

# HP OpenView Select Identity

## Connector for Microsoft Windows Active Directory and Exchange 2000

### Installation Guide

Software Version: 3.0.1



October 2004

© 2004 Hewlett-Packard Development Company, L.P.

## Legal Notices

### Warranty

*Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.*

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

### Restricted Rights Legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company  
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

### Copyright Notices

© 2004 Hewlett-Packard Development Company, L.P.

No part of this document may be copied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>). Portions Copyright (c) 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.

This product includes software developed by Teodor Danciu (<http://jasperreports.sourceforge.net>). Portions Copyright (C) 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](http://www.waveset.com)). Portions Copyright © 2003 Waveset Technologies, Inc. 6034 West Courtyard Drive, Suite 210, Austin, Texas 78730. All rights reserved.

Portions Copyright (c) 2001-2004, Gaudenz Alder. All rights reserved.

## Trademark Notices

HP OpenView Select Identity is a trademark of Hewlett-Packard Development Company, L.P. Microsoft, Windows, the Windows logo, and SQL Server are trademarks or registered trademarks of Microsoft Corporation.

Sun™ workstation, Solaris Operating Environment™ software, SPARCstation™ 20 system, Java technology, and Sun RPC are registered trademarks or trademarks of Sun Microsystems, Inc. JavaScript is a trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

This product includes the Sun Java Runtime. This product includes code licensed from RSA Security, Inc. Some portions licensed from IBM are available at <http://oss.software.ibm.com/icu4j/>.

IBM, DB2 Universal Database, DB2, WebSphere, and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

This product includes software provided by the World Wide Web Consortium. This software includes xml-apis. Copyright © 1994-2000 World Wide Web Consortium, (Massachusetts Institute of Technology, Institute National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. <http://www.w3.org/Consortium/Legal/>

Intel and Pentium are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.

AMD and the AMD logo are trademarks of Advanced Micro Devices, Inc.

BEA and WebLogic are registered trademarks of BEA Systems, Inc.

VeriSign is a registered trademark of VeriSign, Inc. Copyright © 2001 VeriSign, Inc. All rights reserved.

All other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

## Support

Please visit the HP OpenView web site at:

**<http://openview.hp.com/>**

There you will find contact information and details about the products, services, and support that HP OpenView offers.

You can go directly to the support web site at:

**<http://support.openview.hp.com/>**

The support web site includes:

- Downloadable documentation
- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information

# contents

<b>Chapter 1</b>	<b>Installing the Connector</b> .....	7
	Deploying on the Web Application Server .....	8
	Installing the Agent on the Windows Server .....	9
	Determining the Version of ADSI .....	10
	Installing the Agent .....	10
<b>Chapter 2</b>	<b>Understanding the Mapping Files</b> .....	14
	User Attributes for Active Directory .....	15
	User Attributes for Exchange .....	21
<b>Chapter 3</b>	<b>Uninstalling the Connector</b> .....	22
	Uninstalling the Active Directory Connector .....	22
	Uninstalling the Agent .....	23

## Installing the Connector

The Windows Active Directory connector enables HP OpenView Select Identity to manage user data in Windows Active Directory systems. Because Microsoft Exchange 2000 relies on Active Directory for storing user data, you can also use this connector to provision user mailboxes in Exchange 2000.

This connector is a two-way connector and pushes changes made to user data in the Select Identity database to the target Windows Active Directory server. It also enables the agent on the Windows server to send password updates back to Select Identity. The mapping files, which are included with the connector, control how Select Identity fields are mapped to Active Directory fields.

The Windows Active Directory connector is packaged in the following files, which are located in the `Active Directory` folder on the Select Identity Connector CD:

- `ADConnector.rar` — contains the binaries for the connector
- `ADSchema.jar` — contains the following mapping files:
  - `aduser.properties` — maps the Select Identity user attributes to the Active Directory user attributes
  - `adgroup.properties` — maps the Select Identity group attributes to Active Directory group attributes; note that group provisioning is not currently supported, though this file must be extracted during installation

- `adcomputer.properties` — maps the Select Identity computer attributes to the Active Directory attributes; note that computer provisioning is not currently supported, though this file must be extracted during installation
- `ADSetup.zip` — contains the installation executable for the Active Directory agent

## Deploying on the Web Application Server

To install the Windows Active Directory connector on the Select Identity server, complete these steps.



Perform this procedure after the Select Identity product installation. This procedure installs the connector on WebLogic 8.1; you must be familiar with the WebLogic platform.

