

HP OpenView Select Identity

**Connector for
HP OpenVMS VAX and Alpha,
Versions 6.2, 7.2, 7.3, and 7.3-2**

Installation and Configuration Guide

**Connector Version: 1.4
Select Identity Version: 3.3.1**



August 2005

© 2005 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

© 2005 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.
- BouncyCastle engine for keystore management, bouncycastle.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.

UNIX is a registered trademark of The Open Group.

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://passport2.hp.com/hpp/newuser.do>

contents

Chapter 1	Installing the Connector	7
	System Requirements.	8
	Deploying on the Web Application Server.	9
	Installing Expect and the Connector Scripts	10
Chapter 2	Configuring the Connector	14
Chapter 3	Understanding the Mapping File	19
	General Information.	20
	VMS Mapping Information	23
Chapter 4	Uninstalling the Connector	34
Appendix A	Troubleshooting	35
Appendix B	Understanding the Installed Scripts	37

Installing the Connector

The HP OpenVMS VAX and Alpha connector — hereafter referred to as the VMS connector — enables HP OpenView Select Identity to perform the following tasks in OpenVMS systems on VAX and Alpha platforms:

- 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 VMS connector is a one-way connector and pushes changes made to user data in the Select Identity database to a target OpenVMS system. The mapping file controls how Select Identity attributes are mapped to VMS attributes.

The VMS connector is packaged in the following files:

- `VmsConnector.rar` — Contains the binaries
- `vmsschema.jar` — Contains the mapping file
- `vms-expect-scripts.zip` — Contains a set of scripts that perform user provisioning operations on VMS v7.2, 7.3, and 7.3-2 for the connector on Windows
- `vms-expect-scripts.tar.gz` — Contains the scripts that perform user provisioning operations on VMS v7.2, 7.3, and 7.3-2 for the connector on UNIX
- `vms62-expect-scripts.zip` — Contains a set of scripts that perform user provisioning operations on VMS v6.2 for the connector on Windows
- `vms62-expect-scripts.tar.gz` — Contains the scripts that perform user provisioning operations on VMS v6.2 for the connector on UNIX

These files are located in the `VAX-VMS` directory on the Select Identity Connector CD.

System Requirements

The VMS connector is supported in the following environment:

Select Identity Version	Application Server	Database	VMS Version
3.0.2	WebLogic 8.1.2 on Windows 2003	SQL Server 2000	VAX 7.2, VAX 7.3, Alpha 7.3-2
	WebLogic 8.1.2 on Solaris 9	Oracle 9i	VAX 6.2

Select Identity Version	Application Server	Database	VMS Version
3.3	WebLogic 8.1.4 on Windows 2003	SQL Server 2000	VAX 7.2, VAX 7.3, Alpha 7.3-2
	WebLogic 8.1.4 on Solaris 9	Oracle 9i	VAX 6.2
3.3.1	WebLogic 8.1.4 on Windows 2003	SQL Server 2000	VAX 7.2, VAX 7.3, Alpha 7.3-2
	WebLogic 8.1.4 on Solaris 9	Oracle 9i	VAX 6.2

Deploying on the Web Application Server

To install the VMS connector on the Select Identity server, complete the steps in this section.

- 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 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.)
- 3 Copy the `VmsConnector.rar` file from the Select Identity Connector CD to the connector subdirectory.
- 4 Extract the contents of the `vmsschema.jar` file (on the Select Identity Connector CD) to the schema subdirectory.
- 5 Ensure that the CLASSPATH environment variable in the WebLogic server startup script references the schema subdirectory.
- 6 Modify the mapping files, if necessary. See [Understanding the Mapping File on page 19](#) 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 `VmsConnector.rar` file from the list. It is stored in the connector subdirectory.
- 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, see [Configuring the Connector on page 14](#) about registering and configuring the connector in Select Identity.

