

HP Select Identity Software

Connector for IBM Tivoli Directory Server (Bidirectional LDAP Based)

Connector Version: 1.02

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

© Copyright 2006-2007 Hewlett-Packard Development Company, L.P.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>). Portions Copyright © 1999-2003 The Apache Software Foundation. All rights reserved.

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	7
2	Introduction	9
	About HP Select Identity	9
	About Connectors	9
	About IBM Tivoli Directory Bidirectional LDAP Connector	9
	High-Level Architecture	10
	Overview of Installation Tasks	11
3	Installing the Connector	13
	IBM Tivoli Directory Bidirectional LDAP Connector Files	13
	System Requirements	14
	Extracting Contents of the Schema File	14
	Verifying Configurable Parameters	14
	Installing the Connector RAR	15
	Installing the Password Plug-In	16
	Configuring IBM Tivoli Directory Server Changelog for Reverse Synchronization	17
4	Configuring the Connector with Select Identity	19
	Configuration Procedure	19
	Add a New Connector	19
	Add a New Resource	19
	Map Attributes	21
	Configure Workflow External Call on Select Identity	22
5	Uninstalling the Connector	23
A	Overview of Reverse Synchronization by Polling	25
	Overview of Reverse Synchronization by Polling	25
	About Cyclic Request	25
B	Troubleshooting	27

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 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
<i>Release Note</i> IBM Tivoli BiLDAP Connector v1.02 Release Note.htm	This file contains necessary information on new features of the connector, enhancements, known problems or limitations, and support information.	/Docs/ subdirectory under the connector directory.
<i>Connector Deployment Guide (for Select Identity 4.20)</i> connector_deploy_SI4.20.pdf	Connector deployment guides provide detailed information on: <ul style="list-style-type: none"> • Deploying a connector on an application server. • Configuring a connector with Select Identity. 	/Docs/ root directory on the product's CD media.
<i>Connector Deployment Guide (for Select Identity 4.10-4.13)</i> connector_deploy_SI4.13.pdf		
<i>Connector Deployment Guide (for Select Identity 4.0-4.01)</i> connector_deploy_SI4.pdf	Refer to these guides when you need generic information on connector installation.	
<i>Connector Installation and Configuration Guide</i> IBM Tivoli BiLDAP_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 IBM Tivoli Directory. An HP Select Identity connector for IBM Tivoli Directory enables you to provision users and manage identities on IBM Tivoli Directory Server. At the end of this chapter, you will be able to know about:

- The benefits of HP Select Identity.
- The role of a connector.
- The connector for IBM Tivoli Directory.

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 IBM Tivoli Directory Bidirectional LDAP Connector

The bidirectional LDAP based connector for IBM Tivoli Directory Server — hereafter referred to as IBM Tivoli Directory Bidirectional LDAP connector — enables Select Identity to perform the following tasks in IBM Tivoli Directory:

- 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

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

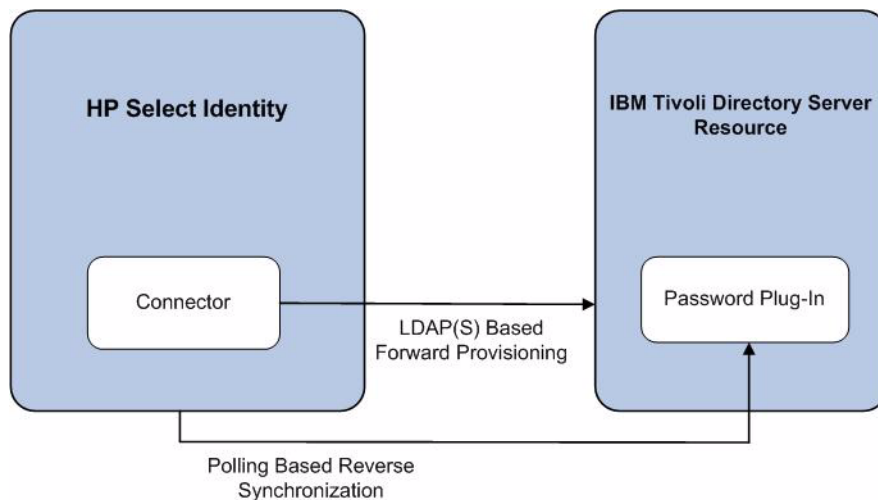
The reverse synchronization feature reconciles user account changes made on the IBM Tivoli Directory resource with Select Identity. Select Identity periodically polls the IBM Tivoli Directory resource to retrieve changes through the connector.

