

# HP OpenView Select Identity

Connector for Citrix Password Manager

Connector Version: 1.0

---

## Installation and Configuration Guide

Document Release Date: March 2006  
Software Release Date: March 2006



## Legal Notices

### Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

### Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

### Copyright Notices

© Copyright 2006 Hewlett-Packard Development Company, L.P.

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](http://www.waveset.com)). Portions Copyright © 2003 Waveset Technologies, Inc. 6034 West Courtyard Drive, Suite 210, Austin, Texas 78730. All rights reserved.

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

### Trademark Notices

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

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

JAVA™ is a US trademark of Sun Microsystems, Inc.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California

UNIX® is a registered trademark of The Open Group.

## Support

Please visit the HP OpenView support web site at:

**<http://www.hp.com/managementsoftware/support>**

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

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 enhancement requests online
- Download software patches
- 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://www.hp.com/managementsoftware/access\\_level](http://www.hp.com/managementsoftware/access_level)**

To register for an HP Passport ID, go to:

**<http://www.managementsoftware.hp.com/passport-registration.html>**

---

# Contents

- 1 Introduction ..... 7
  - About HP OpenView Select Identity ..... 7
  - About Connectors ..... 7
  - About Citrix Password Manager Connector ..... 7
- 2 Installing the Connector ..... 9
  - System Requirements ..... 9
  - Installation Procedure ..... 9
    - Extract the Contents of Schema File ..... 10
    - Deploy the Connector on Application Server ..... 10
    - Set up the Secure Socket Layer (SSL) Truststore ..... 10
    - Configure the Connector with OVSI ..... 11
- 3 Uninstalling the Connector ..... 15
- A Sample Deployment Scenario ..... 17
  - Scenario A ..... 17
  - Scenario B ..... 20



# 1 Introduction

This chapter gives an overview of the HP OpenView Select Identity connector for Citrix Password Manager. An HP OpenView Select Identity connector allows you to provision users and manage identities on resource\_system. At the end of this chapter, you will be able to know about:

- the benefits of HP OpenView Select Identity
- the role of a connector
- the connector for Citrix Password Manager

## About HP OpenView Select Identity

HP OpenView Select Identity (OVSI) provides a new approach to identity management. It helps you manage the entire identity lifecycle of an enterprise application. By using OVSI, you can automate the process of provisioning and managing user accounts and access privileges across platforms, applications, and corporate boundaries. OVSI communicates with the enterprise information system through connectors, and automates the tasks of identity management. The enterprise information system, which is also referred to as **resource**, can be a database, a directory service, or an ERP package, among many others.

## About Connectors

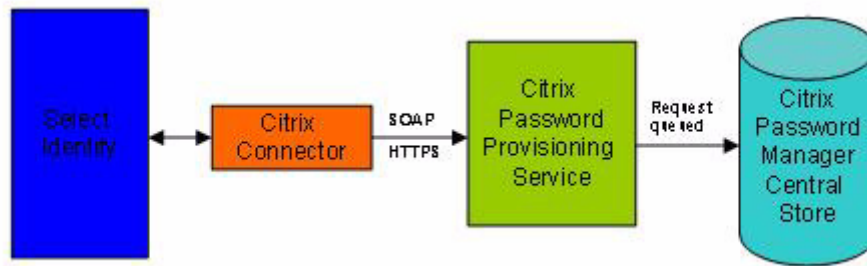
You can establish a connection between a resource and OVSI by using a connector. A connector is resource specific. It is installed on the system where OVSI is installed. The combination of OVSI and connector helps you perform a set of tasks on the resource to manage identity. A connector can be **unidirectional** or **bidirectional**. A unidirectional connector helps you manage identities from OVSI, but if any change takes place in resource, it cannot communicate that back to OVSI. On the other hand, a bidirectional connector can reflect the changes made on resource back to OVSI. This property of bidirectional connectors is known as **reverse synchronization**.

## About Citrix Password Manager Connector

The Citrix Password Manager connector — hereafter referred to as Citrix connector — enables HP OpenView Select Identity to perform provisioning tasks on Citrix Password Manager (CPM). The connector communicates to the Citrix Password Provisioning Web

Service (PPWS) by exchanging SPML payloads. The connector provisions Secondary Credentials to CPM. The communication model of Citrix connector is illustrated in the diagram below.

**Figure 1 Communication Model of Citrix Connector**



The Citrix connector enables you to perform the following tasks on Citrix Password Manager system by using OVSI.

