

HP OpenView Select Identity

Connector for CA eTrust LDAP Servers

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

© Copyright 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). 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, Institut 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

Chapter 1	Installing the Connector	7
Chapter 2	Understanding the Mapping File	9
	General Information	10
	eTrust LDAP Mapping Information	13
Chapter 3	Uninstalling the Connector	15

Installing the Connector

The eTrust LDAP connector enables HP OpenView Select Identity to manage user data in LDAP on eTrust servers. It is a one-way connector and pushes changes made to user data in the Select Identity database to a target LDAP server. The mapping file controls how Select Identity fields are mapped to LDAP fields.

The eTrust LDAP connector is packaged in the following files:

- `schema.jar` – contains the attribute mapping files for this system
- `TALDAPv3.rar` – contains the connector's binary files

These files are located in the `LDAP_eTrust` directory on the Select Identity Connector CD.

To install the eTrust LDAP connector on the Select Identity server, complete these steps.



Perform this procedure after the Select Identity product installation. The application server in this example is WebLogic 8.1, therefore you must be familiar with the WebLogic platform.

- 1 A `Select_Identity` directory was created on the application server during the product installation. Create a `connector` folder in this directory.
- 2 Copy the `TALDAPv3.rar` file to the `connector` folder in the `Select_Identity` directory.
- 3 Copy `schema.jar` file from the Select Identity Connector CD to a temporary directory.
- 4 Extract the `schema.jar` contents to the `Select_Identity` directory.
- 5 Ensure that the `CLASSPATH` environment variable in the WebLogic server startup script references the `Select_Identity` directory.
- 6 Modify the mapping file, if necessary. See [Understanding the Mapping File on page 9](#) for details.
- 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 `TALDAPv3.rar` file from the list. It is stored in the `Select_Identity\connector` 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 eTrust LDAP resource. See the *HP OpenView Select Identity Administrator Guide* for procedures. The Resource Access Information appendix provides detailed information about creating an eTrust LDAP resource.

Understanding the Mapping File

The eTrust LDAP connector is deployed with the `CAEtrust.xml` mapping file, which describes the attributes required by the system. The file is created in XML, according to SPML standards, and is bundled in a JAR file called `schema.jar`. The mapping file is used to map user account additions and modifications from Select Identity to the system resource. When you deploy a resource using the Resources page of the Select Identity client, you can review this file.

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

This file does not need to be edited unless you want to map additional attributes to your resource. If attributes and values are not defined in this mapping file, they cannot be saved to the resource through Select Identity.

General Information

The following operations can be performed in the mapping file:

- Add a new attribute mapping
- Delete an existing attribute mapping
- Modify attribute mappings

Here is an explanation of the elements in the XML mapping files provided by the eTrust LDAP connector:

- **<Schema>**, **<providerID>**, and **<schemaID>**

Provides standard elements for header information.

- **<objectClassDefinition>**

Defines the actions that can be performed on the specified object as defined by that name attribute (in the **<properties>** element block) and the Select Identity-to-resource field mappings for the object (in the **<memberAttributes>** block). For example, the object class definition for users defines that users can be created, read, updated, deleted, reset, and expired in LDAP.

- **<properties>**

Defines the operations that are supported on the object. This can be used to control the operations that are performed through Select Identity. The following operations can be controlled:

- Create (CREATE)
- Read (READ)
- Update (UPDATE)
- Delete (DELETE)
- Enable (ENABLE)
- Disable (DISABLE)
- Reset password (RESET_PASSWORD)
- Expire password (EXPIRE_PASSWORD)
- Change password (CHANGE_PASSWORD)

The operation is assigned as the name of the <attr> element and access to the operation is assigned to a corresponding <value> element. You can set the values as follows:

- true — the operation is supported by the connector
- false — the operation is not supported by the connector and will throw a permission exception
- bypass — the operation is not supported by the connector but will not throw any exception; the operation is simply bypassed

Here is an example:

```
<objectClassDefinition name="User" description="eTrust User">
  <properties>
    <attr name="CREATE">
      <value>true</value>
    </attr>
    <attr name="READ">
      <value>true</value>
    </attr>
  </properties>
</objectClassDefinition>
```

- **<memberAttributes>**

Defines the attribute mappings. This element contains <attributeDefinitionReference> elements that describe the mapping for each attribute. Each <attributeDefinitionReference> must be followed by an <attributeDefinition> element that specifies details such as minimum length, maximum length, and so on.

