HP OpenView Select Identity

Connector for CA eTrust LDAP Servers

Installation and Configuration Guide

Connector Version: 3.3
Select Identity Version: 3.3

April 2005

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

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.
- BouncyCastle engine for keystore management, bouncycastle.org.

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://www.managementsoftware.hp.com/

This web site provides contact information and details about the products, services, and support that HP OpenView offers.

You can also go directly to the support web site at:

http://support.openview.hp.com/

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 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://support.openview.hp.com/access_level.jsp

To register for an HP Passport ID, go to:

https://passport.hp.com/hpp2/newuser.do

contents

1

Installing the Connector

The CA eTrust LDAP connector enables HP OpenView Select Identity to perform the following tasks in LDAP on CA eTrust 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
- Assign and unassign entitlements to and from users

The eTrust LDAP connector 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.

This connector is supported on non-US platforms. This connector relies on the JNDI (LDAP's resource provider interface) to exchange data with LDAP.

The eTrust LDAP connector is packaged in the following files:

- `schema.jar` — contains the `caetrust.xml` mapping file, which controls how Select Identity fields are mapped to CA eTrust LDAP fields
- `TALDAPv3.rar` — contains the connector's binary files

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

System Requirements

The eTrust LDAP connector is supported in the following environment:

Select Identity Version	Application Server	Database
3.0.2	WebLogic 8.1.2 on Windows 2003	SQL Server 2000
	WebLogic 8.1.2 on Solaris 9	Oracle 9i
	WebLogic 8.1.2 on HP-UX 11i	Oracle 9i
	WebSphere 5.1.1 on Solaris 9	DB2 8.2 (or DB2 8.1 Service Pack 7)
3.3	WebLogic 8.1.4 on Windows 2003	SQL Server 2000

The connector is supported with eTrust Directory 4.0 on Windows 2000 and Solaris 9.

Deploying on the Web Application Server

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

1. Create a subdirectory in the Select Identity home directory where the connector's RAR file will reside. For example, you could create the `C:\Select_Identity\connectors` folder on Windows. (A connector subdirectory may already exist.)
2. Copy the `TALDAPv3.rar` file from the Select Identity Connector CD to the connector subdirectory.
3. If deploying the connector on WebLogic, complete the following steps. If deploying on WebSphere, skip to Step 4 on page 10.
   a. Create a schema subdirectory in the Select Identity home directory where the connector's mapping file(s) will reside. For example, you could create the `C:\Select_Identity\schema` folder. (This subdirectory may already exist.)
   b. Extract the contents of the `schema.jar` file (on the Select Identity Connector CD) to the schema subdirectory.
   a. Ensure that the CLASSPATH environment variable in the WebLogic server startup script references the schema subdirectory.
   b. Start the application server if it is not currently running.
   c. Log on to the WebLogic Server Console.
   d. Navigate to ***My_domain*** → **Deployments** → **Connector Modules**.
   e. Click **Deploy a New Connector Module**.
   f. Locate and select the `TALDAPv3.rar` file from the list. It is stored in the connector subdirectory.
   g. Click **Target Module**.
   h. Select the **My Server** (your server instance) check box.
   i. Click **Continue**. Review your settings.
   j. Keep all default settings and click **Deploy**. The Status of Last Action column should display Success.

4 If deploying the connector on WebSphere, complete the following steps:

   a Stop the application server.

   b Extract the contents of the `schema.jar` file (on the Select Identity Connector CD) to the `WebSphere\AppServer\lib\ext` directory.

   c Start the application server.

   d Log on to the WebSphere Application Server Console.

   e Navigate to **Resources** → **Resource Adapters**.

   f Click **Install RAR**.

   g In the Server path field, enter the path to the `TALDAPv3.rar` file. It is stored in the subdirectory created in Step 1.

   h Click **Next**.

   i In the Name field, enter a name for the connector.

   j Click **OK**.

   k Click the **Save** link (at the top of the page).

   l On the Save to Master Configuraton dialog, click the **Save** button.

   m Click **Resources** → **Resource Adapters**.

   n Click the new connector.

   o Click **J2C Connection Factories** in the Additional Properties table.

   p Click **New**.

   q In the Name field, enter the name of the factory for the connector. For the SQL connector, enter **`eis/LDAPv3`**.

   r Click **OK**.

   s Click the **Save** link.

   t On the Save to Master Configuraton dialog, click the **Save** button.

   u Restart WebSphere.