- Add, update, and remove Secondary Credentials for users.
- Retrieve Credential details for a User.
- Verify existence of credential for a User.
- Change user's credential passwords.
- Reset user's credential passwords.

It is a unidirectional connector and pushes changes made to user data in the Select Identity database to a target Citrix Password Manager and its configured user store (such as Active Directory or NTFS File Share).



This connector can be used with OVSI version 4.0 and 3.3.1.



## 2 Installing the Connector

Citrix connector is packaged with the following files.

**Table 1 Citrix Connector Files**

Serial Number	File Name	Description
1.0	CitrixConnector.rar	The connector RAR file (the binaries).
2.0	CitrixConnectorSchema.jar	It contains the Citrix Schema Mapping file.

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

## System Requirements

The Citrix connector is supported in the following environment:

**Table 2 Platform Matrix for Citrix connector**

Select Identity Version	Application Server	Database
3.3.1	Weblogic 8.1.4 on Windows 2003.	Microsoft SQL Server 2000
	Weblogic 8.1.4 on HP-UX 11i.	Microsoft SQL Server 2000
4.0	The Citrix connector is supported on all the platform configurations of Select Identity 4.0.	

This connector is supported with Citrix Password Manager, version 4.1, on Windows 2003.

## Installation Procedure

Perform the following tasks to achieve successful installation of Citrix connector.

- 1 Extract the Contents of Schema File
- 2 Deploy the Connector on Application Server
- 3 Set up the Secure Socket Layer (SSL) Truststore
- 4 Configure the Connector with OVSI

## Extract the Contents of Schema File

Create a subdirectory in the OVSI home directory on OVSI system. Extract the contents of `CitrixConnectorSchema.jar` file to this subdirectory. Ensure that the `CLASSPATH` environment variable in the application server startup script references this Schema subdirectory.

## Deploy the Connector on Application Server

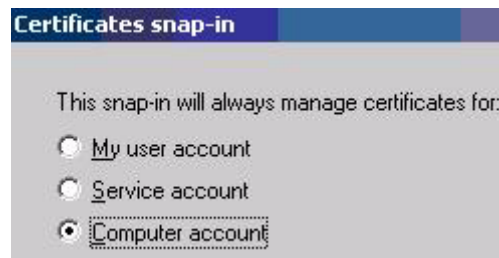
You must deploy the RAR file (`CitrixConnector.rar`) of the connector on an application server. Before deploying the RAR file, you must copy it to a local directory from the connector CD. Refer to *HP OpenView Select Identity Connector Deployment Guide* for more information on deploying a connector on an application server.

## Set up the Secure Socket Layer (SSL) Truststore

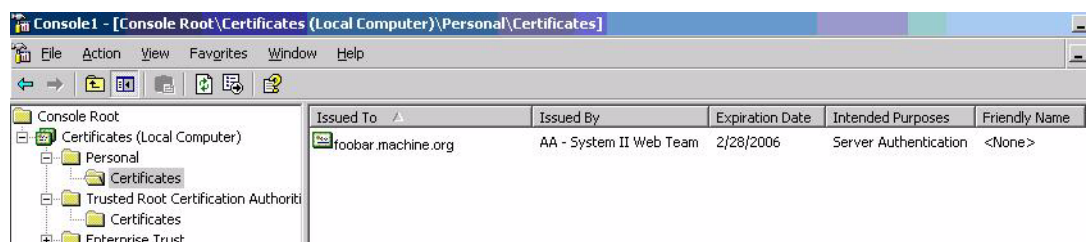
Before configuring the Citrix connector on OVSI, you must set up the SSL Truststore on the OVSI machine by extracting the CA root certificate from Citrix installation because the connector uses SSL Truststore to connect to the PPWS of CPM.

Perform the steps below to obtain the CA root certificate and create SSL Truststore.

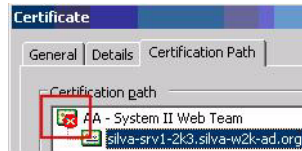
- 1 On the machine where CPM is installed, go to **Start** → **Run**: **mmc**
- 2 Select **Add/Remove Snap-in** → **Add Certificates**.
- 3 Choose Computer Account, and then click **Next**.
- 4 Click **Finish**, and then **OK**.



- 5 In the Console root, expand **Certificates** → **Personal** → **Certificates**.
- 6 Machine's new certificate appears on right pane. The Fully Qualified Domain Name (FQDN) of the machine appears in Issued To column. The certificate authority (For example, AA - System II Web Team) appears in Issued By column.

