HP Select Identity Software

Connector for IBM Tivoli Access Manager

Connector Version: 3.61

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

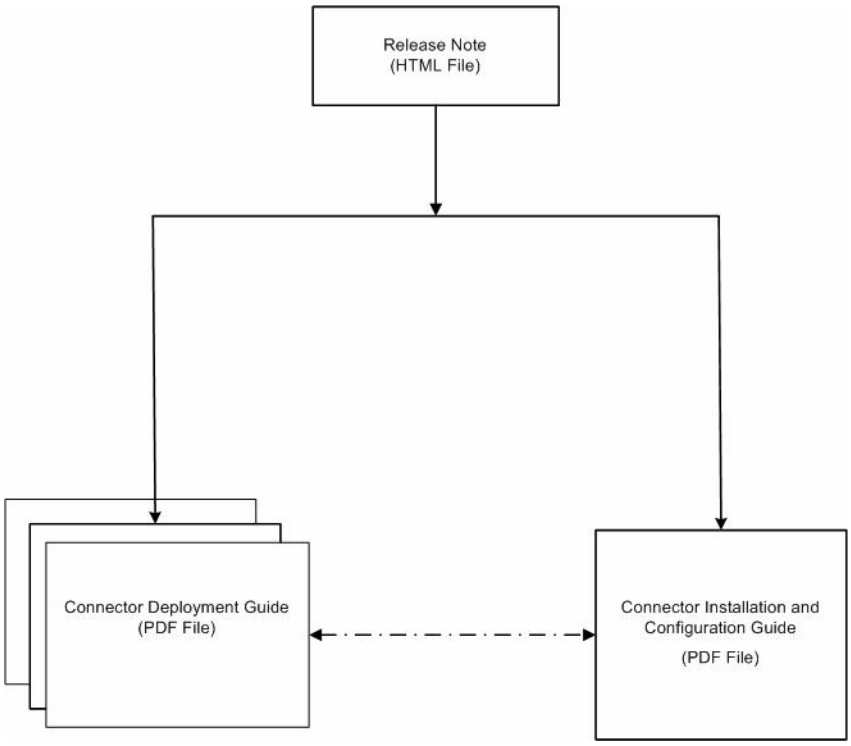


Table 1 Connector Documentation

Document Title and Filename	Contents	Location
Release Note `TAM Connector v3.61 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`		
Connector Installation and Configuration Guide `TAM_guide.pdf`	Connector installation and configuration guide provides installation instructions for a specific connector. It contains resource specific configuration details.	`/Docs/` subdirectory under the connector directory.

2 Introduction

This chapter gives an overview of the HP Select Identity connector for Tivoli Access Manager.

An HP Select Identity connector for Tivoli Access Manager enables you to provision users and manage identities on Tivoli Access Manager. 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 Tivoli Access Manager.

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 TAM Connector

The connector for Tivoli Access Manager — hereafter referred to as TAM connector — enables Select Identity to perform the following tasks on Tivoli Access Manager servers:

- 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

The TAM connector is a unidirectional connector and pushes changes made to user data in the Select Identity database to a target server. The mapping file controls how Select Identity fields are mapped to Tivoli Access Manager fields.

This connector can be used with Select Identity version 3.3.1-4.20.

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 IBM JRE	See Installing IBM JRE on page 14.
	— Install IBM TAM Java Runtime Environment	See Installing TAM Java Runtime Environment on page 14.
	— Configure TAM Java Runtime Environment.	See Configuring TAM Java Runtime Environment on page 16.
	— Create property and key store files.	See Creating the Property and Key Store Files on page 22.
	— 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 23.
	— Install the Resource Adapter Archive (RAR) of the connector on an application server.	See Installing the Connector RAR on page 23.
2	Configure the connector with the Select Identity server.	See Configuring the Connector with Select Identity on page 25.

3 Installing the Connector

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

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

TAM Connector Files

The TAM connector is packaged with the following files.

Table 3 TAM Connector Files

Serial Number	File Name	Description
1	• `TamConnector_420.rar` for WebSphere • `TamConnector_420WL9.rar` for WebLogic	It is the Resource Adapter Archive (RAR) file of the connector. It contains the binaries for the connector
2	`TamSchema.jar`	It contains the mapping file for the connector.
3	`tam-scripts.tar.gz`	It contains the `tamcfg.ksh` script for UNIX systems, which is used to configure the PD JRE, create the configuration and keystore files, and to invoke the TAM client APIs..
4	`tam-scripts.zip`	It contains the `tamcfg.bat` script for Windows-based systems, which is used to configure PD JRE, create the configuration and keystore files, and invoke the TAM client APIs.
5	`TamClient.jar`	It contains the TAM client Java classes, which implement the TAM APIs to access and manage the TAM resource

These files are located in the `IBM Tivoli Access Manager` directory on the Select Identity Connector CD.

