

HP OpenView Select Identity

Web Service Developer 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). 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	Introduction	7
	Operations Supported by the Web Service	8
	Issuing Requests	9
	Elements Implemented by the Web Service	9
	Product Documentation	10
Chapter 2	SPML Examples	12
	Adding a User	12
	Modifying a User	14
	Deleting a User	15
	Retrieving a User Profile	15
	Enabling a User	16
	Changing a User's Password	17
	Terminating a User	18

Introduction

HP OpenView Select Identity provides the ability to provision users in repositories. Provisioning is defined as the "automation of all steps required to manage (setup, amend, and revoke) user or system access entitlements or data relative to electronically published services." Select Identity enables you to programatically provision users in Select Identity through the Web Service.

Consider the following example:

Company X's Human Resources department relies on an enterprise resource planning (ERP) application to manage employees. When a new employee is hired, the HR department adds the employee to the system. However, the new hire will need email and network accounts and access to the systems on which he will fulfill his job responsibilities. The Select Identity Web Service enables you to automate the ERP application to send a request to provision the user. Then, Select Identity can create the necessary accounts and access privileges on Company X's systems according to the services defined for the user.

Operations Supported by the Web Service

Specifically, the Web Service enables you to perform the following operations:

- **User provisioning**

Most of the user operations provided by the Users home page of the Select Identity client can be performed using the Select Identity Web Service. These operations are initiated from an external source and the changes are made in Select Identity. Here is a list of supported operations:

 - Add a user
 - Enable a user
 - Modify user attributes and entitlements
 - Delete a user
 - Retrieve a user profile
 - Enable or disable service membership
 - Reset or changes a user's password
 - Terminate a user
- **Password synchronization**

Using the Web Service, you can change a user's password on a resource then synchronize with Select Identity to change the password stored in the Select Identity repository. This is called reverse synchronization. This enables a resource to push user information to Select Identity. The agent (provided by a two-way connector) on the resource tracks changes made on the resource and synchronizes with Select Identity.

Rules identify the services that are affected when a reverse synchronization operation is issued based on the resource ID sent by the resource. Rules also specify the location of the reverse mapping that should be performed for add and modify operations, such as NT Domain Resource -> ntuser.properties. Thus, reverse synchronization can be performed only for those services with specified rules a mapping for the incoming resource ID. If rules or the mapping does not exist, the request is logged and ignored.

Issuing Requests

External systems can send Simple Object Access Protocol (SOAP) messages to Select Identity for user provisioning, to which the Web Service will send a response. Then, Select Identity can push the users to the appropriate resources as defined by the services assigned to the users.

Select Identity has implemented the Web Service according to the OASIS SPML specification, which defines the concepts, operations, and XML schema for an XML-based provisioning request and response protocol. Refer to the specification for details about all standard elements and attributes.

To issue requests to Select Identity in order to provision users and synchronize data, the external system must send a SOAP message containing a Service Provisioning Markup Language (SPML) request. The request must be sent to the following URL:

`http://select_identity_host:port/lmz/webservice/`

Refer to the online help on the Select Identity CD (in the `docs/api_help/web_service/help` directory) for a client example that issues a request and handles responses.

Elements Implemented by the Web Service

The following elements are implemented and, where possible, extended by Select Identity:

- **`<addRequest>`**
- **`<deleteRequest>`**
- **`<extendedRequest>`**
- **`<modifyRequest>`**
- **`<searchRequest>`**

Refer to the online help provided on the Select Identity CD (in the `docs/api_help/web_service/help` directory) for detailed information about each of these elements. Also, sample XML files are provided to illustrate how to use these elements; refer to the `SampleXML/Web Service` directory on the CD.

Product Documentation

The Select Identity product documentation includes the following:

- Release notes are provided in the top-level directory of the HP OpenView Select Identity CD. This document provides important information about new features included in this release, known defects and limitations, and special usage information that you should be familiar with before using the product.
- For installation and configuration information, refer to the *HP OpenView Select Identity Installation Guide*. All installation prerequisites, system requirements, and procedures are explained in detail in this guide. Specific product configuration and logging settings are included. This guide also includes uninstall and troubleshooting information.
- An *HP OpenView Connector Installation Guide* is provided for each resource connector. These are located on the Select Identity Connector CD.
- Detailed procedures for deployment and system management are documented in the *HP OpenView Select Identity Administrator Guide* and Select Identity online help system. This guide provides detailed concepts and procedures for deploying and configuring the Select Identity system. In the online help system, tasks are grouped by the administrative functions that govern them.
- The *HP OpenView Select Identity Workflow Studio Guide* provides detailed information about using Workflow Studio to create workflow templates. It also describes how to create reports that enable managers and approvers to check the status of account activities.
- The *HP OpenView Select Identity External Call Developer Guide* provides detailed information about creating calls to third-party applications. These calls can then be deployed in Select Identity to constrain attribute values or facilitate workflow processes. In addition, JavaDoc is provided for this API. To view this help, extract the `javadoc.jar` file in the `docs/api_help/external_calls/Javadoc` directory on the HP OpenView Select Identity CD.
- If you need to develop connectors, which enable you to connect to external systems for provisioning, refer to the *HP OpenView Select Identity Connector Developer Guide*. This document provides an overview of the Connector API and the steps required to build a connector. The audience of this guide is developers familiar with Java.

