HP OpenView Select Identity

Connector for IBM Tivoli Access Manager

Connector Version: 3.5

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

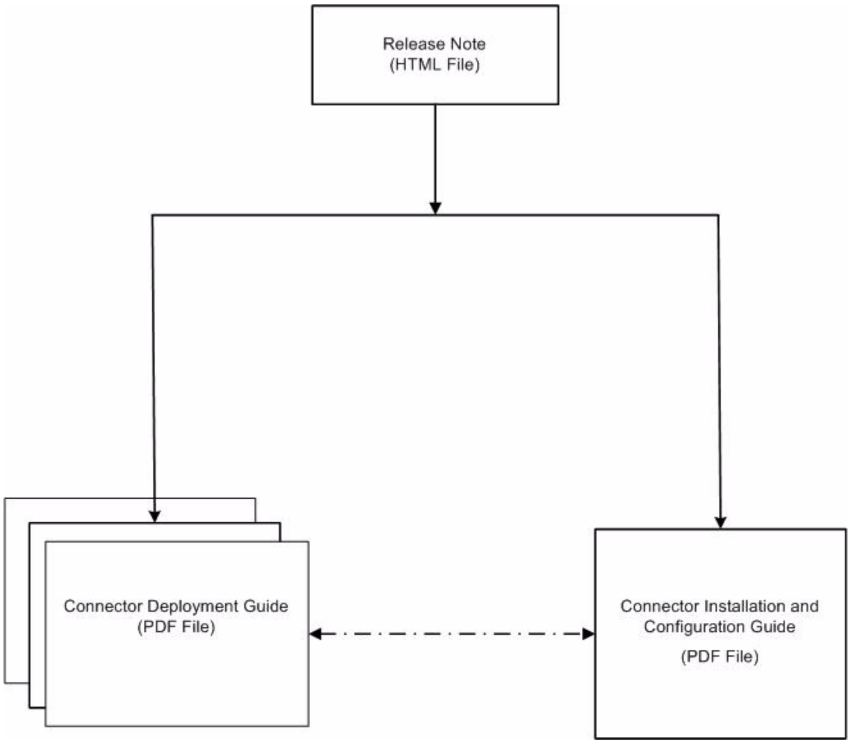

Table 1 Connector Documentation

Document Title and Filename	Contents	Location
Release Note `TAM Connector v3.5 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 4.10) `connector_deploy_SI4.1.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 4.0/4.01.000) `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_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 Tivoli Access Manager. An HP OpenView 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 the HP OpenView Select Identity.
- The role of a connector.
- The connector for Tivoli Access Manager.

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 TAM Connector

The connector for Tivoli Access Manager — hereafter referred to as TAM connector — enables HP OpenView 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 4.10, 4.01.000, 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 13.
	— Meet the system requirements.	See System Requirements on page 14.
	— Configure TAM Java Runtime Environment.	See Configuring TAM Java Runtime Environment on page 14.
	— Create property and key store files.	See Createing the Property and Key Store Files on page 16.
	— Verify the TAM client.	See Verifying the Tivoli Access Manager Client on page 17.
	— 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 20.
	— Install the Resource Adapter Archive (RAR) of the connector on an application server.	See Installing the Connector RAR on page 20.
2	Configure the connector with the Select Identity server.	See Configuring the Connector with Select Identity on page 21.

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.rar`	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	
4.0/4.01.000/4.10	The TAM connector is supported on all the platform configurations of Select Identity 4.0, 4.01.000, and 4.10.		

This connector is supported with TAM 4.1 on Solaris 8 and TAM 5.1 on Windows 2000 and Solaris 9. Also, TAM is supported with the following:

- iPlanet as Directory Server on Windows 2000 and Solaris 9
- Tivoli Policy Server on Windows 2000 and Solaris 9
- Tivoli Authorization Server on Windows 2000 and Solaris 9

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

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 a listing of the files:

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

— 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

- PD_ADMIN_ID
  The name of an administrative account created in Tivoli Access Manager. Select Identity uses this account for user provisioning. Example:

  PD_ADMIN_ID=sec_master

- PD_ADMIN_PASSWD
  The password for the administrative account (PD_ADMIN_ID).

- 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

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

Createing 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 14 (`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 15 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 SI 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.