System Requirements

The TAM connector is supported in the following environment:

Table 4 Platform Matrix for TAM connector

Select Identity Version	Application Server	Database	TAM Version and Operating System
3.3.1	WebLogic 8.1.4 on Windows 2003	Microsoft SQL Server 2000	5.1 on Solaris 9
	WebSphere 5.1.1 on HP-UX 11i	Oracle 9i	
4.0-4.20	The TAM connector is supported on all the platform configurations of Select Identity 4.0-4.20.		

This connector is supported with TAM 4.1 on Solaris 8 and TAM 5.1 on Windows 2000, Solaris 9, and TAM 6.0 on RedHat Enterprise Linux AS Release 3 (Taroon Update 7). Also, TAM is supported with the following:

- iPlanet as Directory Server on Windows 2000 and Solaris 9
- Tivoli Policy Server on Windows 2000, Solaris 9, and RedHat Enterprise Linux AS Release 3 (Taroon Update 7).
- Tivoli Authorization Server on Windows 2000, Solaris 9, and RedHat Enterprise Linux AS Release 3 (Taroon Update 7).

Also, the Tivoli Access Manager Runtime must be installed and configured before you install the TAM connector.

Installing IBM JRE

IBM JRE must be installed before you configure TAM Connector. You can find IBM JRE in IBM TAM Release CD.

For TAM 5.1, you need to have IBM JRE 1.3 installed; For TAM 6.0, you need to have IBM JRE 1.4 installed.

Installing TAM Java Runtime Environment

The installation of IBM package includes PDJrte and TAM RTE. PDJrte, Policy Director Java runtime environment in full name, is an installation package released by IBM for Tivoli Access Manager Java client support. Usually PDJrte and TAM RTE packages are included in the base CD of TAM.

PDJrte 5.1 is for providing the 9 JAR files that the TAM connector requires.

TAM RTE is for the administrator to configure the group information of admin user with `pdadmin`.

After all the above tasks are completed, the two packages PDJrte and TAM RTE can be uninstalled.

It is recommended to install PDJrte 5.1 for both TAM 5.1 and TAM 6.0.

The installation of the TAM 500 MB package is needed ONLY for extracting the following 9 PDJrte 5.1 JAR files into the right folder:

```
ibmjcefw.jar
ibmjceprovider.jar
ibmjsse.jar
ibmpkcs.jar
ibmpkcs11.jar
jaas.jar
PD.jar
local_policy.jar
US_export_policy.jar
```

If you already have these jar files (for example, if you already installed PDJrte 5.1, you should be able to find all these 9 JAR files in the directory `Policy Director/java/export/pdjrte`), then this package installation is not required at all. You can go to Creating PolicyDirector Folder on page 16 directly.

After this step is completed the TAM package is not required to be present. The same jar files can be copied into other Select Identity servers without the full installation again. That is, the TAM 500 MB package installation is NOT required on each of the Select Identity servers that are configured with TAM connector/resource.

Although testing of unlimited strength verion of `local_policy.jar` and `US_export_policy.jar` showed that they are working fine, it is still recommended that you use IBM bundled policy JAR files.

To install PDJrte 5.1 for TAM, you must install and configure TAM (from local) or TAM RTE (from remote) first. It is NOT necessary to install PDJrte 6.0, because PDJrte 5.1 fully support the Select Identity TAM connector. For more information on how to install TAM RTE, please refer to Appendix B, Installing and Configuring TAM Runtime Environment.

PDJrte 5.1 must be installed on the same machine as TAM RTE. You can install both PDJrte 5.1 and TAM RTE on a separate machine other than Select Identity server.

For example, if you are looking for PDJrte 5.1 for UNIX, you can download the patch package for UNIX named `5.1.0-TIV-TAM-FP0026-LIN.tar`, and do the following:

```
# tar xvf /path/to/5.1.0-TIV-TAM-FP0026-LIN.tar

PDAcld-PD-5.1.0-26.i386.rpm

PDAuthADK-PD-5.1.0-26.i386.rpm

PDJrte-PD-5.1.0-26.i386.rpm

PDMgr-PD-5.1.0-26.i386.rpm

PDMgrPrxy-PD-5.1.0-26.i386.rpm

PDRTE-PD-5.1.0-26.i386.rpm

PDWPM-PD-5.1.0-26.i386.rpm

# rpm -i PDJrte-PD-5.1.0-26.i386.rpm
```

Creating PolicyDirector Folder

After the installation of PDJrte 5.1 package, you can find the necessary jar files in the `Policy Director/java/export/pdjrte` folder under pdjrte installation directory.

In order to prepare for later configuration of `$PDHOME` that is defined in `tamcfg.ksh` (for UNIX) or `tamcfg.bat` (for Windows), you need to create a `PolicyDirector` folder in `IBMJREHOME` directory:

- Then copy the '`java/export/pdjrte/`' folder (including the 9 JAR files) into `IBMJREHOME/PolicyDirector/` directory which you defined for `$PD_LIB_DIR` in the tamcfg.ksh;

  If you already have the 9 JAR files in your environment, you need to create `java/export/pdjrte/` folder under `IBMJREHOME/PolicyDirector/` directory and copy the files into `pdjrte/` folder.