- 1 Create a subdirectory in the Select Identity home directory, which was created on the application server during the product installation.
- 2 Copy the `ADConnector.rar` file to the new subdirectory.
- 3 Copy the `ADSchema.jar` file from the Select Identity Connector CD to a temporary folder.
- 4 Extract the `ADSchema.jar` file, which contains the mapping files, to the Select Identity home directory.
- 5 Ensure that the `CLASSPATH` environment variable that is set in the WebLogic startup script references the Select Identity home directory.
- 6 Modify the mapping files, if necessary. These files are described in detail in [Understanding the Mapping Files on page 14](#).
- 7 Start the application server if it is not currently running.
- 8 Log on to the WebLogic Server Console.
- 9 Navigate to ***My\_domain*** → **Deployments** → **Connector Modules**.
- 10 Click **Deploy a New Connector Module**.
- 11 Locate and select the `ADConnector.rar` file from the list. It is stored in the connector subdirectory of the Select Identity home directory.

- 12 Click **Target Module**.
- 13 Select the **My Server** (your server instance) check box.
- 14 Click **Continue**. Review your settings.
- 15 Keep all default settings and click **Deploy**.

The Status of Last Action column should display Success.

After installing the connector, log on to the Select Identity client and deploy the connector using the Connector pages. Then, create a resource that represents the connector, and configure a Service that relies on the Windows Active Directory resource. See the *HP OpenView Select Identity Administrator Guide* for procedures. The Resource Access Information appendix provides detailed information about creating a Window Active Directory resource.

## Installing the Agent on the Windows Server

After you install the Windows Active Directory connector on the Select Identity server, you can install the agent on the Windows system. The agent is a suite of Services and support DLLs deployed on the resource.

The following environment is required:

- Microsoft Windows 2000 Server, Service Pack 4 or later. The system must also be a domain controller (Primary / Backup domain controller).
- Active Directory ADSI 5,0,00,0. See below for information about determining the version of ADSI.
- Internet Explorer 5.5 or later (supporting MSXML 2.0 or later).
- Winsock 2.0 or later.
- If the server and resource machines communicate across a firewall, they must allow bidirectional TCP flow on port 5000 (this can be configured on any other port, as well).

You also need the administrative user name and password to log on to the system during the installation.

## Determining the Version of ADSI

To determine the version of ADSI, review the following key in the registry:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Active Setup\  
Installed Components\{E92B03AB-B707-11d2-9CBD-0000F87A369E}

The following table describes ADSI versions with the values that may be found in this registry key:

Version	Value
Earlier than 2.5	N.A.
2.5	2,5,00,0
Windows 2000	5,0,00,0
DSClient	5,0,00,0

Versions earlier than ADSI 2.5 do not create this registry key. If this key is not present, look then for the following key:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Ads

If this key is present, ADSI 2.0 is installed. If this key is not present, it may be an improper installation, or no ADSI is installed at all.

## Installing the Agent

Perform the following to install the agent:

- 1 Copy the ADSetup.zip file from the Select Identity Connector CD to a folder on the Windows Active Directory server.
- 2 Extract the ADSetup.zip file.
- 3 Double-click SETUP.exe to start the installation program.
- 4 Click **Next** to proceed through the installation.
- 5 If needed, provide administrative logon information when prompted.

- 6 Configure the Windows Active Directory agent options. The configuration is defined on the HP Openview Active Directory Connector dialog.

- a Select the **Enable AD Connector Agent** check box. This starts the connector, enabling it to receive provisioning requests from Select Identity.
  - b In the Active Directory Port field, enter the number of the Active Directory listening port, such as 389.
  - c Enter a port number in the Connector Server Port field. The connector uses this port to communicate with the agent. The default is 5000.
  - d Select the **Enable Log Option** check box to enable logging for the connector on the Select Identity server. Then, configure the following logging options:
    - Select the depth of logging from the Log Level drop-down list. The levels include Basic, Intermediate, Advanced, and Developer, where Developer is the most verbose level.
    - Specify where the log file will reside in the Log File field. The default value is *install\_dir*\Logs.
- 7 Perform the following to enable reverse synchronization and reconciliation. This step is optional.
- a Ensure that the **Enable Notification Agent** option is *not* selected. This check box is provided for future support; this functionality is not currently supported
  - b If you want to synchronize the Windows server password with Select Identity, select **Enable Password Synchronization**. This is used by the agent to synchronize password changes with Select Identity. The

information is sent back to Select Identity in the form of an SPML `extendedRequest` over SOAP and HTTP or HTTPS.