Verifying the Tivoli Access Manager Client

The Tivoli Access Manager client is a client application that uses TAM APIs to access and provision on the TAM resource. It takes command line arguments that support user operations such as listing users and groups, creating users and groups, and so on. You can use the TAM client to verify the connectivity to the TAM resource and to verify provisioning.

To use the TAM client, you can run the `tamcfg` script, which was used to configure the TAM JRE and to create of the property and key store files. Run the `tamcfg.bat` script (for Windows) or `tamcfg.ksh` script (for UNIX) from the command line in a similar way it was used in the previous procedures but with a different set of arguments. Both scripts take the **tamclient** argument to run the Java class TamClient. This class implements all user-related operations.

The following are the arguments to be passed to the `tamcfg` script for executing the commands.

`tamcfg tamclient function appName keyField`

where:

- **`tamclient`** is a constant that is always specified
- **`function`** is the name to be executed, such as isUserExists, getGroups, and so on.
- **`appName`** is the application name that you provided in the `tamcfg` script.
- **`keyField`** is the key field of the user. This argument is optional but necessary for such functions as isUserExists.

The following are examples used for performing various operations to validate whether the TAM client is working properly.

doTest

Use the doTest function to test connectivity to the TAM resource. If this test fails, it means that some of the configuration done in earlier steps is wrong or you do not have access to TAM Policy Server. In this case, you must edit the `tamcfg` script and verify that all variables are correct. Then, you must regenerate the property and key store files. The following is an example of the command run on UNIX:

```
tamcfg.ksh tamclient doTest SI88aTam141
```

where **SI88aTam141** is the application name provided in the `tamcfg` script. If the command runs successfully, the command returns `OK`.

isUserExists

Use this function to verify for the existence of a user in TAM. The following is an example of the command run on UNIX:

```
tamcfg.ksh tamclient isUserExists SI88aTam141 tamuser01
```

If the user exists, the command returns `OK`. However, if the user does not exist, the command returns `ERROR`.

getGroups

Use this function to list all groups that exist on the TAM resource. The following is an example of the command run on UNIX:

```
tamcfg.ksh tamclient getGroups SI88aTam141
```

Here is the output:

```
handleResult(msgs): ENTER
handleResult(msgs): EXIT-0
groupkey::::hr-mgrs
groupkey::::qa-mgrs
groupkey::::pd-mgrs
groupkey::::SecurityGroup
groupkey::::ivmgrd-servers
groupkey::::iv-admin
groupkey::::secmgrd-servers
groupkey::::webseal-servers
groupkey::::webseal-mpa-servers
groupkey::::ivacld-servers
groupkey::::remote-acl-users
OK
```

findUser

Use this function to retrieve the details of an existing user on the TAM resource. The following is an example of this command run on UNIX:

`tamcfg.ksh tamclient findUser SI88aTam141 tamuser01`

The following is the output:

```
User id = tamuser01

Description = Tivoli Access Manager 5.1 First User

Account valid = true

Password valid = true

Policy Director user = true

Has single-signon capabilities = false

Registry name = cn=tamuser01first tamuser01last-B07242BA-BAE7-077B-

B511-F90D8A93B899,ou=People,dc=qa,dc=trulogica,dc=com

First name = tamuser01first

Last name = tamuser01last

Groups =

User policy =

User id = tamuser01

Account expiration date = null (not enforced)

Maximum failed logins allowed before account disabled = 0 (not enforced)

Account disable time interval (in minutes) = 0 (not enforced)

Spaces allowed in password = false (not enforced)

Maximum password age (in seconds) = 0 (not enforced)

Maximum repeated characters allowed in password = 0 (not enforced)

Minimum number of alphabetic characters required in password = 0 (not
enforced)

Minimum number of non-alphabetic characters required in password = 0 (not
enforced)

Minimum password length = 0 (not enforced)

Account is accessible on the following days = Any day (not enforced)

Account accessible starttime (in minutes after midnight on accessible days) =
0

Account accessible endtime (in minutes after midnight on accessible days) = 0

OK
```

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 (`TamConnector.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/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 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	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_Identity\tamclient\tamcfg.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.	

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 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 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.
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.

Table 6 TAM Mapping Information

Select Identity Resource Attribute	Attribute on Connector	TAM User Attribute	Attribute on Physical Resource (iPlanet)	Description
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 OpenView 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 OpenView Select Identity Connector Deployment Guide* for more information on deleting the connector from Select Identity and application server.

A Appendix: 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.