JavaDoc is also provided for the Connector API. To view this help, extract the `javadoc.jar` file in the `docs/api_help/connectors/Javadoc` directory on the HP OpenView Select Identity CD.

- The *HP OpenView Select Identity Web Service Developer Guide* describes the Web Service, which enables you to programmatically provision users in Select Identity. This guide provides an overview of the operations you can perform through use of the Web Service, including SPML examples for each operation.

An independent, web-based help system is available for this API. To view this help, double-click the `index.htm` file in the `docs/api_help/web_service/help` directory on the HP OpenView Select Identity CD.

SPML Examples

This chapter provides examples of SPML you must send when issuing requests. For more examples and a complete description of the elements and their attributes, refer to the online help on the Select Identity CD, in the docs/api_help/web_service/help directory. Also, sample XML files are provided to illustrate how to use these elements; refer to the SampleXML/Web Service directory on the CD.

Adding a User

The following is an example of the **<addRequest>** element. The **<operationalAttributes>** element provides login credentials for the admin administrator, and the service for which the user is added is the Firewall Service. The **<attributes>** element specifies information about the user. These attributes are service-specific.

```
<soap:Envelope xmlns:soap='http://schemas.xmlsoap.org/soap/envelope/'>
<soap:Body>
<addRequest requestID='12345'
  execution='urn:oasis:names:tc:SPML:1:0#asynchronous'>
  <operationalAttributes>
    <attr name='urn:trulogica:concerro:2.0#serviceName'>
      <value>Firewall Service</value>
    </attr>
```

```
<attr name='urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName'>
  <value>admin</value>
</attr>
<attr name='urn:trulogica:concerro:2.0#password'>
  <value>abc123</value>
</attr>
</operationalAttributes>
<attributes>
  <attr name='First Name'>
    <value>John</value>
  </attr>
  <attr name='Last Name'>
    <value>Doe</value>
  </attr>
  <attr name='Salutation'>
    <value>Mr.</value>
  </attr>
  <attr name='User Name'>
    <value>jdoe</value>
  </attr>
  <attr name='Business Phone'>
    <value>972-801-1234</value>
  </attr>
  <attr name='Domain'>
    <value>1</value>
  </attr>
  <attr name='Mail Host'>
    <value>Yahoo.com</value>
  </attr>
  <attr name='Email'>
    <value>jdoe@yahoo.com</value>
  </attr>
  <attr name='DomainKey'>
    <value>Firm ID</value>
  </attr>
</attributes>
</addRequest>
</soap:Body>
</soap:Envelope>
```

Modifying a User

The following is an example of the **<modifyRequest>** element. The **<operationalAttributes>** element provides login credentials for the admin administrator, for the Firewall Service. The **<identifier>** element provides the user ID of the user to modify. The **<attributes>** element specifies information to be modified for the user.

```
<soap:Envelope xmlns:soap='http://schemas.xmlsoap.org/soap/envelope/'>
<soap:Body>
<modifyRequest requestID='12345'
  execution='urn:oasis:names:tc:SPML:1:0#asynchronous'>
  <operationalAttributes>
    <attr name='urn:trulogica:concero:2.0#serviceName'>
      <value>Firewall Service</value>
    </attr>
    <attr name='urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName'>
      <value>admin</value>
    </attr>
    <attr name='urn:trulogica:concero:2.0#password'>
      <value>abc123</value>
    </attr>
  </operationalAttributes>
  <identifier
identifierType='urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName'>
    <id>jdoe</id>
  </identifier>
  <modifications>
    <modification name='Title' operation='replace'>
      <value>Manager</value>
    </modification>
    <modification name='Business Phone' operation='replace'>
      <value>972-801-2222</value>
    </modification>
  </modifications>
</modifyRequest>
</soap:Body>
</soap:Envelope>
```

Deleting a User

The following is an example of the **<deleteRequest>** element. The **<operationalAttributes>** element provides login credentials for the admin administrator, for the Firewall Service. The **<identifier>** element provides the user ID of the user to delete.

```
<soap:Envelope xmlns:soap='http://schemas.xmlsoap.org/soap/envelope/'>
<soap:Body>
<deleteRequest requestID='12345'
  execution='urn:oasis:names:tc:SPML:1:0#asynchronous'>
  <operationalAttributes>
    <attr name='urn:trulogica:concerro:2.0#serviceName'>
      <value>Firewall Service</value>
    </attr>
    <attr name='urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName'>
      <value>dave_usa</value>
    </attr>
    <attr name='urn:trulogica:concerro:2.0#password'>
      <value>trul0g1ca</value>
    </attr>
  </operationalAttributes>
  <identifier
  identifierType='urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName'>
    <id>jdoe</id>
  </identifier>
</deleteRequest>
</soap:Body>
</soap:Envelope>
```

