006

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

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

Please visit the HP OpenView support web site at:

http://www.hp.com/managementsoftware/support

This web site provides contact information and details about the products, services, and support that HP OpenView offers.

HP OpenView online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valuable support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit enhancement requests online
- Download software patches
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter 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 log in. Many also require a support contract.

To find more information about access levels, go to:

http://www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

http://www.managementsoftware.hp.com/passport-registration.html

Contents

1 Documentation Map

This chapter describes the organization of HP OpenView 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 OpenView Select Identity connector. For a list of available product documentation, refer to the table 1.

Figure 1 Documentation Map

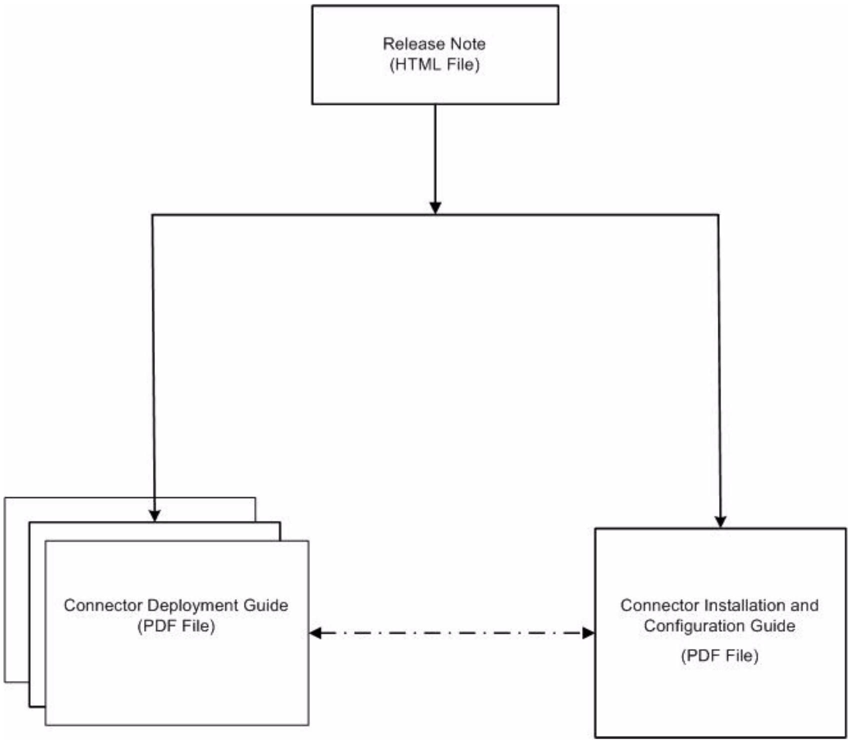

Release Note
(HTML File)
Connector Deployment Guide
(PDF File)
Connector Installation and Configuration Guide
(PDF File)

Table 1 Connector Documentation

Document Title and Filename	Contents	Location
Release Note `3270_RACF Connector v3.3 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 4.0/4.01.000) `connector_deploy_SI4.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/` subdirectory under the connector directory.
Connector Deployment Guide (for Select Identity 3.3.1) `connector_deploy_SI3.3.1.pdf`		
Connector Installation and Configuration Guide `3270_RACF_install.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 OpenView Select Identity connector for RACF. An HP OpenView Select Identity connector for RACF enables you to provision users and manage identities on RACF security system. At the end of this chapter, you will be able to know about:

- The benefits of the HP OpenView Select Identity.
- The role of a connector.
- The connector for RACF.

About HP OpenView Select Identity

HP OpenView 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 the RACF Connector

The 3270 Emulation connector for RACF security system — hereafter referred to as RACF connector —enables HP OpenView Select Identity to perform the following tasks on RACF security systems on OS/390 mainframes:

- 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
- Retrieve a list of supported user attributes
- Grant and revoke entitlements to and from users

It is a one-way connector and pushes changes made to user data in the Select Identity database to a target RACF server.

➤ The RACF connector can be used with Select Identity 4.0 and 3.3.1.

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 11.
	— Meet the system requirements.	See System Requirements on page 11.
	— Create macros.	See Creating Macros on page 12.
	— 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 17.
	— Install the Resource Adapter Archive (RAR) of the connector on an application server.	See Installing the Connector RAR on page 17.
2	Configure the connector with the Select Identity server.	See Configuring the Connector with Select Identity on page 19.