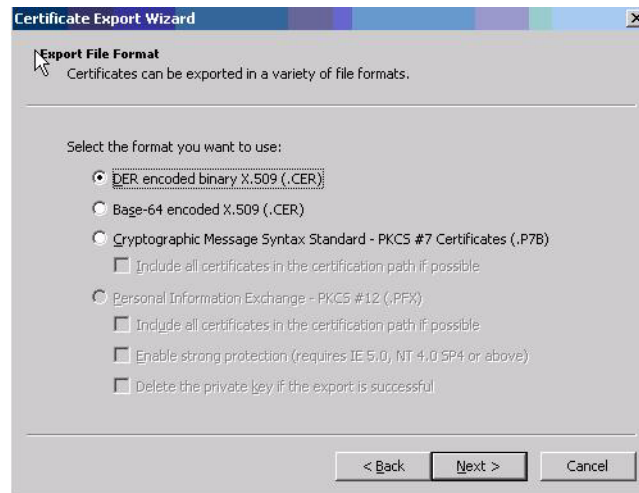


- 7 Double click on **Server** Certificate, choose the Certification Path tab, double click the topmost certificate (the Root CA) - the one highlighted with red X.



The root CA certificate appears

- 8 Choose the Details tab of this certificate, click **Copy to File**, and then export the DER encoded certificate to a local directory.



- 9 After you extract the certificate into a file, you must store it (this contains the CA certificate of the Root CA of Citrix Provisioning service's server certificate) to OVSI machine at `<BEA_JAVA_HOME>\jre\lib\security`. This is the truststore used by Citrix Connector during SSL handshake with Citrix provisioning service.
- 10 To import the certificate, run the Java keytool command from `<BEA_JAVA_HOME>\bin` as:
 

```
keytool -import -file CARootCert.cer -keystore cacerts
```

 The password for default cacerts Truststore is: `changeit`  
 When prompted for Trust this certificate? [no]:, enter **yes**.
- 11 If the application server is still running, you must restart it for the import to take effect.

## Configure the Connector with OVSI

After deploying the connector to an application server, you must configure it with Select Identity. To configure the connector with OVSI, perform the following steps.

- 1 Add a new connector – Add a new connector on OVSI. Refer to *HP OpenView Select Identity Connector Deployment Guide* for information on adding a new connector. While adding the connector, under Current Resource Connectors section in Manage Connectors page, do the following:
  - In the Connector Name text box, specify a name for the connector.
  - In the Pool Name text box, enter **eis/CitrixConnector**

- Under Mapper Available section, select **No**.
- 2 Add a new resource – You must add a new resource to OVSI that uses the newly added connector. Refer to *HP OpenView Select Identity Connector Deployment Guide* for the instruction to add a new resource to OVSI. While entering the resource parameters for Citrix connector, refer to the table below.

**Table 3 Resource Configuration Parameters**

Field Name	Sample Values	Description
Authoritative Source	<i>No</i>	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.
Citrix Password Provisioning Service Endpoint URL	<i>https://&lt;CitrixHostFullName&gt;/MPMService/ProvisionSvc.asmx</i>	The Endpoint URL of the Citrix Password Provisioning Service. This service maybe installed on the same machine as Citrix Password Manager or different machine.
Application Name	<i>ApplicationName</i>	The Application Definition Name of the application to which credentials are to be provisioned. This should be exactly the same value (case sensitive) as that of the Application Definition name.  Refer the Access Console Suite of CPM or consult Citrix Administrator for obtaining the Application Definition name.
User Name	<i>Administrator</i>	The username with READ+WRITE access to the CPM central store (Active Directory/NTFS File Share).
Password	<i>password</i>	Password of the user with READ+WRITE access to central store.
Domain Name	<i>Citrixtest</i>	The Domain name under which the CPM machine is present in.
Schema Mapping File	<i>CitrixSchemaMapping.xml</i>	The Schema Mapping XML file name for Citrix Connector.

- 3 Map the attributes – You must map the OVSI attributes to the attributes of the resource. Refer to *HP OpenView Select Identity Connector Deployment Guide* for information on mapping attributes. While mapping the attributes, refer to the following table for resource specific mapping information.