- Under the same `IBMJREHOME\PolicyDirector\` directory, check the existence of an `etc` sub-directory. If no, create an `etc` sub-directory. Then, after you execute **`tamcfg.bat jrtcfg`** (for Windows) and **`tamcfg.ksh jrtcfg`** (for UNIX), the following two files are created, which contain IBM JRE information:

  `pdjrte_mapping`

  `pdjrte_paths`

Configuring TAM Java Runtime Environment

The TAM Java Runtime Environment (JRE) component enables Java applications to manage and use TAM security. Before deploying the connector, you must configure the TAM JRE. This enables the connector to access and provision users in TAM. This section explains the `tamcfg.bat` (for Windows) and `tamcfg.ksh` (for UNIX) scripts, which can be used to configure the TAM JRE.

1. Create a subdirectory in the Select Identity home directory where the TAM client will reside. For example, you could create the `C:\Select_Identity\tamclient` folder on Windows, or you could create the `/opt/Select_Identity/tamclient` directory on UNIX.

   This TAM client directory will also store the `CFG.properties` and `KeyStore` that will be created using the `tamcfg` script.

2. On Windows, extract `tamcfg.bat` from the `tam-scripts.zip` file to the TAM client subdirectory. On UNIX, extract `tamcfg.ksh` from the `tam-scripts.tar.gz` file to the TAM client subdirectory.

3. Copy the `TamClient.jar` file from the Select Identity Connector CD to the TAM client subdirectory.

4. Make sure that all of the directories and files that are used to define the variables in `tamcfg.bat` or `tamcfg.ksh` exist with the required permissions. All of the variables are explained below.

   — JREHOME
   The JRE home directory. This must be the path to the IBM JDK JRE. Examples:

JREHOME=/opt/WebSphere/AppServer/java/jre

JREHOME=
C:\Program Files\WebSphere\AppServer\java\jre

Make sure PolicyDirector resides here and this subdirectory contains the java/export/pdjrte subdirectory with all of the TAM JAR files. If not, create these subdirectories and copy the TAM JAR files here, which come with the TAM installation. Here is the listing of the 9 JAR files:

```
ibmjcefw.jar
ibmjceprovider.jar
ibmjsse.jar
ibmpkcs.jar
ibmpkcs11.jar
jaas.jar
PD.jar
local_policy.jar
US_export_policy.jar
```

You need to set PD.jar into your CLASSPATH.

— PDHOME
The home directory of Tivoli Access Manager Policy Director runtime. Examples:

PDHOME=$JREHOME/PolicyDirector

PDHOME=%JREHOME%\PolicyDirector

— PD_LIB_DIR
The folder where Policy Server JAR files are located. Examples:

PD_LIB_DIR=$PDHOME/java/export/pdjrte

PD_LIB_DIR=%PDHOME%\java\export\pdjrte

— TAM_CLIENT_DIR
The folder where Select Identity's TamClient.jar is installed. Examples:

TAM_CLIENT_DIR=/opt/Select_Identity/tamclient

TAM_CLIENT_DIR=C:\Select_Identity\tamclient

This folder will also contain the TAM key store and configuration files. These files are generated by the tamcfg script and are referenced later.

— APP_SERVER_IP
The IP Address of the machine on which Select Identity will be running. Example:

APP_SERVER_IP=16.73.17.88

— POLICY_SERVER_IP
The IP Address of Tivoli Access Manager Policy Server. Example:

POLICY_SERVER_IP=15.70.184.141

— APP_SERVER_NAME
The name of the Select Identity application, which is used to create an account for the Select Identity application to access TAM. It is also used to create a registry user in TAM Policy Server. Example:

APP_SERVER_NAME=SI88aTam141

— AUTH_SERVER_IP
The IP Address of Tivoli Access Manager Authentication Server. Usually this is the same as the machine on which the Policy Server is running. Example:

AUTH_SERVER_IP=$POLICY_SERVER_IP

— APP_MODE
Set to **remote** if the Select Identity application will run on a machine remote from the machine running the Tivoli Access Manager Policy Server. Example:

APP_MODE=remote

— OPERATION
The operation to be performed with SvrSslCfg. For the first creation of the key store and configuration file, this must be set to **create**. If there is any changes to the other variables, specify **replace** for regeneration.

OPERATION=create

Below is an example for your reference:

First, copy the TAM 5.1 java files to the IBM JRE which you will use to configure TAM client. If you have installed PDJrte, the files should reside in `/opt/PolicyDirector/java` directory; or, you can copy the directory which includes the 9 JAR files from another machine with PDJrte installed.

```
# mkdir /opt/IBMJava2-142/jre/PolicyDirector

# cd /opt/PolicyDirector

# cp -R java  /opt/IBMJava2-142/jre/PolicyDirector
```

Second, follow the instructions of this *HP Select Identity Connector for IBM Tivoli Access Manager Installation and Configuration Guide*, copy `tamcfg.ksh` and `tamclient.jar` files to a directory (for example `/opt/tamclient`), then edit `tamcfg.ksh` manually to fit your environment.