Retrieving a User Profile

The following is an example of the **<searchRequest>** element. It searches for the user identified by the sk061001 ID for the iPlanet resource.

```
<soap:Envelope xmlns:soap='http://schemas.xmlsoap.org/soap/envelope/'>
<soap:Body>
<searchRequest requestID='12345'
  execution='urn:oasis:names:tc:SPML:1:0#synchronous'>
  <operationalAttributes>
    <attr name='urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName'>
      <value>concerrosa</value>
    </attr>
    <attr name='urn:trulogica:concerro:2.0#password'>
```

```

        <value>abc123</value>
      </attr>
    </operationalAttributes>
    <searchBase type='urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName'>
      <id>sk061001</id>
    </searchBase>
    <filter>
      <equalityMatch name='urn:trulogica:conceroc:2.0#resourceId'>
        <value>local-iPlanet</value>
      </equalityMatch>
    </filter>
  </searchRequest>
</soap:Body>
</soap:Envelope>

```

Enabling a User

The following is an example of the **<extendedRequest>** attribute, to enable a user's account.

```

<soap:Envelope xmlns:soap='http://schemas.xmlsoap.org/soap/envelope/'>
<soap:Body>
<extendedRequest requestID='1769'
execution='urn:oasis:names:tc:SPML:1:0#asynchronous'>
  <operationalAttributes>
    <attr name='urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName'>
      <value>concerosa</value>
    </attr>
    <attr name='urn:trulogica:conceroc:2.0#password'>
      <value>abc123</value>
    </attr>
  </operationalAttributes>
  <identifier type='urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName'>
    <id>sk061001</id>
  </identifier>
  <providerIdentifier providerIDType='urn:oasis:names:tc:SPML:1:0#URN'>
    <providerID>urn:trulogica:conceroc:2.0</providerID>
  </providerIdentifier>
  <operationIdentifier operationIDType='urn:oasis:names:tc:SPML:1:0#URN'>
    <operationID>urn:trulogica:conceroc:2.0#enable</operationID>
  </operationIdentifier>
  <attributes/>
</extendedRequest>
</soap:Body>
</soap:Envelope>

```


Changing a User's Password

The following is an example of the **<extendedRequest>** attribute, to change a user's password.

```
<soap:Envelope xmlns:soap='http://schemas.xmlsoap.org/soap/envelope/'>
<soap:Body>
<extendedRequest requestID='1769'
execution='urn:oasis:names:tc:SPML:1:0#asynchronous'>
  <operationalAttributes>
    <attr name='urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName'>
      <value>concerosa</value>
    </attr>
    <attr name='urn:trologica:concerero:2.0#password'>
      <value>abc123</value>
    </attr>
  </operationalAttributes>
  <identifier type='urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName'>
    <id>sk061001</id>
  </identifier>
  <providerIdentifier providerIDType='urn:oasis:names:tc:SPML:1:0#URN'>
    <providerID>urn:trologica:concerero:2.0</providerID>
  </providerIdentifier>
  <operationIdentifier operationIDType='urn:oasis:names:tc:SPML:1:0#URN'>
    <operationID>urn:trologica:concerero:2.0#changePassword</operationID>
  </operationIdentifier>
  <attributes>
    <attr name='urn:trologica:concerero:2.0#resourceId'>
      <value>local-iPlanet</value>
    </attr>
    <attr name='urn:trologica:concerero:2.0#newPassword'>
      <value>zzzz1234</value>
    </attr>
  </attributes>
</extendedRequest>
</soap:Body>
</soap:Envelope>
```

Terminating a User

The following is an example of the **<extendedRequest>** attribute, to terminate a user.

```
<soap:Envelope xmlns:soap='http://schemas.xmlsoap.org/soap/envelope/'>
<soap:Body>
<extendedRequest requestID='1769'
execution='urn:oasis:names:tc:SPML:1:0#asynchronous'>
  <operationalAttributes>
    <attr name='urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName'>
      <value>concerosa</value>
    </attr>
    <attr name='urn:trologica:concerro:2.0#password'>
      <value>abc123</value>
    </attr>
  </operationalAttributes>
  <identifier type='urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName'>
    <id>sk061001</id>
  </identifier>
  <providerIdentifier providerIDType='urn:oasis:names:tc:SPML:1:0#URN'>
    <providerID>urn:trologica:concerro:2.0</providerID>
  </providerIdentifier>
  <operationIdentifier operationIDType='urn:oasis:names:tc:SPML:1:0#URN'>
    <operationID>urn:trologica:concerro:2.0#terminate</operationID>
  </operationIdentifier>
</extendedRequest>
</soap:Body>
</soap:Envelope>
```