▶ This connector can be used with Select Identity 4.01-4.20.

High-Level Architecture

Figure 2 illustrates a high-level architecture of IBM Tivoli Directory Bidirectional LDAP connector. The connector uses an agent (Password Plug-In) to reconcile password changes to Select Identity. The Password Plug-In is installed on IBM Tivoli Directory Server.

Figure 2 High-Level Architecture of the IBM Tivoli Directory Bidirectional LDAP Connector



Overview of Installation Tasks

Before you start installing the connector, you must ensure that system requirements and all the installation prerequisites are met. Refer to the [Table 2](#) for an overview of installation tasks.

Table 2 Organization of Tasks

Task Number	Task Name	Reference
1	Install the connector on the Select Identity server.	See Installing the Connector on page 13.
	— Meet the system requirements.	See System Requirements on page 14.
	— Extract contents of the Schema file (file that contains the mapping files for the connector) to a location on the Select Identity server.	See Extracting Contents of the Schema File on page 14.
	— Verify configurable parameters in the <code>TivoliConfig.properties</code> file.	See Verifying Configurable Parameters on page 14.
	— Install the Resource Adapter Archive (RAR) of the connector on an application server.	See Installing the Connector RAR on page 15.
	— Install the Password Plug-In	See Installing the Password Plug-In on page 16.
	— Configure IBM Tivoli Directory Server for reverse synchronization.	See Configuring IBM Tivoli Directory Server Changelog for Reverse Synchronization 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 IBM Tivoli Directory Bidirectional LDAP connector on Select Identity server. At the end of this chapter, you will know about

- Software requirements to install the IBM Tivoli Directory Bidirectional LDAP connector.
- Procedure to install IBM Tivoli Directory Bidirectional LDAP connector.

IBM Tivoli Directory Bidirectional LDAP Connector Files

The IBM Tivoli Directory Bidirectional LDAP connector is packaged in the following files, which are located in the `Bidirectional LDAP Connector - IBM Directory` directory of the Select Identity Connector CD:

Table 3 IBM Tivoli Directory Bidirectional LDAP Connector Files

Serial Number	File Name	Description
1	<ul style="list-style-type: none">• <code>TivoliConnector_420.rar</code> for WebSphere• <code>TivoliConnector_420WL9.rar</code> for WebLogic	It contains the binaries for the connector.
2	<code>TivoliSchema.jar</code>	It contains the mapping file (<code>Tivoli.xml</code>), which control how Select Identity fields are mapped to IBM Tivoli Directory Server fields. It also contains the <code>TivoliConfig.properties</code> configuration files.
3	<code>TivPassfilt.dll</code> and <code>TivoliProperties.ini</code>	Password Plug-In files
4	<code>OpenSSLDLL.zip</code>	It contains the following dll files: <ul style="list-style-type: none">• <code>libeay32.dll</code>• <code>libssl32.dll</code>

System Requirements

The IBM Tivoli Directory Bidirectional LDAP connector is supported in the following environment:

Table 4 Platform Matrix for IBM Tivoli Directory Bidirectional LDAP Connector

Select Identity Version	Application Server	Database
4.01-4.20	The IBM Tivoli Directory Bidirectional LDAP connector is supported on all the platform configurations of Select Identity 4.01-4.20.	

The IBM Tivoli Directory Bidirectional LDAP connector is supported with IBM Tivoli Directory Server 5.2 on Windows 2003.

The IBM Tivoli Directory Bidirectional LDAP connector is internationalized and able to operate with languages that are supported by the Java Unicode specification. If you wish to use the connector on non-English platforms, make sure that the following prerequisites are met:

- The Select Identity server should be configured for internationalization. Refer to the *HP Select Identity Installation and Configuration Guide* for more information.
- The resource should be configured to support local language characters.

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

Verifying Configurable Parameters

The `TivoliConfig.properties` file, which is present in the `TivoliSchema.jar` file, contains the following configurable parameters. These parameters can be changed manually. Before installing the connector, verify the parameter values and change the values if they don't match with the values mentioned below.

- `entitlement-delimiter=|`
It contains the string delimiter that is displayed between an entitlement type and its name.
- `modify_replace=false`
It is a configuration parameter that can be set to true or false. When it is set to false, IBM Tivoli Directory Bidirectional LDAP connector uses modify/add and modify/delete operations to support multivalued attribute. When it is set to true, IBM Tivoli Directory Bidirectional LDAP connector uses modify/replace operation to support multivalued attribute.