Installing Expect and the Connector Scripts

The VMS connector provides a set of scripts that perform user provisioning operations for the connector. They are run using a tool called Expect. Install Expect and the scripts on the system where the application server and Select Identity server are installed by completing the following steps:

- 1 Install Expect and Telnet, if they were not previously installed, as follows:

On UNIX

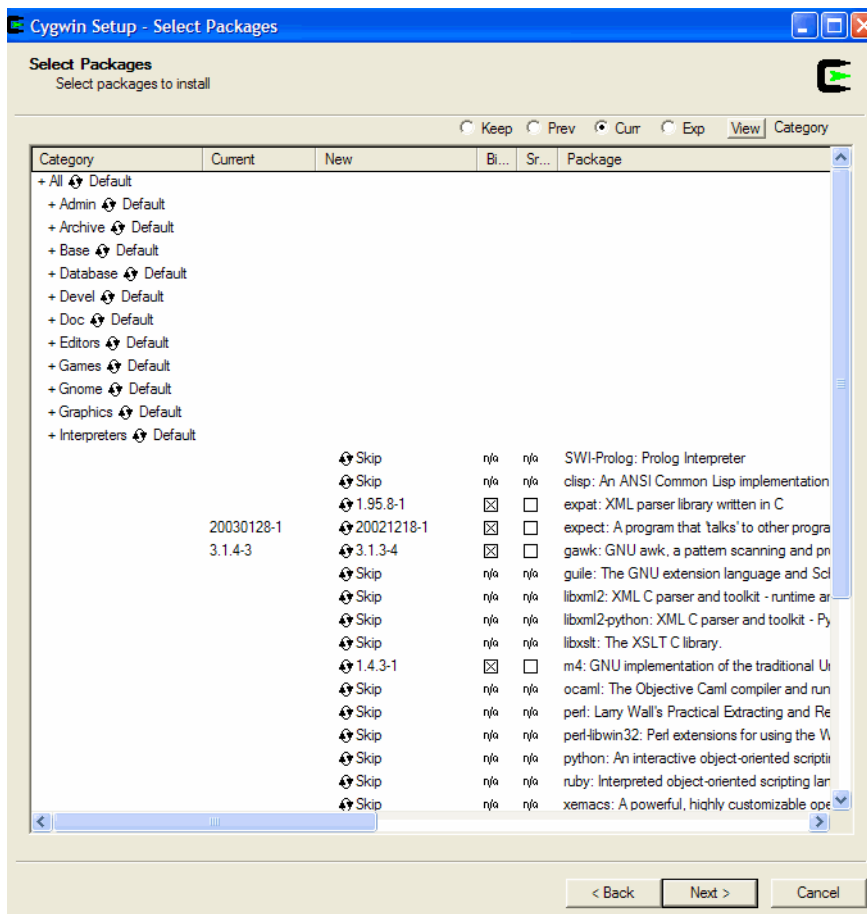
Download Expect from <http://expect.nist.gov/> and install it on the UNIX server. When deploying the VMS system as a resource in Select Identity, provide the location of the Expect executable on the Access Info page. TCL/TK and GCC are prerequisites for running Expect.

Telnet is provided by the operating system.