The following is a sample `tamcfg.ksh` as in a successful configuration:

```
#!/bin/ksh


#
# Configuration for the client that accesses Tivoli Access Manager
#
# You can use this script to do the following:
#    - Configure TAM Java Runtime Environment (using PdJrteCfg)
#    - Generate KeyStore/Config property files for SI to access TAM
#
# Edit the following fields to make sure the info is correct
#
# NOTE: This script will be used even by the connector and so
# this should be placed in a folder where no one can mess around with
#


# ----------------------- Configuration variables --------------------------


# JRE Home Directory
# Make sure there is PolicyDirector under this folder
# and this folder has java/export/pdjrte folder with
```

```
# all the TAM jar files. If this is not the case, create these
# folders and simply copy the TAM jar files there
JREHOME=/opt/IBMJava2-142/jre

# Home of Tivoli Access Manager Policy Director runtime
PDHOME=$JREHOME/PolicyDirector

# Folder where Policy Server Jar files are located
PD_LIB_DIR=$PDHOME/java/export/pdjrte

# Folder where SI's TamClient.jar is installed
TAM_CLIENT_DIR=/opt/TAM

# Folder where Tam KeyStore and Config files are to be put
# These files are generated by a script below, and are referenced later
# and should be in the classpath or ext dirs folder
TAM_CONFIG_DIR=$TAM_CLIENT_DIR

# IP Address of the machine on which SI will be running
APP_SERVER_IP=16.157.53.79

# IP Address of Tivoli Access Manager Policy Server
POLICY_SERVER_IP=IDMLinuxAS3

# Name of the SI application
# This name is used to create an account for the SI application to access TAM
# and a registry user is created in TAM Policy Server
APP_SERVER_NAME=SI4100000

# Name of an admin account created in Tivoli Access Manager
# SI uses this account for user provisioning
#PD_ADMIN_ID=sec_master

# Admin password
#PD_ADMIN_PASSWD=123!@#asd

# IP Address of Tivoli Access Manager Authentication Server
# Usually this is the same as the machine on which the policy server is
running
AUTH_SERVER_IP=$POLICY_SERVER_IP

# Set this to remote if the SI application will be running on
```

```
# a machine remote from the machine running the Tivoli Access Manager Policy
Server
APP_MODE=remote

# Operation to be performed with SvrSslCfg
# For first time creation of KS and Property file this must be create
# If there is any changes to above information, use replace for regeneration
OPERATION=create
#OPERATION=replace

#
# ------------------------------------------------------
#  Don't change anything below this line
# ------------------------------------------------------

# Config Home
CFGHOME=$JREHOME
APP_CLS_PATH="$PD_LIB_DIR/PD.jar:$TAM_CLIENT_DIR/
TamClient.jar:$TAM_CONFIG_DIR"
# Location/name of the properties file to be generated
CFG_FILE=$TAM_CONFIG_DIR/${APP_SERVER_NAME}_TAM_CFG.properties
# Location/name of keystore file to be generated
KEY_FILE=$TAM_CONFIG_DIR/${APP_SERVER_NAME}_TAM_KEY.ks

PD_CLS_OPTION=sslcfg
if [ $# -gt 0 ]
then
PD_CLS_OPTION=$1
fi

if [ $PD_CLS_OPTION = "jrtcfg" ]
then
# ---------- read PD_ADMIN_ID and PD_ADMIN_PASSWD -----
echo "Please enter TAM Admin Account ..."
stty -echo
read PD_ADMIN_ID
stty echo

echo "Please enter TAM Admin Account Password ..."
stty -echo
read PD_ADMIN_PASSWD
stty echo
```

```
# ---------- read PD_ADMIN_ID and PD_ADMIN_PASSWD -----
  $JREHOME/bin/java -Dpd.home=$PDHOME -classpath $APP_CLS_PATH
com.tivoli.pd.jcfg.PDJrteCfg -action config -java_home $JREHOME -host
$POLICY_SERVER_IP -port 7135 -config_type full -domain Default
elif [ $PD_CLS_OPTION = "sslcfg" ]
then
# ---------- read PD_ADMIN_ID and PD_ADMIN_PASSWD -----
echo "Please enter TAM Admin Account ..."
stty -echo
read PD_ADMIN_ID
stty echo

echo "Please enter TAM Admin Account Password ..."
stty -echo
read PD_ADMIN_PASSWD
stty echo
# ---------- read PD_ADMIN_ID and PD_ADMIN_PASSWD -----
  $JREHOME/bin/java -Dpd.home=$PDHOME -Djava.home=$JREHOME -classpath
$APP_CLS_PATH com.tivoli.pd.jcfg.SvrSslCfg -action config -admin_id
$PD_ADMIN_ID -admin_pwd $PD_ADMIN_PASSWD -appsvr_id $APP_SERVER_NAME
-appsvr_pwd abc123 -port 7777 -mode $APP_MODE -host $APP_SERVER_IP -policysvr
$POLICY_SERVER_IP:7135:1 -authzsvr $AUTH_SERVER_IP:7136:1 -cfg_file $CFG_FILE
-key_file $KEY_FILE -cfg_action $OPERATION
else
  $JREHOME/bin/java -classpath $APP_CLS_PATH
com.trulogica.truaccess.connector.tam.TamClient $*
fi
```

5 After verifying for the existence of all files and directories, run the following command to configure the PD JRE component. Pass **jrtcfg** as the argument to the script.