**Table 4 Citrix Mapping Information**

Select Identity Resource Attribute	Citrix Password Manager Attribute	Description
UserFQDN*	userFQDN	The Fully-Qualified-Domain-Name of the User to whom credentials are to be provisioned for the Application Definition part of Resource Creation parameters (Application Name). This can be of format '<Domainname>\<Username>' or 'CN=sid2000,CN=Users,DC=citrixtest,DC=com'.
CredentialName	CredentialName	The name of the Secondary Credential to be provisioned. This is optional. If the value is not provided, the Application Name (in the Connection Parameters) is taken as the default CredentialName.
CredentialDescription	description	The description of the secondary credential.
ProvisionDescription	provision-description	This is Administrator data that is not viewable or editable by the Agent. This is provided solely for the convenience of the Provisioning Administrator
CitrixGUID*	CitrixGUID	This is a unique ID of the credential that is automatically generated by the connector. This is the Key Field and needs to be mapped to an Attribute on OVSI and a dummy value needs to be passed while adding the user. This value will not be used by connector.
Credential UserID*	userID	The user's account for this credential.

**Table 4 Citrix Mapping Information**

<b>Select Identity Resource Attribute</b>	<b>Citrix Password Manager Attribute</b>	<b>Description</b>
Credential Password*	password	The user's password for this credential.
CustomField1	CustomField1	The custom values for this credential. This can be something like 'Domain name' needed along with user account information (userid/password). To know if the credential requires a custom field, refer the 'Application definition'.
CustomField2	CustomField2	The second custom field value for the credential.

- 4 Associate the newly added resource to a service. Refer to *Service Studio* chapter of *HP OpenView Select Identity Administrator Guide* for more information on service.

---

## 3 Uninstalling the Connector

If you want to uninstall a connector from Select Identity, perform the following steps:

- Remove all resource dependencies.
- Delete the connector from OVSI.
- Delete the connector from application server.

See *HP OpenView Select Identity Connector Deployment Guide* for more information on deleting the connector from application server and OVSI.





# A Sample Deployment Scenario

Citrix connector provisions secondary credentials to end users. The unique identifier for each end user is its fully qualified domain name (FQDN). The FQDN is used as an attribute while provisioning the credentials. This end user can be created through OVSI or the end user maybe existing and the FQDN value is used while provisioning.

The example deployment scenario has the following environment:

- Citrix Password Manager 4.1 on Windows 2003 installed with Active Directory 2003 as Central Store.
- Citrix connector v1.0 deployed on OVSI 4.0.

These are two sample scenarios and the Citrix connector does not mandate the usage of the Active Directory connector or any other connector with it.

## Scenario A

The end user is created from OVSI using another connector. This user is then provisioned secondary credentials for various application definitions as additional services for the base user. The end user is the identity on OVSI and secondary credentials as the associated services with the user's primary service.

- 1 The Active Directory connector is deployed and configured on OVSI. This Active Directory connector is capable of provisioning users to the Active Directory central store of CPM.

### ADExchResource: Resource Access Information

Review the access information about the resource and edit as necessary. Click Apply.

*Required Field \**

Domain: *	citrixtest.com
Username: *	administrator
Password: *	*****
Server Name: *	sint24
AD Port: *	389
Agent Port: *	5000

- 2 The Citrix connector is deployed and configured on HP OVSI. The Citrix resource is capable of provisioning secondary credentials to an Existing Application Definition on CPM called 'Test1'

## CitrixResource-Test1: Resource Access Information

Review the access information about the resource and edit as necessary. Click Apply. Select the next link to continue updating the resource.

### Required Field \*

Citrix Password Provisioning Service Endpoint URL: \* <https://sint19/MPMService/ProvisionSvc.aspx>  
Application Name: \* Test1  
User Name: \* Administrator  
Password: \* \*\*\*\*\*  
Domain Name: \* citrixtest  
Schema Mapping File: \* CitrixSchemaMapping.xml ([View](#))

- 3 Relevant attributes for the Citrix Resource of Test1 are created on HP OVSI and mapped to the schema mapping file attributes. The CitrixGUID is the key field but its value is auto-generated by CPM. So this value is automatically set by the connector during add operation. This attribute just needs to be mapped and provided a dummy value. Below, the attribute is mapped to UserName attribute of OVSI.

## CitrixResource-Test1: Resource Attribute Mapping

Map the applicable resource attributes to the associated HP OpenView Select Identity attributes.

Resource Attribute	↓	Attribute
CitrixGUID		UserName
Credential Password		Test1-Password
Credential UserID		Test1-UserID
CredentialDescription		Test1-Desc
CredentialName		Test1-Name
CustomField1		Test1-Domain
CustomField2		
ProvisionDescription		ProvisionDesc
UserFQDN		UserFQDN
CitrixResource-Test1_ENTITLEMENTS		CitrixResource-Test1_ENTITLEMENTS
CitrixResource-Test1_KEY		CitrixResource-Test1_KEY

- 4 OVSI Services for Active Directory resource and Citrix resource are created.
- 5 The end user is created using the Active Directory connector. This is the user to which you can provision secondary credentials. The FQDN of this user will be used as a required attribute by Citrix connector.