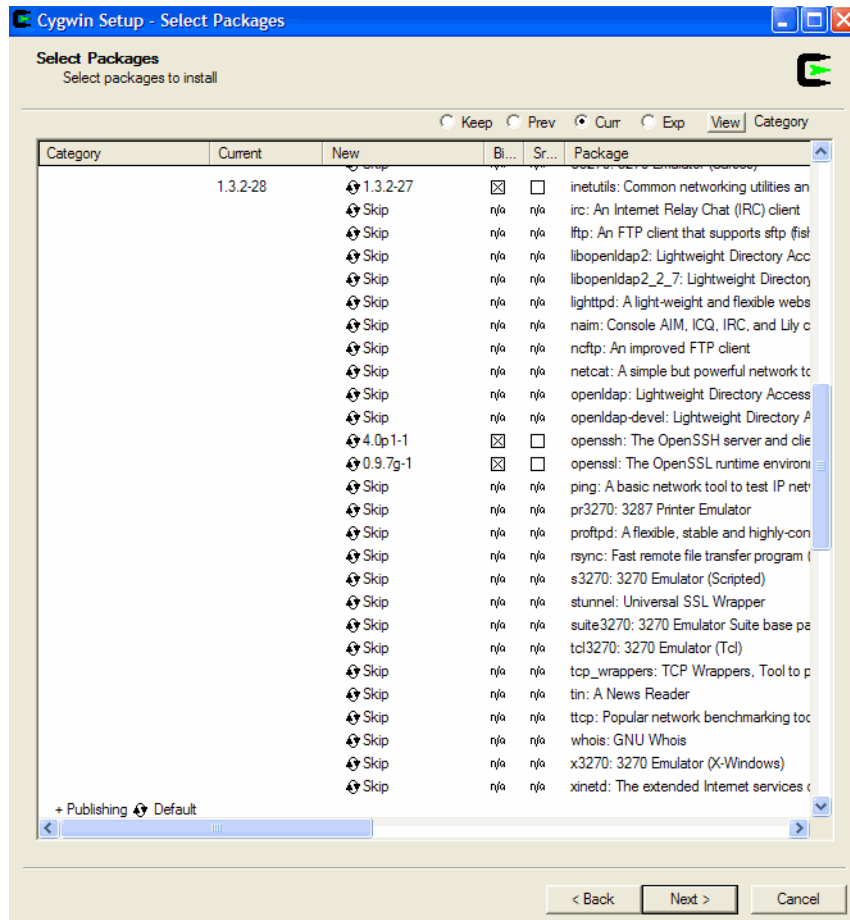
On Windows

Download the Cygwin setup wizard from <http://www.cygwin.com/setup.exe>. Be sure to install Expect (version 5.26) and the the inetutils

package. Expect is listed in the Interpreters category in Cygwin's installer:



The inetutils package are listed in the Net category, as shown in this snapshot:



2 Install the scripts, as follows:

On UNIX and VMS 6.2

Create a directory called `vms` in the Select Identity home directory; when deploying the OpenVMS resource, you will provide the location of this directory. Then, extract the `vms62-expect-scripts.tar.gz` file using these commands:

```
gzip -d vms62-expect-scripts.tar.gz
tar xvf vms62-expect-scripts.tar
```

On UNIX and VMS 7.2, 7.3, and 7.3-2

Create a directory called `vms` in the Select Identity home directory; when deploying the OpenVMS resource, you will provide the location of this directory. Then, extract the `vms-expect-scripts.tar.gz` file using these commands:

```
gzip -d vms-expect-scripts.tar.gz  
tar xvf vms-expect-scripts.tar
```

On Windows

Extract the `vms-expect-scripts.zip` or `vms62-expect-scripts.zip` file from the Select Identity Connector CD to a local directory on the application server, such as `C:\Select_Identity\vms`. When deploying the OpenVMS resource, you will provide the location of this directory.

3 *On Windows*

Ensure that Cygwin's `bin` directory is included in the Windows server `PATH` environment variable.

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 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:

[Home](#) > [Connectors](#) > **View Connector : VmsConnector**

Connector Information	
* Connector Name:	VmsConnector
* Pool Name:	eis/VmsConnector

- 2 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 Value	Description
Resource Name	VmsResource	Name of the resource.
Host Name	16.138.247.179	Host name or IP address of VMS machine.
User Name	system	VMS admin user account name.
User Password	admin123	VMS admin user password.
Executable	C:/cygwin/bin/expect.exe	Expect script executable file, which is required to run scripts.
Script Location	<i>On UNIX:</i> /connectorScripts/expect/vms <i>On Windows:</i> /cygdrive/c/vms/scripts/	Location of Expect scripts that are used by the connector. Note that on Windows, you should include a trailing slash in the path."c" is name of the drive.
Mapping File	VmsConnector.xml	The attribute mapping XML file.

Complete the steps in this procedure as described in the “Resources” chapter of the *HP OpenView Select Identity Administrator Guide*.



Make sure that the specified user has the SYSPRV privilege on the VMS system.