On UNIX:
tamcfg.ksh jrtcfg

On Windows:
tamcfg.bat jrtcfg

If an "Authentication method is unavailable" error occurs while running the `tamcfg` script, verify whether the Directory Server, Policy Server, and Authentication Server are running.

You will get the following output:

```
Configuration of Access Manager Java Runtime Environment is in
progress.

This might take several minutes.

Configuration of Access Manager Java Runtime Environment completed
successfully.
```

When you execute the following commands:

on Windows:

tamcfg.bat jrtcfg

tamcfg.bat sslcfg

on UNIX:

tamcfg.ksh jrtcfg

tamcfg.ksh sslcfg

The script will prompt you to provide admin ID and password. The admin ID and password you provide here must be the same as those given in the resource access info page.

If you use the default admin account (`sec_master`) as PD_ADMIN_ID, or the user account you use exists in `iv-admin` group, then TAM Runtime Environment is not required; otherwise you need to install and configure TAM Runtime Environment. For more information, please refer to Appendix B, Installing and Configuring TAM Runtime Environment.

Creating the Property and Key Store Files

The connector uses secure communication with the TAM Policy Server. You must perform steps to generate the configuration property files and key store file.

The same script used in Configuring TAM Java Runtime Environment on page 16 (`tamcfg.bat` or `tamcfg.ksh`) can be used to create the configuration property file and key store file. First, you must configure the PD JRE then you can create the configuration and key store files.

The files will be created in the directory specified by the TAM_CONFIG_DIR variable. This is the same directory where you extracted the `tamcfg` script.

Complete the following steps to created the files:

1. Make sure that all of the directories and files that are used to define the variables in `tamcfg.bat` or `tamcfg.ksh` exist with the required permissions. See step 4 on page 16 for an explanation of the variables.

   Also, note that this script uses the `com.tivoli.pd.jcfg.SvrSslCfg` Java class to create the required property and key store files.

2. Execute the `tamcfg` script as shown below :

   On Windows :
   tamcfg.bat sslcfg

   On UNIX:
   tamcfg.ksh sslcfg

   This command creates two files:

   — *APP_SERVER_NAME*_TAM_CFG.properties

   — *APP_SERVER_NAME*_TAM_KEY.ks

where *APP_SERVER_NAME* is the name of the Select Identity application that you specified in the `tamcfg` script. These files are used by the TAM connector client and should not be edited, moved, or deleted from this directory.

For UNIX, before you execute the `tamcfg.ksh sslcfg`, you need to create a null `PDJLog.properties` in `$(JREHOME)/PolicyDirector` manually and touch it.

The following is a sample for UNIX:

```
# touch /opt/IBMJava2-142/jre/PolicyDirector/PDJLog.properties

# ./tamcfg.ksh sslcfg
```

After execution, you will get the following output:

```
The configuration completed successfully.
```

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 `TamSchema.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 (such as `TamConnector_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/TamConnector`**.

4 Configuring the Connector with Select Identity

This chapter describes the procedure to configure the TAM 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 TAM 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/TamConnector`**.
- 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

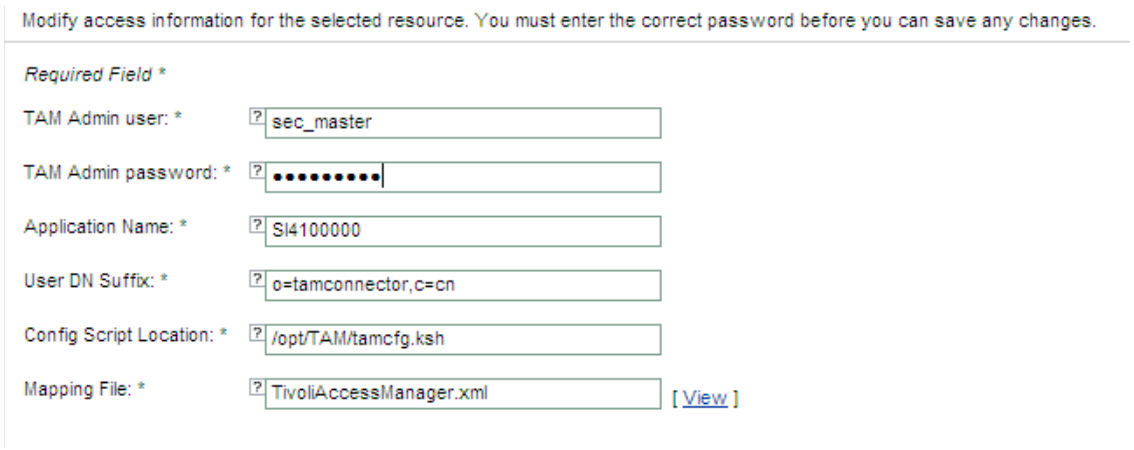
Add a new resource in Select Identity that uses the newly added connector. Refer to the *HP Select Identity Connector Deployment Guide* for detailed instructions on adding a resource in Select Identity.