Each <attributeDefinitionReference> element contains the following attributes:

- Name — the name of the reference.
- Required — if this attribute is required in the provisioning (set to true or false).
- Conzero:tafield — the name of the Select Identity resource attribute.
- Conzero:resfield — the name of the physical resource attribute from the resource schema. If the resource does not support an explicit schema (such as UNIX), this can be a tag field that indicates a resource attribute mapping.

- `Concero:isKey` — An optional attribute that, when set to true, specifies that this is the key field to identify the object on the resource. Only one `<attributeDefinitionReference>` can be specified where `isKey="true"`. This key field does not need to be the same as the key field of the identity object in Select Identity.
- `Concero:init` — An optional attribute that identifies that the attribute is initialized with the value of the attribute passed in from Select Identity.

Here is an example:

```
<memberAttributes>
  <attributeDefinitionReference name="User Name"
    required="true" concero:tafield="[User Name]"
    concero:resfield="cn" concero:isKey="true"
    concero:init="true" />
```

The interpretation of the mapping between the connector field (as specified by the `Concero:tafield` attribute) and the resource field (as specified by the `Concero:resfield` attribute) is determined by the connector. The eTrust LDAP connector has code to interpret the mappings in one way, as follows:

- The connector attribute names are specified in square braces, like this: `[xyz]`. The value of attribute `xyz` is taken from the `UserModel` during provisioning.
- Composite attributes can be specified in the eTrust LDAP connector mapping file. To do this, specify `[attr1] xxxx [attr2]` as the connector attribute. This specifies that the value of the `attr1` and `attr2` attributes should be combined with the string `xxxx` to form a mapping for the specified resource field. eTrust LDAP connector has code to handle these composite mappings.

- **<attributeDefinition>**

Defines the properties of each object's attribute. For example, the attribute definition for the `HomeDir` attribute defines that it must be between zero and 100 characters in length and can contain the following letters, numbers, and characters: `a-z`, `A-Z`, `0-9`, `@`, `+`, and a space.

Here is an excerpt from the `CAetrust.xml` file:

```
<attributeDefinition name="HomeDir" description="User Home
directory" type="xsd:string" >
  <properties>
```

```

    <attr name="minLength">
      <value>0</value>
    </attr>
    <attr name="maxLength">
      <value>128</value>
    </attr>
    <attr name="pattern">
      <value><![CDATA[[a-zA-Z0-9@]+]]> </value>
    </attr>
  </properties>
</attributeDefinition>

```

- **<concerro:entitlementMappingDefinition>**
Defines how entitlements are mapped to users.
- **<concerro:objectStatus>**
Defines how to assign status to a user.
- **<concerro:relationshipDefinition>**
Defines how to create relationships between users.

eTrust LDAP Mapping Information

The following are the attribute mappings supported for CA eTrust. These are listed in the `CAEtrust.xml` mapping file. You can add, modify, or delete attributes once you are familiar with the contents of this 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 the eTrust LDAP server. These attributes cannot be changed. See the *HP OpenView Select Identity Connector Developer Guide* for more information about attributes and mapping information.

Select Identity Resource Attribute	CA eTrust LDAP Attribute	Description
UserName	cn	Key field on the resource
Password	userpassword	
First Name	givenname	
Last Name	sn	
Middle Name	initials	
FirstName + LastName	uid	
Last Name + First Name	displayName	
Email	mail	
Address1	postalAddress	
Address2	street	
City	l	
State	st	
Zip	postalCode	
Title	title	
Business Phone	telephoneNumber	
Home Phone	homePhone	
Mobile Phone	mobile	
Disable Function	Description="Disabled"	Marks the user as disabled
Enable Function	Description="Active"	Marks the user as enabled

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 using the Select Identity client Connectors pages.

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**.