After you deploy the resource for the connector, the Basic Info page of the resource properties will look similar to this:

Resource Information	
* Resource Name:	Vms62Res
Resource Description:	<input type="text"/>
* Resource Type:	VmsConnector
* Authoritative Source:	Yes
* Delete User:	Yes
Reconciliation Workflow:	
Resource Owner:	
* Resource Id:	1105

The Additional Info page will look similar to this:

Resource Information	
Resource Name:	Vms62Res
<input checked="" type="checkbox"/> Manage User	
Associate to Group:	<input checked="" type="checkbox"/>

The Access Info page will look similar to this:

Resource Access Information	
* Resource Name:	Vms62Res
* Host Name:	16.32.32.67
* User Name:	SYSTEM
* User Password:	*****
* Executable:	C:/cygwin/bin/expect.exe
* Script Location:	/cygdrive/d/projects/si/devarea/VaxVms/scripts/vms/
* Mapping File:	VmsConnector.xml

- 3 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 connector, the View Attributes page for the resource will look similar to this:

(Resource Name=Vms62Res)				
<< < Page <input type="text" value="1"/> of 1 > >>				Total Records: 43
Name	Min Length	Max Length	Attribute Mapped To	Authoritative
Access	0	400		
Account	0	8		
Add_Identifier	0	8		
AST Queue Limit	0	10		
Batch	0	12		
Buffered IO Byte Limit	0	10		
Buffered IO Count Limit	0	10		
Command Language Interpreter	0	31		
Command Language Interpreter Tables	0	31		
Device	0	31		
Dialup	0	12		
Direct IO Count Limit	0	10		
Directory	0	39	Directory	N
Gid	0	31	Groupid	N
Initial Byte Quota	0	10		
Local	0	12		
Lock Queue Limit	0	10		

Login Command File	0	31		
Maximum Active jobs or process	0	10		
Maximum Detached jobs	0	10		
Maximum jobs	0	10		
Maximum Shared Files	0	10		
Network	0	12		
Open File Limit	0	10		
Owner	0	31	FirstName	N
Paging File Limit	0	10		
Password	0	32	Password	N
Password Life Time	0	4		
Password Minimum	0	4		
Primary Days	0	100		
Priority	0	2		
Privileges	0	39		
Remote	0	12		
Secondary Password	0	23		
Subprocess Creation Limit	0	10		
Total entries in Timer Queue	0	10		
Uid	0	31		
User Name	0	12	UserName	N
Vms62Res_ENTITLEMENTS	1	255	Vms62Res_ENTITLEMENTS	Y
Vms62Res_KEY	1	255	Vms62Res_KEY	Y
WSDEFAULT	0	10		
WSEXTENT	0	10		
WSQUOTA	0	10		

- 4 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 2](#) while creating this service.

Understanding the Mapping File

The VMS connector is deployed with the `VmsConnector.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 `vmsschema.jar`. The mapping file is used to map user account additions and modifications from Select Identity to the OpenVMS 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 “user” can have a different name on different resources, such as “ACCOUNT” for OpenVMS, “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 file:

- **<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 OpenVMS.

- **<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
- bypass — the operation is not supported by the connector

Here is an example:

```
<objectClassDefinition name="User" description="Vms 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— whether this attribute is required in the provisioning (set to true or false).
- Concero:tafield — the name of the Select Identity resource attribute. In general, the attribute assigned to tafield should be the same as the physical resource attribute, or at least the connector attribute. For example, it is recommended to have the following:

```
<attributeDefinitionReference name="FirstName"
  required="false" concero:tafield="[givenname]"
  concero:resfield="givenname" concero:init="true"
  concero:isMulti="true"/>
```

instead of this:

```
<attributeDefinitionReference name="FirstName"
required="false" concero:tafield="[FirstName]"
concero:resfield="givenname" concero:init="true"
concero:isMulti="true"/>
```

- **Concero:resfield** — the name of the physical resource attribute from the resource schema. If the resource does not support an explicit schema, this can be a tag field that indicates a resource attribute mapping.

Also, the attribute name may be case-sensitive; for example, if the attribute is defined in all uppercase letters on the resource, be sure to specify it in all uppercase letters here.

- **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.

Note that for a key field mapping where `isKey="true"` and `tafield` is not assigned the `UserName` attribute, `UserName` should not be used in any other mapping. That is, `UserName` can be assigned to `tafield` only in cases where it is mapped to the key field in the resource. Example:

