

**Oracle® Enterprise Single Sign-on  
Provisioning Gateway**

TIM Integration and Installation Guide

Release 11.1.1.2.0

**E15704-02**

November 2010

**ORACLE®**

Copyright © 2006-2010, Oracle. All rights reserved.

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

**U.S. GOVERNMENT RIGHTS** Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

## Contents

|   |    |
|---|----|
| Abbreviations and Terminology.....                                      | 4  |
| About Oracle Enterprise Single Sign-on Provisioning Gateway .....       | 5  |
| About This Document.....  | 6  |
| Installation Prerequisites .....  | 7  |
| Release Structure and Package Contents .....                            | 8  |
| Installation Steps .....  | 9  |
| Post Installation Work .....  | 10 |
| ESSO-PG Functional Test .....   | 10 |
| Extend the ITIM Schema to Include E-SSO (ESSO-LM) Attributes.....       | 11 |
| Configure the LDAP Browser to Connect to the IBM Directory Server ..... | 11 |
| Configure ITIM 5.0 or 5.1 to Call the ESSO-PG Connector .....           | 13 |
| Configure ITIM 4.6 to Call the ESSO-PG Connector .....                  | 14 |
| Creating the Service for Active Directory (ITIM 5.0 or 5.1) .....       | 16 |
| Creating the Service for AD (ITIM 4.6) .....                            | 18 |
| Configure the Service Form .....  | 18 |
| Configure the Person Form .....   | 18 |
| Schema Attribute Meta-Values .....                                      | 21 |
| Meta-Value Rules .....  | 21 |
| Supported Meta-Value Tags.....  | 22 |
| Configuring Workflows .....   | 23 |
| Configuring the WorkFlow for the Add Operation.....                     | 23 |
| Configuring the WorkFlow for the Change Password Operation.....         | 23 |
| Configuring the WorkFlow for the Delete Operation .....                 | 23 |
| Configuring the WorkFlow for the Modify Operation.....                  | 23 |
| Upgrading to the New Connector .....                                    | 24 |
| Uninstalling ITIM.....  | 25 |

## Abbreviations and Terminology

Following is a list of commonly-used abbreviations and terminology.

| Abbreviation or Term   | Full Name   |
|------------------------|---|
| Administrative Console | ESSO-LM Administrative Console                          |
| Agent                  | Logon Manager   |
| FTU                    | First-Time Use Wizard                                   |
| ESSO-AM                | Oracle Enterprise Single Sign-on Authentication Manager |
| ESSO-Anywhere          | Oracle Enterprise Single Sign-on Anywhere               |
| ESSO-PG                | Oracle Enterprise Single Sign-on Provisioning Gateway   |
| ESSO-KM                | Oracle Enterprise Single Sign-on Kiosk Manager          |
| ESSO-LM                | Oracle Enterprise Single Sign-on Logon Manager          |
| ESSO-PR                | Oracle Enterprise Single Sign-on Password Reset         |

## About Oracle Enterprise Single Sign-on Provisioning Gateway

ESSO-PG can receive and process provisioning requests initiated by IBM Tivoli Identity Manager (ITIM or TIM). The integration of ESSO-PG with TIM is accomplished through a workflow extension that TIM uses to communicate with the ESSO-PG Web Service.

This workflow extension is the TIM Provisioning Workflow Interface (Connector). The Connector communicates requests from TIM to the ESSO-PG Web Service. The Connector itself can be installed locally or in a remote manner to allow remote invocation by TIM.

This guide is intended for experienced application programmers responsible for the development of TIM. Readers are expected to understand TIM administration concepts. The person completing the installation procedure should also be familiar with the site's system standards. Readers should be able to perform routine security administration tasks.



The instructions in this guide provide an overview of the ESSO-PG-TIM interface, installation instructions, and a sample integration scenario. Steps for integrating into your organization's specific workflow scenario might vary. This guide is intended to serve purely as an example of how to integrate TIM and ESSO-PG in a basic workflow scenario. Review the information provided in this guide to determine how to accomplish integration for your organization. The TIM Connector is set up to work out-of-the-box in a local environment.

## **About This Document**

This document outlines the steps for installing ITIM 4.6, 5.0, or 5.1 and configuring it for integration with Oracle Enterprise Single Sign-on Logon Manager (ESSO-LM) and Oracle Enterprise Single Sign-on Provisioning Gateway (ESSO-PG). ESSO-LM allows you use a single password to log on to any password-protected application on your desktop, your network, and the Internet. It works "out-of-the-box" (without programming or additional network infrastructure) with virtually all applications, including Windows, Web, Java, and host/mainframe applications. ITIM 5.0 and ITIM 5.1 can be integrated with multiple ESSO-PG Servers.