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	TAM75	Name given to the resource.	
Connector Name	TAM	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. 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.
Application Name	gvSI86TAM75	Name of the application configured to access TAM. This is the name given in the `tamcfg.bat` or `tamcfg.ksh` script while generating the configuration property and key store files.	
User DN Suffix	ou=People,dc=qa ,dc=HP	The complete DN suffix of the users in the Directory Store. This is where users will be provisioned.	
Config Script Location	*On Windows*: C:\Select_Identi ty\tamclient\ta mcfg.bat *On UNIX*: /opt/ Select_Identity/ tamclient/ tamcfg.ksh	Full path to the location of the `tamcfg.bat` or `tamcfg.ksh` script, which is installed in the TAM client subdirectory.	
TAM Admin user	sec_master	This is the TAM administrator account, which is used to provision the users into TAM.	
TAM Admin password		Password for the TAM administrator.	

Below is a Resource Access Information screenshot for your reference when installing the TAM resource in Select Identity environment:



If you use the default admin account (`sec_master`) as TAM Admin user, or the user account you use exists in `iv-admin` group, then TAM Runtime Environment is not required; otherwise you need to install and configure TAM Runtime Environment. For more information, please refer to Appendix B, Installing and Configuring TAM Runtime Environment.

Map Attributes

After successfully adding a resource for the TAM 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 TAM Mapping Information

Select Identity Resource Attribute	Attribute on Connector	TAM User Attribute	Attribute on Physical Resource (iPlanet)	Description
GUID	GUID	cn		The user's global ID.
[First Name] [Last Name]-[GUID]	cn	Part of Registry Name (DN)	cn	The user's common name.
User Name	uid	UserName	uid	A value from 1-100 alphanumeric characters in length.

Table 6 TAM Mapping Information (cont'd)

Select Identity Resource Attribute	Attribute on Connector	TAM User Attribute	Attribute on Physical Resource (iPlanet)	Description
Password*	Password	Password	userPassword	1-10 alphanumeric characters. This value is encrypted.
First Name	fname	First name	cn	A value from 1-50 alphanumeric (including '.') characters in length.
Last Name	lname	Last name	sn	A value from 1-50 alphanumeric (including '.') characters in length.
Description**	description	Description	description	A value from 1-100 alphanumeric characters in length.
GUID	GUID	cn		The user's global ID.
[First Name] [Last Name]-[GUID]	cn	Part of Registry Name (DN)	cn	The user's common name.

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

5 Uninstalling the Connector

If you want to uninstall a connector from Select Identity, perform the following steps:

- Remove all resource dependencies.
- Delete the connector from Select Identity Connectors page.
- Delete the connector from application server.

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

A Troubleshooting

This appendix describes common problems seen during the installation and execution of the connector.

- While running the `tamcfg` script to generate the property or key store files, the following error may occur:

  ```
  Authentication method is unavailable
  ```

  In this case, check if the Directory Server, Policy, and Authentication servers are running.

- If creating a user, adding entitlements, or removing entitlements takes too long or hangs, restart the Directory server.

- When the number of users in IBM Tivoly Access Manager exceeds 5000, the resource server cannot be accessed. This happens because the look-through limit defined on the iPlanet Directory Server exceeds the set limit, the directory server returns a status of LDAP_ADMINLIMIT_EXCEEDED, and IBM Tivoli Access Manager treats it as an error. The look-through limit is a performance related parameter that can be customized by iPlanet LDAP administrator.

  In the iPlanet Console, perform the following steps:

  a. Select the Configuration tab and expand the Data entry.

  b. Select the Database Settings item and select the LDBM Plug-in Settings tab.

  c. In the Look-through Limit field, enter the maximum number of entries you want the server to check in response to a search request. The default look-through limit value is 5000.

     If you do not want to set a limit, type -1 in this field. If you bind to the directory as the Directory Manager, by default the look-through limit is unlimited, and overrides any settings you specify in this field.

B Installing and Configuring TAM Runtime Environment

If you use the default admin account (`sec_master`) as PD_ADMIN_ID, or the user account you use exists in `iv-admin` group, then TAM Runtime Environment is not required; otherwise you need to install and configure TAM Runtime Environment.