- c** Enter the IP address of the server running Select Identity in the Server field.
- d** Enter the port of the application server running Select Identity, such as port 7001 for WebLogic, in the Port field.
- e** Enter the base URL for the Select Identity Web Service in the Base field. The default value is `/lmz/webservice/`.
- f** Select **HTTP** or **HTTPS** from the Server Type drop-down list. This defines the protocol for sending passwords to Select Identity.
- g** If the Select Identity Web Service requires authentication, enter the user name in the User Name field.
- h** Enter the password of account in the Password field.
- i** Keep the default settings in the Time Out and Retries fields. The Time Out field specifies the number of milliseconds after which the request times out. The Retries field specifies the number of retries that the agent will attempt to send the SPML request.
- j** Configure the Operational Attribute settings. This enables you to send information in SPML requests back to Select Identity (in the header of the request) for synchronization.
  - Enter the name of the administrator account on the Active Directory resource in the Username field.
  - Enter the account's password in the Password field.
  - Add the resource ID operational attribute. First, enter **urn:trulogica:concero:2.0#resourceId** in the Attribute Name and click **>>**. Then, in the Attribute Value field, enter the name of the resource that you create in Select Identity for this Windows server, and click **>>**. For example, if you specify **WindowsActiveDir** here, you must specify **WindowsActiveDir** when creating the resource for this connector in Select Identity.
  - Add the reverse synchronization operational attribute. First, enter **urn:trulogica:concero:2.0#reverseSync** in the Attribute Name and click **>>**. Then, enter **true** in the Attribute Value field and click **>>**.

**8** After defining all of your settings, click **OK**.

- 9 After the installation is complete, click **Finish**.
- 10 If you configured reverse synchronization in [Step 7 on page 11](#), verify that the "When maximum log size is reached: Overwrite Events as needed" option is enabled in the "Security Log" properties on the Windows system. To view this configuration, select **Start** → **Settings** → **Control Panel**, double-click **Administrative Tools**, then double-click **Event Viewer**. Right-click **Security Log** and select **Properties**.

Also, if you installed the agent on a Windows 2000 Server (Primary Domain Controller or Backup Domain Controller), you must enable strong password enforcement. To do so, select **Start** → **Settings** → **Control Panel**, double-click **Administrative Tools**, then double-click **Local Security Policy**. Expand the `Account Policies` folder and double-click **Passwords must meet complexity requirements**. Select the **Enable** option and click **OK**.

- 11 Restart the Windows server.

The installation process performed the following:

- Created the target folder with the binaries and support files in the appropriate folders. Placed `TLPassfilt.dll` and `TLUtils.dll` in the Windows System folder, `$WinSysPath$(c:\winnt\system32)`. The following folder structure was created:
  - `<TARGETDIR>` — The parent folder
  - `<TARGETDIR>\Bin` — Program binaries
  - `<TARGETDIR>\Logs` — Connector log folder
  - `<TARGETDIR>\Map` — Mapping of operational attributes
  - `<TARGETDIR>\Servers` — Server binaries
- Created and configured corresponding services.
- Created a Program group and shortcuts for the connector configuration console and the uninstallation script.
- Set up the registry for program parameters.

## Understanding the Mapping Files

The Windows Active Directory connector is deployed with the following mapping files:

- `aduser.properties`
- `adgroup.properties`
- `adcomputer.properties`

These files contain the attributes required by the resource and are used to map user account additions and modifications from Select Identity to the system resource. When you deploy a resource through the Resources pages on the Select Identity client, you can review this file.



Note that the `adgroup.properties` and `adcomputer.properties` files are installed with the Windows Active Directory connector and must be present on the system, but group and computer provisioning is not supported at this time.

You can create attributes that are specific to Select Identity using the Attributes pages on the Select Identity client. You can then use these attributes to associate Select Identity user accounts with system resources by mapping the attributes in the mapping file described in this chapter. This process becomes necessary because, for example, a single attribute “username” can have a different definition on three different resources, such as “login” for UNIX, “UID” for a database, and “userID” on a Windows server.

You do not need to edit the `aduser.properties` file unless you want to map additional attributes to the Active Directory resource. If attributes and values are not defined in this mapping file, they cannot be saved to the resource through Select Identity.



You *must* edit the `aduser.properties` mapping file if you wish to provision user mailboxes in Exchange 2000. By default, the mapping file is configured for Active Directory only.