```
<attributeDefinitionReference name="UserName"
required="true" concero:tafield="[UserName]"
concero:resfield="uid" concero:isKey="true"
concero:init="true"/>
```

- **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="Vms-UName"
    required="true" concero:tafield="User Name"
    concero:resfield="username" concero:init="true" />
  ...
</memberAttributes>
```

- **<attributeDefinition>**

Defines the properties of each object's attribute. For example, the attribute definition for the Directory attribute defines that it must be between one and 50 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 `VmsConnector.xml` file:

```
<attributeDefinition name="GroupName" description="GroupName"
  type="xsd:string">
  <properties>
    <attr name="minLength">
      <value>1</value>
    </attr>
    <attr name="maxLength">
      <value>8</value>
    </attr>
    <attr name="pattern">
      <value>
        <![CDATA[ [a-zA-Z0-9@+ ] ]>
      </value>
    </attr>
  </properties>
</attributeDefinition>
```

- **<concerno:entitlementMappingDefinition>**

Defines how entitlements are mapped to users.

- **<concerno:objectStatus>**

Defines how to assign status to a user.

- **<concerno:relationshipDefinition>**

Defines how to create relationships between users.

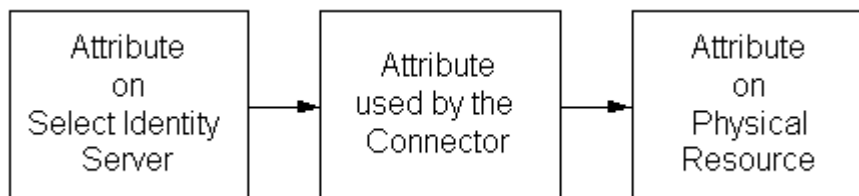
VMS Mapping Information

The following is a description of the columns provided in the tables below:

- **Select Identity Resource Attribute** — The name of the attribute on the Select Identity server.
- **Connector Attribute**— The attribute used by the VMS connector.

- **Actual Attribute on OpenVMS System** — The name of the attribute on the OpenVMS system, to which the Select Identity and logical resource attributes are mapped. These attributes cannot be changed.
- **Description** — A description of the attribute and any noteworthy information needed when assigning values to the attribute.

Here is an illustration of how the attributes are related:



The following table describes the mappings in the `VmsConnector.xml` 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 OpenVMS system. These attributes cannot be changed.

Also, some connector attributes must be mapped in a different way than normal attributes to leverage advanced Select Identity functionality. See the Description column for more information.

Select Identity Resource Attribute	Attribute on Connector	Attribute on OpenVMS Resource	Description
Account	account	ACCOUNT	Default name for the user account.
Password	password	PASSWORD	The user's first password. Specify an alphanumeric string, which can include dollar signs (\$) and underscores (_), with up to 32 characters.

Select Identity Resource Attribute	Attribute on Connector	Attribute on OpenVMS Resource	Description
Secondary Password	password2		The user's secondary password, which is optional. Specify an alphanumeric string, which can include dollar signs (\$) and underscores (_), with up to 32 characters.
Access	access	ACCESS	The time range in which the user can access the system on primary and secondary days (see Primedays). Specify a range of hours (0-23, 0-23).
AST Queue Limit	astlm	ASTLM	The AST queue limit, which is the total number of asynchronous system trap (AST) operations and scheduled wake-up requests that the user can queue at one time.
Batch	batch	BATCH	The hours of access to run batch jobs. By default, a user can submit batch jobs any time. Specify a range of hours (0-23,0-23).

Select Identity Resource Attribute	Attribute on Connector	Attribute on OpenVMS Resource	Description
Buffered IO Count Limit	biolm	BIOLM	A buffered I/O count limit for the BIOLM field of the UAF record. This limit is the maximum number of outstanding buffered I/O operations, such as terminal I/O.
Buffered IO Byte Limit	bytlm	BYTLM	The buffered I/O byte limit for the BYTLM field of the UAF record. This limit is the maximum number of bytes of non-paged system dynamic memory that a user's job can consume at one time. Non-paged dynamic memory is used for operations such as I/O buffering, mailboxes, and file-access windows.
Command Language Interpreter	Cli	CLI	The name of the default command language interpreter (CLI) for the CLI field of the UAF record. The CLI name is a string of 1-31 alphanumeric characters and should be either DCL or MCR. The default is DCL. This setting is ignored for network jobs.