## Installation Prerequisites

The software prerequisites for installing IBM Tivoli Identity Manager 4.6, 5.0, and 5.1 can be found on the IBM Web site.

The ESSO-PG Server and Console must be installed. See the *ESSO-PG Installation and Setup Guide* for installation instructions. Carefully review the *ESSO-PG Release Notes* for system requirements.

To install the ITIM Connector, the following components must be installed:

- Java 1.4.2 or Java 1.5.8
- IBM TIM 4.6 / IBM TIM Express 4.6 / IBM TIM 5.0 or 5.1

### Active Directory Adapter

Active Directory is the source primarily used to store the Oracle credentials. The installation document has been prepared assuming that Active Directory is the source for storing Oracle connector credentials; thus the Active Directory Adapter is required to be installed on ITIM.

## Release Structure and Package Contents

The release package includes:

- **4.6 lib:** contains all the .jar files needed for version 4.6.
- **5.0 lib:** contains all the .jar files needed for version 5.0 and 5.1.
- **Document:** contains all documents for installations.
- **Libraries:** contains workflow extensions and schema modifications.
- **Scripts:** contains all the scripts needed to create the sample work flow.
- **Resources:** contains the key used in the installation and the sample files used for installation.



The library files for release 4.6 and release 5.0 are included in the release package. (Library files for release 5.0 also work with release 5.1.)

## **Installation Steps**

You can find instructions on the IBM Web site for installing and configuring the:

- Database
- Directory Server

You can also refer to the IBM Web site for instructions on installing:

- The Web Sphere Application Server
- Tivoli Identity Manager
- The AD Adapter

## Post Installation Work

### ESSO-PG Functional Test

For TIM 5.0 or 5.1 where integration for Multiple ESSO-PG installations is required, perform the test as stated below and refer to "Release Package\vGoTest" for the necessary libraries and tools needed to complete this test.

#### Prerequisites

- JDK 1.5 must be installed on the machine where ITIM is installed.
- The test machine must be able to access the ESSO-PG Web Services URL.  
Example :<http://localhost:82/> ESSO-PG Service/UP.asmx
- The user you are adding to ESSO-PG must exist in the ESSO-PG repository.

#### Test Steps

1. Copy the folder "vGoTest," located in: Release Package\vGoTest, to a local folder (for example, C:\TEMP).
2. Copy the PMProperties folder located in the folder: Release Package\vGoTest, to C:\.
3. Modify the PMClientConfiguration.properties in the PMProperties folder, and add the values for the following properties in the properties file:
  - javaCLI.serviceurl  
Example: <http://localhost:82/v-GO PM Service/UP.asmx>
  - javaCLI.applicationname  
Example: AD Server 2003
  - javaCLI.username  
Example: TestDomain\\user1 (TestDomain is the name of the domain where the ESSO-PG repository is located, and user1 is the user that has been created and for whom the passlogix credentials are to be added.)
  - javaCLI.serviceuser  
Example: plogix\\administrator
  - javaCLI.serviceuserpassword  
Example: sena@120

(Read each property's description for the values to set in the properties file.)

4. Open a command prompt and add the jars in: C:/TEMP/lib folder to the classpath, along with the PMTest.jar.  
(<http://java.sun.com/j2se/1.5.0/docs/tooldocs/windows/classpath.html>)
5. Change the directory location to: C:\TEMP\vGoTest, and open the command prompt at this location. Execute the following at the command prompt:  
`java com.sena.edir.TIMInterface`
6. If everything is correct, the output will be similar to the following:  

```
Invoked the command add_credential with return
f216b216-4ec1-44c9-859c-76662c79471a
```
7. Perform steps 3 through 6 for all instances of the ESSO-PG Server installation.

## Extend the ITIM Schema to Include E-SSO (ESSO-LM) Attributes

The schema for ITIM must be extended to include E-SSO (ESSO-LM) attributes. The steps for ITIM 5.0 (and for ITIM 5.1) are the same as those for ITIM 4.6. The files used to extend the ITIM 5.0 schema can be accessed from the Release Package of ITIM 4.6, as described below.