5 Modify the mapping file, if necessary. See Understanding the Mapping File on page 11 for details.

After installing the connector, refer to Configuring the Connector on page 17 to register and configure this connector in Select Identity.

2

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>
```

- **<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).
  - Concero:tafield — the name of the Select Identity resource attribute.
  - Concero: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>
```

- **<concero:entitlementMappingDefinition>**

  Defines how entitlements are mapped to users.

- **<concero:objectStatus>**

  Defines how to assign status to a user.

- **<concero: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. .

Select Identity Resource Attribute	CA eTrust LDAP Attribute	Description
UserName	cn	Key field on the resource
Password	userpassword	
First Name	givenname	

Select Identity Resource Attribute	CA eTrust LDAP Attribute	Description
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

3

Configuring the Connector

After you deploy the connector on the application server, you must configure Select Identity to use the connector by deploying it in the Select Identity client. The following provides an overview of the procedures you must complete in order to deploy your connector. It also provides connector-specific information you must provide when configuring Select Identity to use the connector.

1. Before deploying the connector in Select Identity, connect to LDAP using an LDAP browser or another utility. This will help ensure that the LDAP resource is available and the correct parameters are known before deploying the resource in Select Identity.
2. Register the connector with Select Identity by clicking the **Deploy New Connector** button on the Connectors home page. Complete this procedure as described in the "Connectors" chapter of the *HP OpenView Select Identity Administrator Guide*.

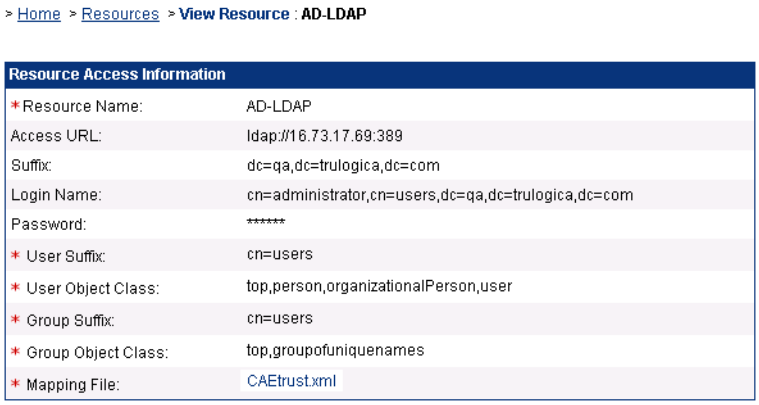
   After you deploy the connector, the connector properties will look similar to this:

3 Deploy a resource that uses the newly created connector. On the Resources home page, click the **Deploy New Resource** button. When configuring the resource, refer to the following table for parameters specific to this connector:

Field Name	Sample Values	Description
Resource Name	ETrust	Name of the target resource.
Resource Type	ETrust LDAP	The connector that was deployed in Step 2 on page 17.
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 the eTrust LDAP connector, select this option.
Access URL	ldap://136.168.1.20:389	URL access to the resource.
Suffix	c=AU	The domain(s) to which the users will be provisioned.
Login Name	admin	Login account with administrative privileges to add and delete users. This is required to log in to the resource.
Password	Password123	Password corresponding to the login account.
User Suffix	ou=ADMINISTRATION, ou=CORPORATE, ou=DEMOCORP	Suffix part of user's distinguished name. This is the location in the tree where the users will be provisioned.

Field Name	Sample Values	Description
User Object Class	inetorgperson	Object class of users.
Group Suffix	ou=ADMINISTRATION, ou=CORPORATE, ou=DEMOCORP	Suffix part of group's distinguished name. This is the location in the tree where the user groups will be provisioned.
Group Object Class	OrganizationalUnit	Object class of user groups.
Mapping File	CAEtrust.xml	Location of the connector mapping file, which is used to map resource attributes to Select Identity attributes.