Select Identity Resource Attribute	Attribute on Connector	Attribute on OpenVMS Resource	Description
Command Language Interpreter Tables	clitables	CLITABLES	User-defined CLI tables for the account. Specify 1-31 characters. The default is SYSS\$LIBRARY:DCLTABLES. This setting is ignored for network jobs to guarantee that the system-supplied command procedures used to implement network objects function properly.
Device	device	DEVICE	The name of the user's default device at login. This is an alphanumeric string containing 1-31 characters.
Dialup	dialup	DIALUP	The hours of access to dialup logins. The default is full access. Specify a range of hours (0-23,0-23).
Direct IO Count Limit	diolm	DIOLM	The direct I/O count limit for the DIOLM field of the UAF record. This is the maximum number of outstanding direct I/O operations (usually disk).
Directory	directory	DIRECTORY	The default directory during login.

Select Identity Resource Attribute	Attribute on Connector	Attribute on OpenVMS Resource	Description
Lock Queue Limit	enqlm	ENQLM	The lock queue limit for the ENQLM field of the UAF record. This is the maximum number of locks that are queued by the user at one time.
Open File Limit	fillm	FILLM	The open file limit for the FILLM field of the UAF record. This limit is the maximum number of files that can be open at one time, including active network logical links.
Initial Byte Quota	jtquota	JTQUOTA	The initial byte quota with which the job-wide logical name table is to be created.
Login Command File	lgicmd	LGICMD	The name of the default login command file.
Local	local	LOCAL	The hours of access for interactive logins from local terminals. By default, there are no restrictions on local logins. Specify a range of hours (0-23,0-23).

Select Identity Resource Attribute	Attribute on Connector	Attribute on OpenVMS Resource	Description
Maximum Active jobs or process	maxacctjobs	MAXACCTJOBS	The maximum number of batch, interactive, and detached processes that can be active at one time for all users of the same account. By default, a user has a maximum of 0, which represents an unlimited number.
Maximum Detached jobs	maxdetach	MAXDETACH	The maximum number of detached processes for the cited user name that can be active at one time.
Maximum jobs	maxjobs	MAXJOBS	The maximum number of processes (interactive, batch, detached, and network) for the cited user name that can be active simultaneously.
Network	network	NETWORK	The hours of access for network batch jobs. By default, network logins have no restrictions. Specify a range of hours (0-23,0-23).
Owner	Owner	OWNER	The name of the account owner. Specify an alphanumeric string containing 1-12 characters.

Select Identity Resource Attribute	Attribute on Connector	Attribute on OpenVMS Resource	Description
Paging File Limit	pgflquota	PGFLQUOTA	The paging file limit. This is the maximum number of pages that the person's process can use in the system paging file.
Subprocess Creation Limit	prclm	PRCLM	The subprocess creation limit. This is the maximum number of subprocesses that can exist at one time for the specified user's process.
Primary days	primedays	PRIMEDAYS	The primary and secondary days for logging in. By default, primary days are Monday - Friday, and secondary days are Saturday and Sunday.
Priority	priority	PRIORITY	The default base priority. The value is an integer from 0-31 for timesharing users.
Password Life Time	pwdlifetime	PWDLIFETIME	The number of days a password is valid.
Password Minimum length	pwdminimum	PWDMINIMUM	The minimum password length in characters. Specify a string 0-32 in length.

Select Identity Resource Attribute	Attribute on Connector	Attribute on OpenVMS Resource	Description
Remote	remote	REMOTE	The hours during which access is permitted for interactivelogins from network remote terminals (with the DCL command SET HOST). By default, remote logins have no access restrictions. Specify a range of hours (0-23,0-23).
Maximum Shared Files	shrfillm	SHRFILLM	Maximum number of shared files that the user can open at one time.
Total entries in Timer Queue	tqelm	TQELM	The total number of entries in the timer queue plus the number of temporary common event flag clusters that the user can have at one time. By default, a user can have 10.