ADExchService : sid211	
Status:	Enabled
Account ID:	sid211
<b>Context Attribute</b>	
City:	
<b>Service Attributes</b>	
ADExchResource_ENTITLEMENTS:	?
CommonName:	? sid211
Email:	? sid211@hp.com
FirstName:	? sid
LastName:	? manchi
UserSuffix:	? ou=ovsi

- 6 Perform Subscribe to Service... for the user created above. Select CitrixService-Test1. Provide the relevant data for provisioning the secondary credential for the end user for the Application Definition 'Test1'.

---

*Required Field \**

City:\*

Activation Date  

---

City	? <input type="text"/>
ProvisionDesc:	? ANAKIN
Test1-Desc:	? SKYWALKER
Test1-Domain:*	? REPUBLIC
Test1-Name:	? sid211
Test1-Password:*	? .....
Test1-UserID:*	? sid211Test1
UserFQDN:*	? citrixtest\sid211
UserName	? sid211

- 7 The end user now has the secondary credential for 'Test1' application definition provisioned. This can be verified by re-starting the 'Password Manager Agent'.
- 8 For provisioning secondary credentials for multiple Application Definitions for an end user, OVSI Resources should be created and configured for each application definition on CPM (as in step 3 for Test1 application definition). Each such Resource can be associated with services and the 'Subscribe to Service...' operation can be used to provision the secondary credential for that Application definition.

## Scenario B

The end user already exists on the domain. The FQDN of this user is then used to provision secondary credentials for various application definitions as identities on OVSI. That is, each secondary credential is the identity on OVSI created by an add operation.

- 1 The Secondary credential is recognized as an identity on OVSI.
- 2 The Citrix Connector is deployed and configured on OVSI. The Citrix resource is capable of provisioning secondary credentials to an Existing Application Definition on CPM called 'Test6'.

### CitrixResource-Test6: Resource Access Information

Review the access information about the resource and edit as necessary. Click Apply. Select the next link to continue updating the resource.

#### Required Field \*

Citrix Password Provisioning Service Endpoint URL: \* <https://sint19MPMService/ProvisionSvc.aspx>  
Application Name: \* Test6  
User Name: \* Administrator  
Password: \* \*\*\*\*\*  
Domain Name: \* citrixtest  
Schema Mapping File: \* CitrixSchemaMapping.xml ([View](#))

- 3 Relevant attributes for the Citrix Resource of Test6 are created on OVSI and mapped to the schema mapping file attributes. The CitrixGUID is the key filed but its value is auto-generated by CPM. So this value is automatically set by the connector during add operation. This attribute just needs to be mapped and provided a dummy value. Below, the attribute is mapped to UserName attribute of OVSI.

### CitrixResource-Test6: Resource Attribute Mapping

Map the applicable resource attributes to the associated HP OpenView Select Identity attributes.

Resource Attribute	↓	Attribute
CitrixGUID		UserName
Credential Password		Test6-Password
Credential UserID		Test6-UserID
CredentialDescription		Test6-Desc
CredentialName		Test6-Name
CustomField1		Test6-Connection
CustomField2		
ProvisionDescription		ProvisionDesc
UserFQDN		UserFQDN
CitrixResource-Test6_ENTITLEMENTS		CitrixResource-Test6_ENTITLEMENTS
CitrixResource-Test6_KEY		CitrixResource-Test6_KEY

- 4 OVSI Services Citrix Resource is created.
- 5 Perform 'Create User' for the above Resource and provide relevant values.

---

*Required Field \**

City:\*

Activation Date  

---

City	<input type="text"/>
ProvisionDesc:	<input type="text" value="Test6Prov"/>
UserFQDN:	<input type="text" value="cfrixtest\sid211"/>
UserName:	<input type="text" value="sid211test6"/>
Test6-Password:	<input type="password" value="....."/>
Test6-Desc:	<input type="text" value="Provision Test6"/>
Test6-Connection:	<input type="text" value="APJ"/>
Test6-Name:	<input type="text" value="sid211"/>
Test6-UserID:	<input type="text" value="sid211"/>

- 6 The secondary credential is provisioned and is an identity on OVSI referred by the value for 'UserName' provided.