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 `3270 Emulation for RACF` directory on the Select Identity Connector CD:

Table 3 RACF Connector Files

Serial Number	File Name	Description
1	`RacfConnector.rar`	The Resource Adapter Archive (RAR) file contains the connector binaries.
2	`RacfSchema.jar`	The Schema file contains the mapping files that contain attribute information of RACF.

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	WebLogic 8.1.4 on Windows 2003	Microsoft SQL Server 2000
	WebSphere 5.1.1 on HP-UX11i	Oracle 9i
4.0	The RACF connector is supported on all the platform configurations of Select Identity 4.0.	

This connector is supported with RACF security systems on OS/390 or z/OS, version 2 release 10. In addition, the RACF connector uses the IBM SecureWay Host Access Class Library, version 3.0.4-B20000515, to communicate with RACF.

Creating Macros

The RACF connector uses “screen scraping” to establish a session and perform provisioning operations using the 3270 emulator. The commands that are used during the initial logon phase can vary greatly depending on the 3270 emulator used. For this reason, the RACF connector supports the configuration of a macro that defines logon session request and response sequences. This macro is loaded and executed by the connector at run time to establish the session with server.

You must manually create the macro using a text editor. You can obtain the command sequence for the logon session using any 3270 emulator client against the 3270 server where users will be provisioned by the connector. This is an important step in deploying the RACF connector. If the macro does not execute the actual command sequence, the connector cannot communicate with the 3270 server.

Use an existing 3270 emulator, or download one from an available site, install the emulator, and connect to the system. This chapter does not provide installation instructions for the emulator because the procedure is dependent on the chosen emulator. However, you will need the following information to connect to the system:

- Host name or IP address of the 3270 server
- Port number of the server
- User profile with administrative privileges, which will be used to provision users
- Password of the administrative user

Use this information to establish a session with the 3270 server. The screen should show you options to log on.

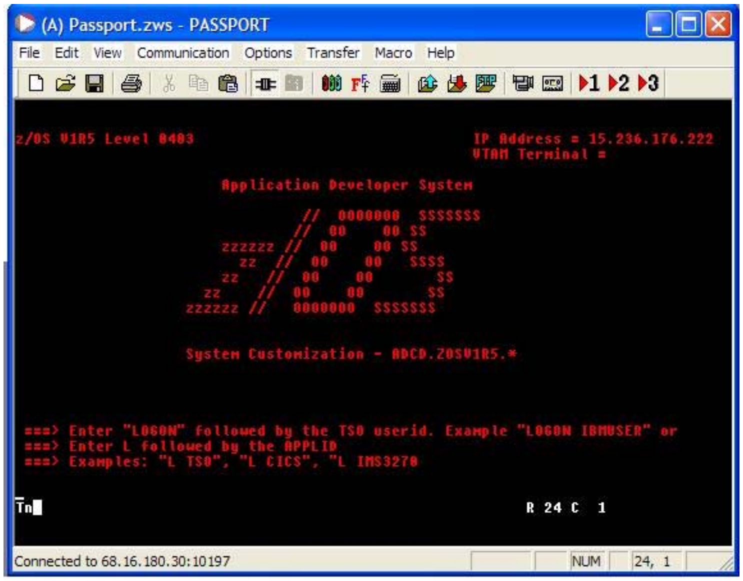
Logon Macro

This macros is required and must contain the sequence of request and response messages to be sent to establish a logon session with the server.

The following are example screens that are used to test the RACF connector.

- Initial Screen

  The administrative user ID is provided on this screen. Here is an example screen that displays when you first connect to the 3270 server:



```
z/OS V1R5 Level 0403                                      IP Address = 15.236.176.222
                                                          VTAM Terminal =

                          Application Developer System

                                   //  0000000  SSSSSSS
                                  //  00    00 SS
                          zzzzzz //  00    00 SS
                            zz  //  00    00   SSSS
                          zz   //  00    00       SS
                        zz    //  00    00       SS
                      zzzzzz //   0000000  SSSSSSS


                      System Customization - ADCD.ZOSV1R5.*



 ===> Enter "LOGON" followed by the TSO userid. Example "LOGON IBMUSER" or
 ===> Enter L followed by the APPLID
 ===> Examples: "L TSO", "L CICS", "L IMS3270


Tn                                                           R 24 C  1
```