Select Identity Resource Attribute	Attribute on Connector	Attribute on OpenVMS Resource	Description
Uid	uid		The user identification code (UIC). The UIC value is a group number from 1-37776 (octal) and a member number in the range of 0-177776 (octal), which are separated by a comma and enclosed in brackets. VMS reserves groups 1 and 300-377 for its use. Each user must have a unique UIC. By default, the UIC value is [200,200].
Wsdefault	wsdefault	WSDEFAULT	The default working set limit (the initial limit of physical pages the process can use).
Wsextent	wsextent	WSEXTENT	The working set maximum, which is the maximum amount of physical memory allowed to the process. The system provides memory to a process beyond its working set quota only when it has excess free pages. The additional memory is recalled by the system if needed.

Select Identity Resource Attribute	Attribute on Connector	Attribute on OpenVMS Resource	Description
Wsquota	wsquota	WSQUOTA	The working set quota, which is the maximum amount of physical memory a user process can lock into its working set. It also represents the maximum amount of swap space that the system reserves for this process and the maximum amount of physical memory that the system allows the process to consume if the system-wide memory demand is significant.
Gid	gid		The group ID. The default group on the resource is 200. Create this attribute as a context attribute in Select Identity.

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 Connectors home page on the Select Identity client.

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**.

After deleting the connector, you can remove the Expect scripts as well. Remove the scripts from the directory on the Select Identity server where they were extracted (see [Step 2 on page 12](#)).



Troubleshooting

The following information is provided to help you diagnose connectivity and configuration problems that you may encounter when using the connector to provision users on the resource. You may need to consult your system or web application administrator for detailed help.

- On the Select Identity server, if installed on a Windows system, ensure that Cygwin's `bin` directory is included in the Windows server's `PATH` environment variable.
- Verify that the path to Telnet is configured properly on the UNIX system. Use the UNIX command `which telnet` to find the path of Telnet. If the path is different than the path specified in the Expect scripts, use the path found on the UNIX system. You may want to specify the full path to Telnet in the scripts.
- Ensure that the Telnet daemon is configured and running on the target VMS system. Use `telnet <VMS_IP_address or Host_name>` to determine if it is running on the VMS system.
- Verify that Telnet allows for enough connections to handle provisioning requests. The number of connections depends on the number of connections allowed by the application server for the connector. To view

the connection configuration and connections on the application server, perform one of the following procedures:

To view the connection configuration on WebLogic:

- a** Log on to the WebLogic Server Console.
- b** Navigate to *My_domain* → **Services** → **JDBC** → **Connection Pools** → *connection_pool*.

To monitor current connections:

- c** Navigate to *My_domain* → **Deployments** → **Connector Modules** → **VmsConnector**.
- d** Click the **Monitoring** tab to view connections.

Understanding the Installed Scripts

The VMS connector performs operations using a tool called Expect. This tool must be installed on the application server running Select Identity.

The following scripts are provided during the connector installation. The syntax for each script is provided to enable you to run the scripts manually if need be.

- `vms_adduser.exp`

Adds a user on the OpenVMS system.

Syntax:

```
vms_adduser.exp username=<New user name> password=<New user password> owner=<Owner> directory=<Home Directory> primedays=<Primary days> device=<Name of the device> pwdlifetime=<Password life time> account=<Account Name> uid=<Member Id> gid=<Group Id> pwdminimum=<Minimum password length> prclm=<Subprocess Creation Limit> dialup=<Dial Up> wsquota=<working set quota> cli=<command language interpreter> maxdetach=<maximum number of detached processes> astlm=<AST queue limit> local=<Local access time> tqelm=<number of entries in timer queue> clitable=<CLI tables> priority=<Priority> network=<network access time> lgicmd=<Name of login command file> batch=<Access time for batch jobs> remote=<Remote access time> pgflquota=<Paging file limit>
```

```
biolm=<buffered I/O count limit> diolm=<Direct I/O count
limit> enqlm=<Lock queue limit> shrfillm=<Maximum number
of shared files> maxjobs=<Maximum number of processes>
fillm=<open file limit> maxacctjobs=<Maximum number of
batch> bytlim=<Buffered I/O byte limit> server=<IP
Address> login=<Admin User> password=<Admin Password>
```

- vms_modifyuser.exp

Modifies user details on the OpenVMS system.