- `attributeValue-delimiter=|`
It contains the string delimiter that is used to separate attribute values for multi valued attribute.
- `attribute-begins=[[`
Begin parameter to wrap the special base64 encoded attribute values while sending to connector from Select Identity.
- `attribute-ends=]]`
End parameter to wrap the special base64 encoded attribute values while sending to connector from Select Identity.
- `dualLink-support.<entity> = 0` where `<entity>` can be group, role, and so on.
If the value is set to 0, bidirectional linking operation is performed (the user as well as the entity will contain the `Link` attribute).
If the value is set to 1, only user-side linking operation is performed.
If the value is set to 2, only entity-side linking operation is performed.
- `dualLink-support=0`
This specifies whether a `Link` is a User `Link` or a Group `Link`. If it is 0, then it is User `Link` as well as Group `Link`.
- `multivalued-support=false`
This specifies whether Select Identity supports multivalued attributes or not. This property is used in the reverse provisioning, when a multivalued attribute is detected in the reprog during the polling, all the values of this multivalued attribute are combined as single valued string.
If true - Select Identity supports multivalued attributes.
If false - Select Identity does not support multivalued attributes.
- `unlink-before-terminate=false`
If you want to unlink the entitlements while performing a terminate user operation, set this flag to false.
- `mergeChangeLog=true`.
If multiple modifications are done at the resource on a user, all the modifications will be sent as a single reconciliation request when this parameter is set as true.

Installing the Connector RAR

To install the RAR file of the connector (such as `TivoliConnector_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.

Installing the Password Plug-In

The Password Plug-In module detects any change in password on the IBM Tivoli Directory Server. It consists of the `TivPassfilt.dll` and `TivoliProperties.ini` files. Perform the following steps to install the Password Plug-In module on IBM Tivoli Directory Server:

- 1 Extract contents of the `OpenSSLDLL.zip` file and copy the extracted contents to the location

`<system root>\system 32` on resource machine. The contents of this file are:

- `libeay32.dll`
- `libssl32.dll`

- 2 Copy the `TivPassfilt.dll` and `TivoliProperties.ini` files to the `% IBM HOME %\LDAP\bin` folder on the resource system.

- 3 Add following attribute to dn by using LDP:

```
cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas,  
cn=Configuration
```

```
add: ibm-slapdPlugin
```

```
ibm-slapdPlugin: postoperation /bin/TivPassfilt.dll postplugin_init
```

Alternatively, update the `ibmslapd.conf` file (which is in the folder `<% IBM HOME %>\LDAP\etc`) and in the `bmslapd.conf` file, add the following plugin related information under dn:

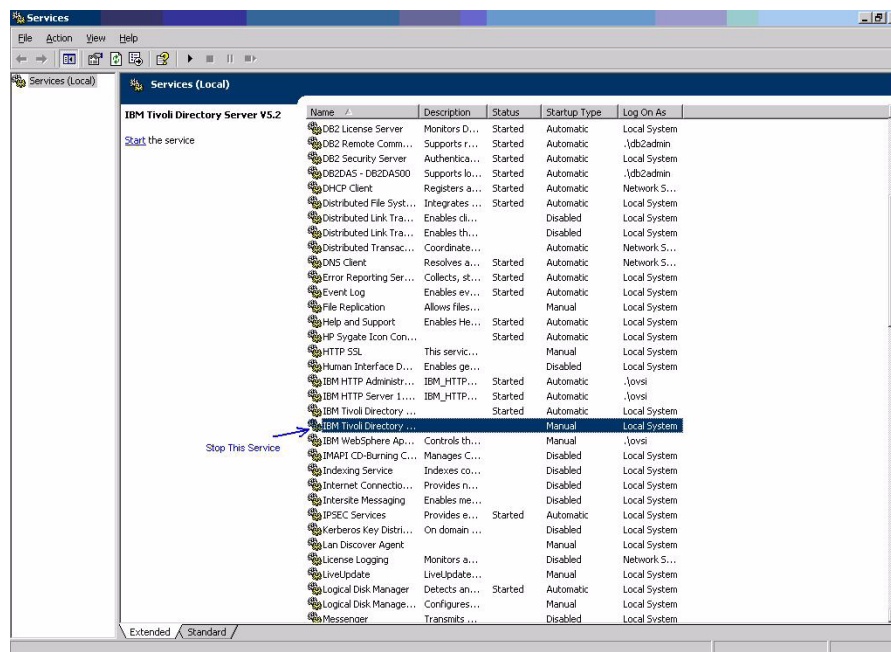
```
cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas,  
cn=Configuration , ibm-slapdPlugin: postoperation /bin/TivPassfilt.dll  
postplugin_init
```

- 4 Restart the server.