Connected to 68.16.180.30:10197 NUM 24, 1

This screens displays the following:

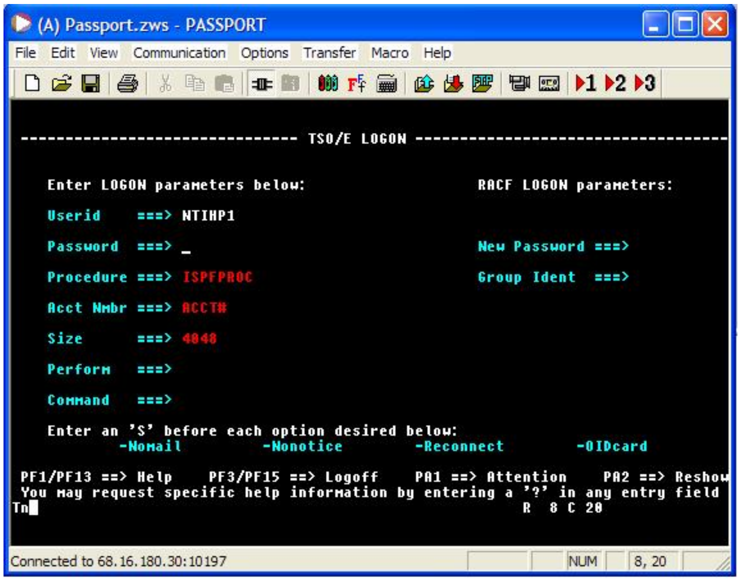
— Wait for a "LOGON" word after the initial connection

— Log on to the system by giving the TSO user ID with the LOGON command, as in this example:

```
LOGON NTIHP1
```

- Password Screen

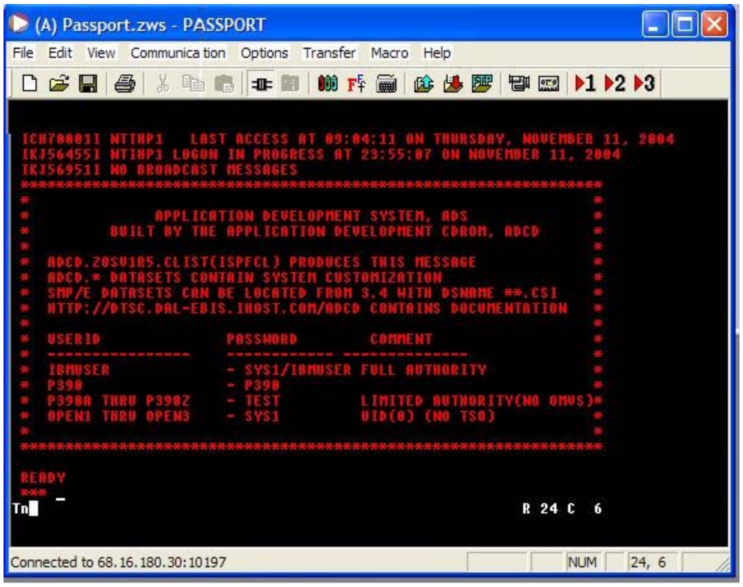
  The following screen displays after the LOGIN NTIHP1 command is issued in the previous screen. It prompts you for the administrative password:



```
------------------------------ TSO/E LOGON -----------------------------------

   Enter LOGON parameters below:                  RACF LOGON parameters:

   Userid    ===> NTIHP1

   Password  ===> _                               New Password ===>

   Procedure ===> ISPFPROC                        Group Ident  ===>

   Acct Nmbr ===> ACCT#

   Size      ===> 4048

   Perform   ===>

   Command   ===>

   Enter an 'S' before each option desired below:
           -Nomail         -Nonotice        -Reconnect        -OIDcard

PF1/PF13 ==> Help    PF3/PF15 ==> Logoff    PA1 ==> Attention    PA2 ==> Reshow
You may request specific help information by entering a '?' in any entry field
Tn                                                       R  8 C 20
```

- Welcome Screen

  After entering the correct password, the system displays a welcome screen, which might look like this:



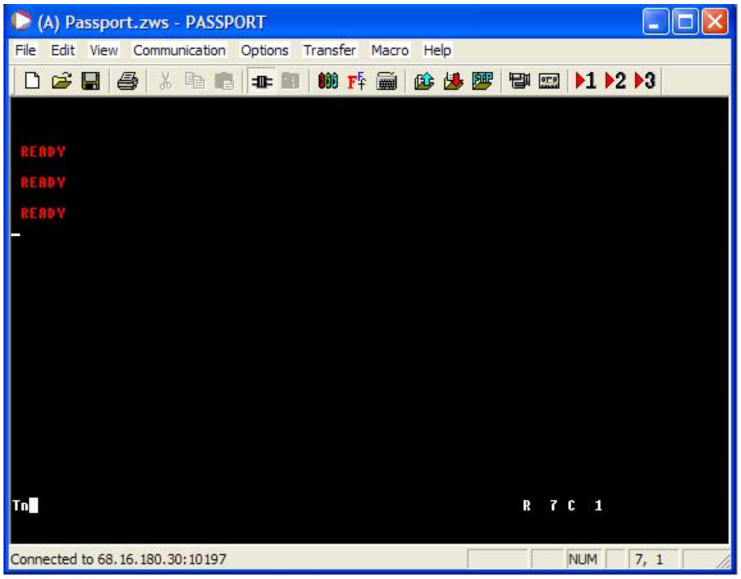
```
ICH70001I NTIHP1   LAST ACCESS AT 09:04:11 ON THURSDAY, NOVEMBER 11, 2004
IKJ56455I NTIHP1 LOGON IN PROGRESS AT 23:55:07 ON NOVEMBER 11, 2004
IKJ56951I NO BROADCAST MESSAGES
*****************************************************************
*                                                               *
*          APPLICATION DEVELOPMENT SYSTEM, ADS                  *
*      BUILT BY THE APPLICATION DEVELOPMENT CDROM, ADCD         *
*                                                               *
*  ADCD.Z0SV1R5.CLIST(ISPFCL) PRODUCES THIS MESSAGE             *
*  ADCD.* DATASETS CONTAIN SYSTEM CUSTOMIZATION                 *
*  SMP/E DATASETS CAN BE LOCATED FROM 3.4 WITH DSNAME **.CSI    *
*  HTTP://DTSC.DAL-EBIS.IHOST.COM/ADCD CONTAINS DOCUMENTATION   *
*                                                               *
*  USERID              PASSWORD        COMMENT                  *
*  ----------------    ------------ --------------              *
*  IBMUSER             - SYS1/IBMUSER FULL AUTHORITY            *
*  P390                - P390                                   *
*  P390A THRU P390Z    - TEST          LIMITED AUTHORITY(NO OMVS)*
*  OPEN1 THRU OPEN3    - SYS1          UID(0) (NO TSO)          *
*                                                               *
*****************************************************************

READY
***
Tn   _                                                  R 24 C  6
```

This shows the following:

- — The logon was successful
- — The system is ready for additional commands
- — The *** prompt means more input is expected and requires that you to send an ENTER command

- Ready Screen

  The system is ready for your command:


(A) Passport.zws - PASSPORT
File Edit View Communication Options Transfer Macro Help
1 2 3

```
READY
READY
READY

Tn                                                   R  7 C  1
```

Connected to 68.16.180.30:10197   NUM   7, 1

You must send several ENTER commands to display the System Ready Screen. You can then enter RACF commands.

Based on the screen output, the following is the sequence of steps required to establish a successful session with the 3270 server:

- Wait for LOGON
- Send LOGON <userid> <ENTER>
- Wait for Password ===>
- Send the password
- Send several <ENTER> commands to display the Ready Screen
- Wait for READY by the system

Here is the macro for this session:

```
Wait("LOGON");Send(LOGON ${user}[enter]);
Wait(Password  ===>);Send(${password}[enter]);Delay(1000);
Send([enter]);Send([enter]);Wait(READY
```

Post-creation Macro

Some systems require that a sequence of commands are executed on a newly created user to grant privileges. If your system requires this, the RACF connector can run another macro after creating a new user. The location of this macro can be given in the connection parameters section when deploying the resource.