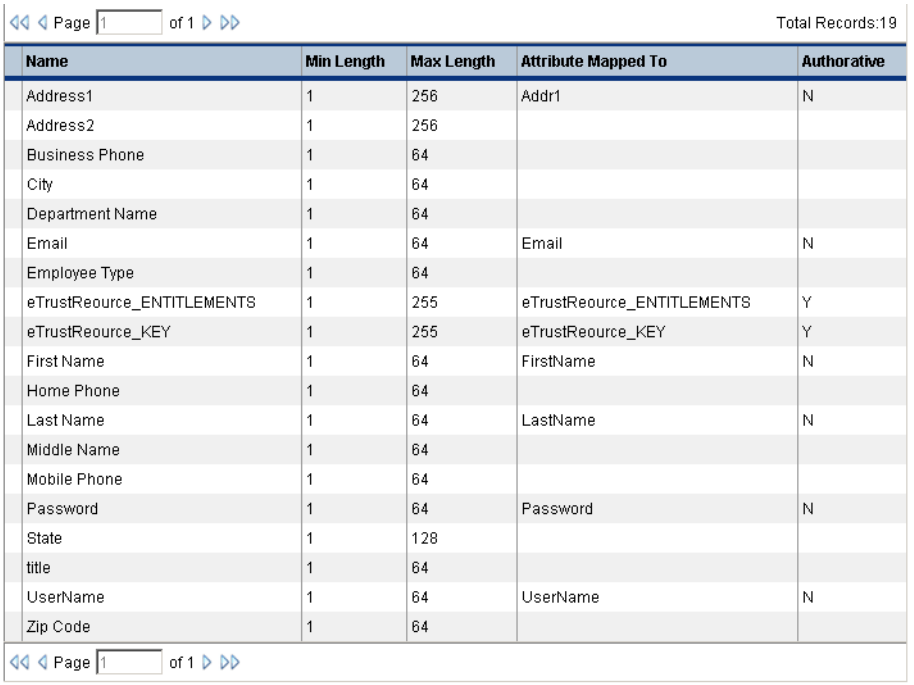
Complete the steps in this procedure as described in the "Resources" chapter of the *HP OpenView Select Identity Administrator Guide*. After you deploy the resource for the eTrust LDAP connector, the Access Info page of the resource properties will look similar to this:



4 Create attributes that link Select Identity to the connector. For each mapping in the connector's mapping file, create an attribute using the Attributes capability on the Select Identity client.

Refer to the "Attributes" chapter in the *HP OpenView Select Identity Administrator Guide* for more information. After you create the attributes

for the eTrust LDAP connector, the View Attributes page for the resource will look similar to this:



Page 1 of 1 Total Records:19

Name	Min Length	Max Length	Attribute Mapped To	Authorative
Address1	1	256	Addr1	N
Address2	1	256		
Business Phone	1	64		
City	1	64		
Department Name	1	64		
Email	1	64	Email	N
Employee Type	1	64		
eTrustReource_ENTITLEMENTS	1	255	eTrustReource_ENTITLEMENTS	Y
eTrustReource_KEY	1	255	eTrustReource_KEY	Y
First Name	1	64	FirstName	N
Home Phone	1	64		
Last Name	1	64	LastName	N
Middle Name	1	64		
Mobile Phone	1	64		
Password	1	64	Password	N
State	1	128		
title	1	64		
UserName	1	64	UserName	N
Zip Code	1	64		

Page 1 of 1

5 Create a Service that will use the newly created resource. To do so, click the **Deploy New Service** button on the Services home page. Complete this procedure as described in "Services" of the *HP OpenView Select Identity Administrator Guide*. You will reference your new resource created in Step 3 while creating this service.

4

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.

On WebLogic

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**.

On WebSphere

Complete the following steps to uninstall the connector on WebSphere:

1. Log on to the WebSphere Application Server Console.
2. Navigate to **Resources** → **Resource Adapters**.
3. Select the connector to uninstall.
4. Click **Delete**.
5. Click the **Save** link (at the top of the page).
6. On the Save to Master Configuraton dialog, click the **Save** button.