Syntax:

```
vms_modifyuser.exp username=<User name> owner=<Owner>
directory=<Home Directory> primedays=<Primary days>
device=<Name of the device> pwdlifetime=<Password life
time> account=<Account Name> pwdminimum=<Minimum password
length> prclm=<Subprocess Creation Limit> dialup=<Dial
Up> wsquota=<working set quota> cli=<command language
interpreter> maxdetach=<maximum number of detached
processes> astlm=<AST queue limit> local=<Local access
time> tqelm=<number of entries in timer queue>
clitables=<CLI tables> priority=<Priority>
network=<network access time> lgicmd=<Name of login
command file> batch=<Access time for batch jobs>
remote=<Remote access time> pgflquota=<Paging file limit>
biolm=<buffered I/O count limit> diolm=<Direct I/O count
limit> enqlm=<Lock queue limit> shrfillm=<Maximum number
of shared files> maxjobs=<Maximum number of processes>
fillm=<open file limit> maxacctjobs=<Maximum number of
batch> bytlim=<Buffered I/O byte limit> server=<IP
Address> login=<Admin User> password=<Admin Password>
```

- vms_findnextmemid.exp

Provides the last member ID of the request existing group on the OpenVMS system.

Syntax:

```
vms_findnextmemid.exp gid=<Groupd Id> server=<IP
Address> login=<Admin User> password=<Admin Password>
```

- `vms_changePassword.exp`

Changes or resets an existing user's password on the OpenVMS system.

Syntax:

```
vms_changePassword.exp username=<User name> password=<New password> passwordflag=<changepassword | resetpassword> server=<IP Address> login=<Admin User> password=<Admin Password>
```

- `vms_enableUser.exp`

Enables an existing (disabled) user on the OpenVMS system.

Syntax:

```
vms_enableUser.exp username=<User name> server=<IP Address> login=<Admin User> password=<Admin Password>
```

- `vms_disableUser.exp`

Disables an existing (active) user on the OpenVMS system.

Syntax:

```
vms_disableUser.exp username=<User name> server=<IP Address> login=<Admin User> password=<Admin Password>
```

- `vms_modifyUserGroups.exp`

Grants or revokes a group (or identifier) from an existing user on the OpenVMS system.

Syntax:

```
vms_modifyUserGroups.exp username=<User name> gname=<Group name> change_access=<grant | revoke> server=<IP Address> login=<Admin User> password=<Admin Password>
```

- `vms_listusers.exp`

Lists all of the users on the OpenVMS system.

Syntax:

```
vms_listusers.exp server=<IP Address> login=<Admin User> password=<Admin Password>
```

- `vms_listgroups.exp`

Lists all of the groups (identifiers) on the OpenVMS system.

Syntax:

```
vms_listgroups.exp server=<IP Address> login=<Admin User>  
password=<Admin Password>
```

- `vms_getUserGroups.exp`

Lists the groups granted to a user on the OpenVMS system.

Syntax:

```
vms_getUserGroups.exp username=<User name> server=<IP  
Address> login=<Admin User> password=<Admin Password>
```

- `vms_finduser.exp`

Tests whether a user exists on the OpenVMS system.

Syntax:

```
vms_findgroup.exp username=<User name> server=<IP  
Address> login=<Admin User> password=<Admin Password>
```

- `vms_findgroup.exp`

Tests whether the requested group (or identifier) exists on the OpenVMS system.

Syntax:

```
vms_findgroup.exp gname=<Group name> server=<IP Address>  
login=<Admin User> password=<Admin Password>
```

- `vms_dotest.exp`

Tests the connection parameters to the OpenVMS system.

Syntax:

```
vms_dotest.exp server=<IP Address> login=<Admin User>  
password=<Admin Password>
```