Configuring IBM Tivoli Directory Server Changelog for Reverse Synchronization

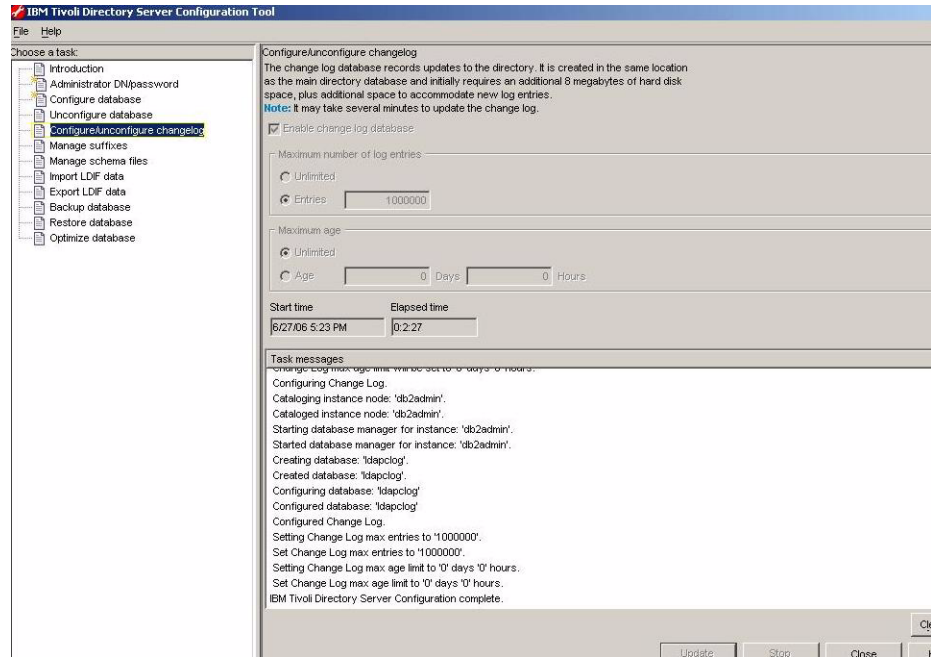
Perform the following steps to configure the Changelog of IBM Tivoli Directory Server to enable reverse synchronization:

- 1 Stop the IBM Tivoli Directory service from the Services window.



- 2 Open the IBM Tivoli Directory Configuration tool.
- 3 In the left pane, click **Configure/unconfigure changelog**.
- 4 In the right pane, select the Enable change log database check box.
- 5 Click **Update**. The Tak Messages pane displays the following message on successful configuration:

IBM Tivoli Directory Server Configuration complete.



4 Configuring the Connector with Select Identity

This chapter describes the procedure to configure the IBM Tivoli Directory Bidirectional LDAP 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 IBM Tivoli Directory Bidirectional LDAP 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/TivoliConnector`.
- 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 instruction on adding a resource in Select Identity.

Refer to the following table while entering the parameters in the Basic Information and the Access Information pages:

Table 5 Resource Configuration Parameters

Field Name	Sample Values	Description
Resource Name	ELDAPTivoli	Name given to the resource.
Connector Name	Tivoli	The newly deployed connector
Authoritative Source	Yes	Whether this resource is a system that is considered to be the authoritative source for user data in your environment. Specify Yes if the resource has to be authoritative.
Delete User	No	Specifies whether the user should be deleted from the resource when a DeleteServiceMembership operation is performed for the user in Select Identity.
Access URL	ldap://sidc:389	Resource connection URL - IP:port
Suffix	DC=hp,DC=com	Default root suffix.
Login Name	cn=root	Admin User Login Name. To block cyclic request, you must use an exclusive login name with administrative privilege and you must not use this login name for any other operation on IBM Tivoli Directory Server.
Password	IBMDSPASSWORD	Password of the admin user.
Default User Suffix	ou=people	Suffix where all users exist.
Default Group Suffix	ou=Groups	Suffix where all groups exist.
Mapping File	Tivoli.xml	Name of the file that specifies the attribute mappings. This file should exist in the classpath of the application server. Click View to open the file in a browser. If this file cannot be viewed, Select Identity could not locate it.
Select Identity Locale	en_US	Locale-specific information. If Country = US and Language = English, current locale string is en_US.