After installing the TAM Runtime Environment, you can verify whether a user account exists in `iv-admin` group or not; and if the use account does not exist in the `iv-admin` group, you can add it into the group.

You can install the TAM Runtime Environment on a separate machine since it is used for admin user account verification and configuration purpose only.

Prerequisites for Configuring TAM

In order to configure TAM connector on UNIX, you must have the following things ready:

- IBM Tivoli Access Manager for e-business;
- IBM PDJrte 5.1.0.x (downloadable from IBM support site);
- Knowledge of how to configure your TAM server;

SSL CA Certificate base64 file of your remote TAM server, which resides in `/var/PolicyDirector/Keytab` folder on your remote TAM server machine, its name is `pdcacert.b64`.

Installing and Configuring TAM Runtime Environment

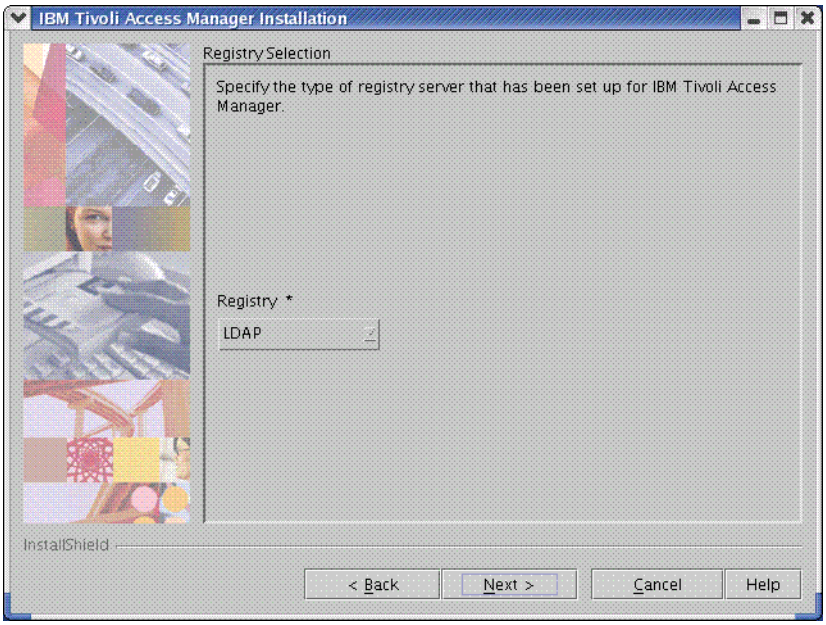
TAM Runtime Environment is the native runtime environment for TAM Client. It must be installed before Java Runtime Environment is installed. On the TAM CD, there are two ways available to install TAM Runtime Environment. For a local TAM Policy Server, you should execute **`install_ammgr`**; For support of a remote TAM service, you should execute **`install_amrte`**.

The remaining part of this section is a sample installation for support of remote TAM service on UNIX:

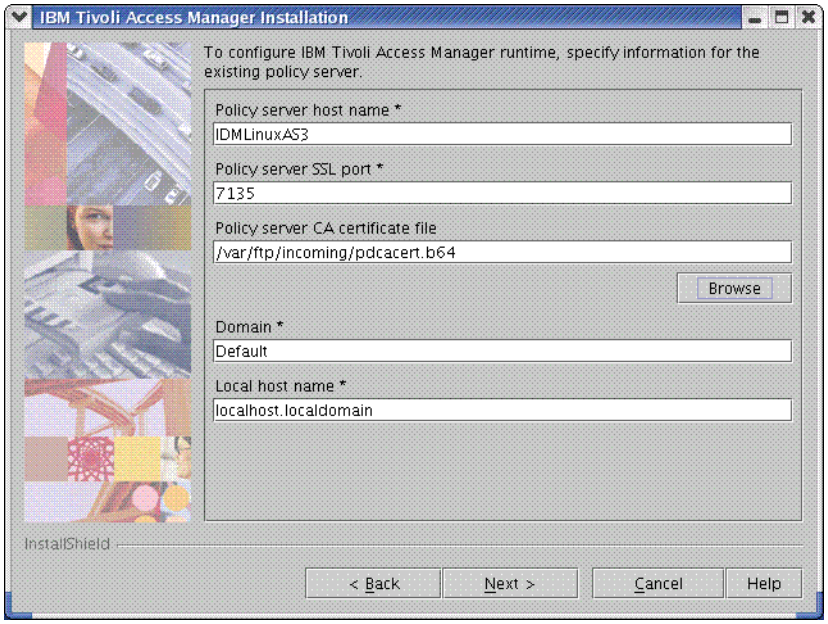
```
# ./install_amrte
```

This installer will install and configure only client environment for TAM server. It will start java GUI interface for the installation and configuration:

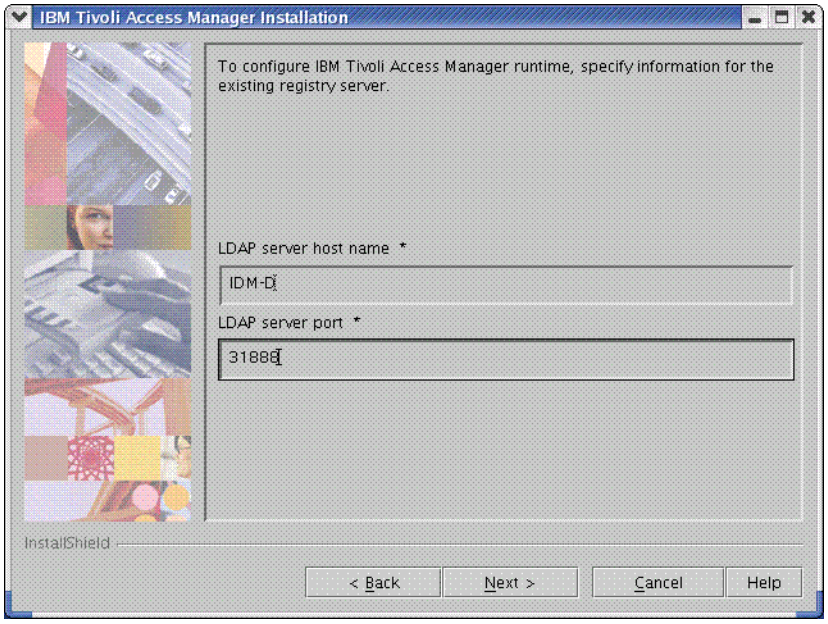
In this step you must first know what kind of directory service your remote TAM server uses.



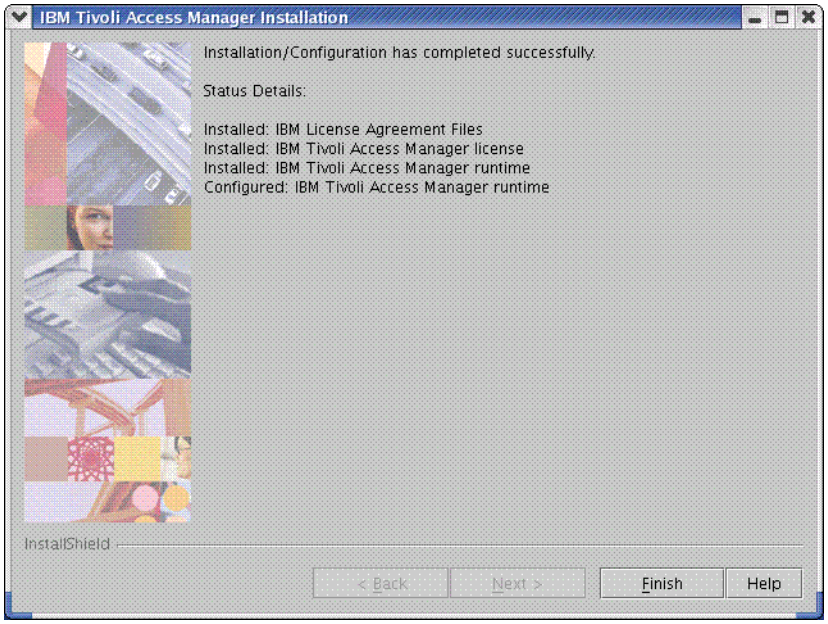
Click **Next** to open next window for common log configuration. In the window opened, fill in corresponding fields with correct information of your TAM server:



Click **Next**. Fill in correct information of your TAM server's directory repository information.



Click **Next**. The installation completion status is displayed. Click **Finish** to complete the installation.



When the installtion is completed, you can use **`pdconfig`** as shown below to check the installed RTE:

```
# pdconfig

       Tivoli Access Manager Setup Menu


        1. Configure Package

        2. Unconfigure Package
```

```
        3. Display Configuration Status
        x. Exit

Select the menu item [x]: 3

        Tivoli Access Manager Configuration Status

        Package Name Configured?

        ____________________________________________________________

        Access Manager Runtime                          Yes

Press Enter to continue.
```

Then you can use pdadmin to verify that the RTE is working OK:

```
# pdadmin
pdadmin> login
Enter User ID: sec_master
Enter Password:
pdadmin sec_master> user list * 100
sec_master
ivmgrd/master
```

Usage of the pdadmin tool is optional, and is used only to verify the provisioning done by the connector. If you have other means to verify the provisioning, then the pdadmin tool is NOT necessary.

Verifying Existence of a User Account in iv-admin Group

You can use the following command to verify whether a user account exists in `iv-admin` group:

```
pdadmin sec_master> group show-members iv-admin
```

Adding a User to iv-admin Group

If you want to add a user (for example, `cupsuser`) to `iv-admin` group, use the following command:

```
pdadmin sec_master> group modify iv-admin add cupsuser
```

Then, you can use the following command to verify the user is added into `iv-admin` group:

```
pdadmin sec_master> group show-members iv-admin
```