1. Back up C:\idsslapd-ldapdb2\etc\v3.modifiedschema. This location will be different on non-Windows platforms.
2. Add the ESSO-LM attribute lines:
  - For ITIM 4.6, ITIM 5.0, and ITIM 5.1: TIM46V3.modifiedschema file (located under Libraries\TIM\_SIMExtensions) to the v3.modifiedschema file.
  - For ITIM Express 4.6: TIMXV3.modifiedschema file (located under Libraries\TIM\_SIMExtensions) to the v3.modifiedschema file.
3. Replace the eraccountitem and erserviceitem object class lines in v3.modifiedschema with the lines from the appropriate modifiedschema file on the CD.



If you have previously modified the eraccountitem or erserviceitem object classes in v3.modifiedschema, you must re-apply the changes in conjunction with these changes.

4. Add the attribute indexes to v3.modifiedschema from the appropriate modifiedschema file on the CD.
5. Save v3.modifiedschema and restart IDS.
6. Import the integration operations. Download an LDAP Browser. A default browser can be downloaded from:

<http://www-unix.mcs.anl.gov/~gawor/ldap/download.html>

## Configure the LDAP Browser to Connect to the IBM Directory Server

The SSOOperations.Idif contains the Add, Delete, ChangePassword, and Restore operations. These are required for all deployments. The SSOMODOperation.Idif file contains the Modify operation, which may or may not apply to the user environment. For this reason, the Modify operation is packaged separately, and installation is optional.

1. Back up current operations by exporting the following objects:
 

```
erglobalid=0000000000000000000022,ou=operations,ou=itim,ou=ibm,DC=COM
erglobalid=0000000000000000000023,ou=operations,ou=itim,ou=ibm,DC=COM
erglobalid=0000000000000000000024,ou=operations,ou=itim,ou=ibm,DC=COM
erglobalid=0000000000000000000025,ou=operations,ou=itim,ou=ibm,DC=COM
erglobalid=0000000000000000000027,ou=operations,ou=itim,ou=ibm,DC=COM
```
2. Edit the SSOOperations.Idif and SSOMODOperation.Idif, located under the Libraries\Extensions folder, to match the DNs used to back up the current operations in the previous step.
3. Delete the current operation objects.
4. Import the operation objects from the SSOOperations.Idif file (and, optionally, the SSOMODOperation.Idif file).



The actual DN will depend on the IDS setup in your environment.

5. Start ITIM.
6. After the schema has been extended, the following attributes should be present in the Directory Server.

| Attribute Name                | Syntax          |
|-------------------------------|-----------------|
| vgoadminid                    | DirectoryString |
| vgoadminpwd                   | binary          |
| vgoApplicationDescription     | IA5String       |
| vgoApplicationDescriptionMeta | IA5String       |
| vgoApplicationID              | IA5String       |
| vgoApplicationIDMeta          | IA5String       |
| vgoApplicationPWD             | IA5String       |
| vgoApplicationUserIDMeta      | IA5String       |
| vgoCredAttribute1             | IA5String       |
| vgoCredAttribute1Meta         | IA5String       |
| vgoCredAttribute2             | IA5String       |
| vgoCredAttribute2Meta         | IA5String       |
| vgoSSOUserID                  | IA5String       |
| vgoSSOUserIDMeta              | IA5String       |
| vgoserver                     | IA5String       |

The erserviceitem Class should have the following attributes added:

- vgoadminid
- vgoadminpwd
- vgoserver
- vgoCredAttribute1Meta
- vgoCredAttribute2Meta
- vgoSSOUserIDMeta
- vgoApplicationDescriptionMeta
- vgoApplicationIDMeta
- vgoApplicationUserIDMeta

The eraccountitem Class should have the following attributes added:

- vgoSSOUserID
- vgoCredAttribute1
- vgoCredAttribute2
- vgoApplicationPWD
- vgoserver
- vgoApplicationID
- vgoApplicationDescription

## Configure ITIM 5.0 or 5.1 to Call the ESSO-PG Connector

1. First, stop the Web Sphere server.

The file "Workflowextensions.xml" in the location:

(drive name):\Program Files\IBM\ITIM\data

is modified to incorporate the operations for the Oracle connector. (A Sample file is present in the Resources folder of the CD).ty6gkj



When modifying the file special care should be taken to not insert any space at the start of the file.

2. Locate the following .jar files (present in the 5.0 lib folder of the CD):

- axis-1.2.1.jar
- bcprov-jdk13-128.jar
- mail.jar
- opensaml-1.0.1.jar
- PMCLI.jar
- wss4j.jar
- xmlsec-1.3.0.jar
- PMAPIInvoker\_6.0.jar
- EncryptionTool.jar

3. Copy the files to the following directory.

(drive name):\Program Files\IBM\Web Sphere\AppServer\profiles\AppSrv01\installedApps\sena-prrqNode01Cell\ITIM.ear

4. Locate the Manifest file in:

(drive name):\Program Files\IBM\Web Sphere\AppServer\profiles\AppSrv01\installedApps\sena-prrqNode01Cell\ITIM.ear\app\_web.war\META-INF.