Here is an example of a post-creation macro, which gives some permissions to the user, such as allowing him to log on to the system:

```
Wait(READY);Send(ALTUSER ${loginUserId} TSO(ACCTNUM(ACCT#) PROC(ISPFPROC)
JOBCLASS(A) MSGCLASS(X) HOLDCLASS(X) SYSOUTCLASS(X) SIZE(4048)
MAXSIZE(0))[enter]);Wait(READY);
Send(PERMIT ACCT# CLASS(ACCTNUM) ID(${loginUserId})[enter]);
Wait(READY);Send(PERMIT ISPFPROC CLASS(TSOPROC)
ID(${loginUserId})[enter]);Wait(READY);Send(PERMIT DBSPROC   CLASS(TSOPROC)
ID(${loginUserId})[enter]);Wait(READY);Send(PERMIT JCL CLASS(TSOAUTH)
ID(${loginUserId})[enter]);Wait(READY);
Send(PERMIT OPER CLASS(TSOAUTH) ID(${loginUserId})[enter]);
Wait(READY);Send(PERMIT ACCT CLASS(TSOAUTH)
ID(${loginUserId})[enter]);Wait(READY);Send(PERMIT MOUNT     CLASS(TSOAUTH)
ID(${loginUserId})[enter]);Wait(READY);
Send(SETROPTS REFRESH RACLIST(TSOPROC)[enter]);Wait(READY
```

Macro Commands

You can specify the following commands in a macro:

- Wait

  Wait for the occurance of a given string

- Send

  Send the given string to the server

- Delay

  Delyas the macro for a specified number of milliseconds, to synchronize with the server

- Special values

  The following special values can be given in the macro:

  ${user} — Provides the administrative user ID

  ${password} — Sends the administrative user's password

  ${app} — Sends the application name

  Some systems require the application name, such as TSO4, to be sent to the system. This name is sent from the connection parameters:

  ${loginUserId} - Specifies the user ID of the user being created

  [enter] - Send an <ENTER> command

Sample Macros

The `RacfSchema.jar` file is shipped with the following macros:

- `LoginSequence.txt` — Sample shown on page 15
- `PostCreate.txt` — Macro that can be run after users are created
- `SampleLoginSequence_1.txt` — Additional login sample macro
- `SampleLoginSequence_2.txt` — Additional login sample macro

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 `RacfSchema.jar` file to a directory that is in the application server `CLASSPATH`. Refer to the *HP OpenView Select Identity Connector Deployment Guide* for detailed instruction to extract contents of the Schema file.

Installing the Connector RAR

To install the RAR file of the connector (`RacfConnector.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 OpenView 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, 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. At the end of this chapter, you will know the procedure to configure the RACF 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

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 OpenView 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 OpenView 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. If you enabled reverse synchronization, this must be the same as the value provided for the urn:trulogica:concero:2.0#resourceId attribute on the agent console.	
Connector Name	RACF	The newly deployed connector.	Known as Resource Type on 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. Specify **No** if the connector is not enabled for reverse synchronization. Specify **Yes** if you want to add users through reverse synchronization. If the resource is not authoritative, the resource can only modify user entitlements during reverse synchronization.	
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.
Host Name		The IP address of the server.	
Port Number	23	The port number used by RACF.	
Admin User Name		Administrative user name for RACF.	
Admin Password		Administrative password for RACF.	
Initial Login Macro	LoginSequence.txt		
Timeout (seconds)	63		
Mapping File	RACF.xml	The mapping file for RACF connector.	

*Instead of creating an authoritative resource, you can create authoritative attributes (in the next step) for the attributes that will be synchronized. Entitlements are authoritative by default in a non-authoritative resource but other attributes are not.

⚠ If Test and Submit fails, the 3270 emulator may be active. The 3270 server allows only one logon session at a time per user. If the ID assigned to the connector (in the logon macro) is currently in use, you must first quit the 3270 emulator then retry the resource deployment.

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 OpenView 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	RACF User Attribute	Description	Mandatory
UserName	USERID	Maximum length is seven characters.	Yes
Password	PASSWORD	Minimum length is eight characters.	No
Default Group	DFLTGRP	Default group of the user in the system. If not assigned, the system will assign a default group.	No
Owner	OWNER	Owner of the user being created. If not assigned, the administrative user who is creating this user is assigned as the owner.	No
[First Name] [Last Name]	NAME	Full name of the user	No

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 OpenView Select Identity Administrator Guide* for information on Select Identity services.

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