The `aduser.properties` file is a text file that maps each Select Identity attribute to an attribute on the resource; the attributes are delimited by `|`. Consider this excerpt:

```
User Name|UserId
```

The Select Identity user attribute is named `User Name` and it is mapped to the `UserId` attribute on the Active Directory resource.

Attributes can be concatenated. The attribute names and the separators must not contain the `|` delimiter. For concatenation, the format is as follows:

```
[<SI Attribute>]<separator>[<SI Attribute>] |<Resource Attribute>
```

as in this example:

```
[First Name] [Last Name] |DisplayName
```

where `First Name` and `Last Name` are attributes in Select Identity. They are concatenated to form the value of the `DisplayName` attribute in Active Directory. A space is used as a separator between the two Select Identity attributes.

## User Attributes for Active Directory

The `aduser.properties` file provides the mandatory mappings that must be configured for Select Identity to provision users in Active Directory. The primary key is `UserId`; this Active Directory attribute must be mapped to a Select Identity attribute in order for user information to be stored on the Active Directory server. It should be the first entry in `aduser.properties`, and `Password` must be the second mapping in the file.

You can edit the Select Identity resource attributes; they reflect the identity information as seen in Select Identity. The physical resource attributes are literal attributes of user accounts on Active Directory. These attributes cannot

be changed. The following table provides a list of all Active Directory attributes that you can map if you wish to provision users with this information. Here is a description of the columns provided in the table:

- **Select Identity Resource Attribute**— The attribute used by the Windows Active Directory connector, as defined in the mapping file.
- **Active Directory User Attribute** — The name of the attribute on the Windows server.
- **Label on Active Directory UI** — The name of the property on the UI that corresponds to the attribute on the Windows server.
- **Description** — A description of the attribute and any noteworthy information needed when assigning values to the attribute.

The mandatory attributes that are mapped by default are noted.

<b>Select Identity Resource Attribute</b>	<b>Active Directory User Attribute</b>	<b>Label on Active Directory UI</b>	<b>Description</b>
User Name	UserId	User Logon Name (on the Account tab)	Primary key for the Active Directory user. Same as samAccountName and UserPrincipalName.
Password	Password	Password (on the Account tab)	User's password.
[First Name] [Last Name]	DisplayName	Display Name (on the General tab)	Name displayed in the address book. This is usually a combination of the user's first name, middle initial, and last name.
countryName	C	Country/Region (on the Address tab)	Two-character abbreviation of the country or region, per the ISO 3166-1 format.

<b>Select Identity Resource Attribute</b>	<b>Active Directory User Attribute</b>	<b>Label on Active Directory UI</b>	<b>Description</b>
Comment	Info	Notes (on the Telephone tab)	Notes about the user.
ScriptPath	ScriptPath	Logon Script (on the Profile tab)	The path of the user's logon script, which can be a .CMD, .EXE, or .BAT file. The string can be null.
HomeDirectory	HomeDirectory	Home Folder: Local path or Home Folder: To (on the Profile tab, field dependent on homeDrive)	A path to a home share or a local directory path, but not both.
(not mapped by default)	GivenName	First Name (on the General tab)	First (given) name.
(not mapped by default)	sn	Last Name (on the General tab)	Last name (surname).
(not mapped by default)	Initials	Initials (on the General tab)	Single-valued property containing the initials of the user's full name. This may be used as the middle initial in the Windows Address Book.
(not mapped by default)	Description	Description (on the General tab)	Description of the user.
(not mapped by default)	physical Delivery OfficeName	Office (on the General tab)	The office location in the user's place of business.
(not mapped by default)	Telephone Number	Telephone Number (on the General tab)	Primary telephone number.

<b>Select Identity Resource Attribute</b>	<b>Active Directory User Attribute</b>	<b>Label on Active Directory UI</b>	<b>Description</b>
(not mapped by default)	Other Telephone	Telephone: Other (on the General tab)	Alternate telephone number.
(not mapped by default)	Mail	E-Mail (on the General tab)	Email address.
(not mapped by default)	wwwHomePage	Web Page (on the General tab)	URL of the user's primary web page.
(not mapped by default)	url	Web Page: Other (on the General tab)	Alternate web page address.
(not mapped by default)	StreetAddress	Street (on the Address tab)	Street address.
(not mapped by default)	PostOfficeBox	P.O.Box (on the Address tab)	Post Office box.
(not mapped by default)	L	City (on the Address tab)	Single-valued property containing the locality, such as the town or city, in the user's address.
(not mapped by default)	St	State/Province (on the Address tab)	State or province.
(not mapped by default)	PostalCode	Zip/Postal Code (on the Address tab)	Postal (zip) code.
(not mapped by default)	HomePhone	Home (on the Telephone tab)	User's home phone number.
(not mapped by default)	OtherHome Phone	Home: Other (on the Telephone tab)	Alternate home phone number.
(not mapped by default)	Pager	Pager (on the Telephone tab)	User's pager number.