Configuring Polling for Reverse Synchronization:

After entering the resource access information, User Reconciliation Policy page appears. On this page, do the following.

- a Check the Polling Enable checkbox. Set the polling interval to the desired value.
- b Under the Modify section, set Reconciliation Workflow as Select Identity Recon User Enable Disable Workflow by using the drop-down box.

Keep all other default settings in this page.

Map Attributes

After successfully adding a resource for the IBM Tivoli Directory Bidirectional LDAP 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 IBM Tivoli Directory Bidirectional LDAP Mapping Information

Select Identity Resource Attribute	Connector Attribute	Attribute on IBM Tivoli Directory Server	Description
Addr1	Address1	postalAddress	
Addr2	Address2	roomNumber	
Email	Email	mail	
UserName	UserName	uid	<i>This attribute is mandatory for user creation.</i>
DN	DN	DN	
Zip	Zip	postalCode	
PhBus	BusinessPhone	telephoneNumber	
Password	Password	userPassword	<i>This attribute is mandatory for user creation.</i>
Title	Title	Title	
LastName	LastName	sn	<i>This attribute is mandatory for user creation.</i>
FirstName	FirstName	givenName	
State	State	st	
userSuffix	userSuffix	userSuffix	
City	City	l	
isAccountEnabled	isAccountEnabled	isAccountEnabled	While associating the resource to a service, do not add this attribute to the service.

Configure Workflow External Call on Select Identity

To achieve reverse synchronization, you must configure the workflow external call for user enable/ disable operation for IBM Tivoli Directory Bidirectional LDAP connector. Refer to *HP Select Identity Deployment Guide* for information on configuring user enable/disable workflow external call. While configuring, enter the parameters as given in [Table 7](#) below.

Table 7 User Enable/Disable Parameters for IBM Tivoli Directory Bidirectional LDAP Connector

Serial Number	Parameter Name	Parameter Value
1	AttributeName	isAccountEnabled
2	EnableValue	true
3	DisableValue	false
4	UserName	Select Identity admin user name. For example, sisa.
5	Password	Select Identity admin password. For example, abc123.
6	Url	Select Identity web service url. For example: <code>http://localhost:7001/lmz/webservice</code>

While entering these parameters, select the Sensitive checkbox only in case of Password.

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

5 Uninstalling the Connector

If you want to uninstall the connector, perform the following steps:

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

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

A Overview of Reverse Synchronization by Polling

Overview of Reverse Synchronization by Polling

Reverse synchronization in IBM Tivoli Directory Bidirectional LDAP connector is achieved by polling. Each time the polling is invoked, the following sequences take place in the background:

- 1 The polling batch task is invoked.
- 2 The polling batch task converts all the ChangeLogs into an SPML file, and the SPML file is converted to a request using the SPML parser and submitted to the Select Identity Reconciliation engine. Then ReconciliationHelper is called to execute all the Modify Requests.
- 3 In the provisioning stage of request execution, Select Identity is updated with the changes in the resource.



On Select Identity, if IBM Tivoli Directory Bidirectional LDAP service view has some attributes as mandatory, all of them should exist on IBM Tivoli Directory Bidirectional LDAP server and they should be sent when reverse add request comes from connector. That is, the only attributes that are coming in reverse add request can be mandatory in Select Identity Service view, if it is mandatory in view and it does not come in reverse add request, request will be rejected by Select Identity.

About Cyclic Request

The IBM Tivoli Directory Bidirectional LDAP connector supports both forward provisioning and change detection. When a forward operation is performed on the resource, the next polling cycle of the connector may detect the operation as if it was performed directly on the IBM Tivoli Directory Server. This is called cyclic request. To block any cyclic request, during resource creation on Select Identity, you must use an exclusive administrative username/login name of IBM Tivoli Directory Server and you must not use that username/login name for any other operation on IBM Tivoli Directory Server.

B Troubleshooting

- While creating and trying to save a resource, you get error The following resource failed to save: Reason: Unable to test connector.

Solution:

Verify the following properties file are in the application server classpath while deploying the connector:

```
com\hp\ovsi\connector\bidirldap\tivoli\  
TivoliConfig.properties
```