<b>Select Identity Resource Attribute</b>	<b>Active Directory User Attribute</b>	<b>Label on Active Directory UI</b>	<b>Description</b>
(not mapped by default)	OtherPager	Pager: Other (on the Telephone tab)	Alternate pager number.
(not mapped by default)	Mobile	Mobile (on the Telephone tab)	Primary mobile telephone number.
(not mapped by default)	OtherMobile	Mobile: Other (on the Telephone tab)	Alternate mobile number.
(not mapped by default)	facsimile Telephone Number	Fax (on the Telephone tab)	Telephone number of the user's business fax machine.
(not mapped by default)	other Facsimile Telephone Number	Fax: Other (on the Telephone tab)	Alternate fax number.
(not mapped by default)	IpPhone	IP phone (on the Telephone tab)	Telephony phone number.
(not mapped by default)	OtherIpPhone	IP phone: Other (on the Telephone tab)	Alternate telephony number.
(not mapped by default)	ProfilePath	Profile Path (on the Profile tab)	A path to the user's profile. This value can be a null string, a local absolute path, or a UNC path.

<b>Select Identity Resource Attribute</b>	<b>Active Directory User Attribute</b>	<b>Label on Active Directory UI</b>	<b>Description</b>
(not mapped by default)	HomeDrive	Home Folder: Connect (on the Profile tab)	If a valid drive letter is specified, the HomeDirectory attribute becomes a share path; otherwise, it is considered a local directory path.
(not mapped by default)	Department	Department (on the Organization tab)	User's department.
(not mapped by default)	Title	Title (on the Organization tab)	User's formal job title or designation, such as "Senior manager."
(not mapped by default)	Company	Company (on the Organization tab)	Company for which the user works.
(not mapped by default)	Manager	Manager: Name (on the Organization tab)	The fully qualified, distinguished name of the manager. The manager's user object contains a directReports property that contains references to all user objects that have their manager properties set to the manager's user object.

## User Attributes for Exchange

If you wish to configure the connector to provision user mailboxes in Exchange 2000, you *must* add the following Exchange 2000 attributes in the `aduser.properties` file:

```
<SI Attribute>|mailNickname
```

```
<SI Attribute>|msExchHomeServerName
```

where the SI attributes are attributes configured on the Select Identity server.

The `mailNickname` attribute on the Exchange 2000 server is the name portion of the Email address. For example, if the email address is `vlee@mydomain.com`, the `mailNickname` attribute is assigned the `vlee` portion of the email address.

The `msExchHomeServerName` attribute is a concatenation of several server values. Here is the syntax:

```
/o=exOrg/ou=First Administrative Group/cn=Configuration/cn=Servers/  
cn=mailStorage
```

where

- *exOrg* is the Exchange organization name. An example is **First Organization**.
- *mailStorage* is the Exchange mailbox name. An example is **MYSTORAGE**.

In addition, you can map an Select Identity attribute to the `HomeMDB` attribute on the Exchange 2000 server. (On the Exchange 2000 interface, this attribute maps to the Mailbox store property on the General tab for Active Directory User.) The `HomeMDB` attribute represents the URL of the user's mailbox. This property is read-only and is set when the mailbox is created.

## Uninstalling the Connector

If you need to uninstall a connector from Select Identity, make sure that the following are performed:

- All resource dependencies are removed.
- The connector is deleted through the Connectors home page on the Select Identity client.

## Uninstalling the Active Directory Connector

Perform the following to delete a connector:

- 1 Log on to the WebLogic Server Console.
- 2 Navigate to ***My\_Domain*** → **Deployments** → **Connector Modules**.
- 3 Click the delete icon next to the connector that you want to uninstall.
- 4 Click **Yes** to confirm the deletion.
- 5 Click **Continue**.

## Uninstalling the Agent

Perform the following steps to delete the agent on the Windows server:

- 1 From the Start menu, select **Programs** → **HP OpenView AD Connector** → **Uninstall Agent**.
- 2 Complete the installation as prompted by the wizard.