5. Update the file with the following information:

```

Class-Path: axis-1.2.1.jar bcprov-jdk13-128.jar mail.jar opensaml-1.0.1.jar
PMCLI.jar wss4j.jar xmlsec-1.3.0.jar PMAPIInvoker_6.0.jar EncryptionTool.jar
ITIM_api.jar ITIM_common.jar ITIM_server.jar
    Created-By: 2.3 (IBM Corporation)
    Ant-Version: Apache Ant 1.6.5
    Created-By: 2.3 (IBM Corporation)
    Ant-Version: Apache Ant 1.6.5
  
```

A sample manifest file is present in the Resources folder in the CD.



The .jar file that is present in the enRole.ear file should have the same name in the Manifest file. For example, if the name of the connector file is PMAPIInvoker-6.0.jar, it should have the same name in the manifest.

6. After the file is modified, the server is restarted.

## Configure ITIM 4.6 to Call the ESSO-PG Connector

1. Using the procedures described on the IBM Web site, add the following installed files—located in the 4.6 lib\jars\_4.6 folder of the Release package—as shared libraries:
  - PMCLI.jar
  - axis.jar
  - bcprov-jdk13-128.jar
  - dom.jar
  - jaxrpc.jar
  - opensaml-1.0.1.jar
  - sax.jar
  - wss4j.jar
  - xalan.jar
  - xercesImpl.jar
  - xmlsec-1.3.0.jar
2. Using the WebSphere Admin Console, set the server Classloader Policy to **Single** and the WAR Classloader Policy for ITIMx to either **Module** or **Application**.
3. Open the 4.6 lib\jars\_4.6 folder, which contains the following file:  
PMAPIInvoker\_6.0.jar.
4. Copy the PMAPIInvoker\_6.0.jar to the following location:  
\$WAS\_HOME/installedApps/<cell>/enRole.ear
5. Add:  
**For ITIM 4.6:** Locate the IBM Websphere's manifest file, at:  
\$WAS\_HOME/installedApps/<cell>/enRole.ear/app\_web.war/META-INF/MANIFEST.MF. Add the jars found in the 4.6 lib\jars\_4.6 folder.



The .jar file that is present in the enRole.ear file should have the same name in the Manifest file. For example, if the name of the connector file is PMAPIInvoker-6.0.jar, it should have the same name in the manifest file.

**For ITIM Express 4.6:** Add the library file as a shared library using the procedure described on the IBM Web site.

6. Go to:

"\com\passlogix\integration\provision\conf"

and modify the **PMClientConfiguration.properties** file to add the location of the ESSO-PG Server. A sample file is included in the Resource folder of the CD.

7. Modify the following attribute:

**javaCLI.serviceurl**

For example:

javaCLI.serviceurl=http://192.168.120.28:80/ESSO-PG Service/UP.asmx

8. Compress the file and create the jar with the same name (**PMAPIInvoker\_6.0.jar**).

9. Back up the workflowextenstions.xml file located in the \$ITIM\_HOME/data folder.

- **For ITIM 4.6:** overwrite the workflowextensions.xml file with the TIM46V3.workflowextensions.xml file, located in the Libraries\TIM\_SIM\Extensions folder.
- **For ITIM 4.6 Express:** overwrite the workflowextensions.xml file with the TIMXV3.workflowextensions.xml file, located in the Libraries\TIM\_SIM\Extensions folder.

## Creating the Service for Active Directory (ITIM 5.0 or 5.1)



This scenario assumes that Active Directory stores the user's SSO credentials.

1. Create a service type for Active Directory, as described in the document for installing the AD Adapter.
2. Log on to the ITIM Administrative console.
3. Select **Configure System->Design Form->services->Active Directory profile**. Add the following attributes:
  - vgoApplicationDescriptionMeta
  - vgoApplicationIDMeta
  - vgoApplicationUserIDMeta
  - vgoCredAttribute1Meta
  - vgoCredAttribute2Meta
  - vgoSSOUserIDMeta
  - vgoadminid
  - vgoadminpwd
  - vgoserver
4. Select **Manage Services**. From the right-hand panel, select **create** to create an AD service. The values for creating the service are as follows:

**\*Service Name:**

Any name.

**\*Description:**

Any description.

**\*URL:**

<http://<machine IP>:<Port>>

Here, machine IP is the IP where the AD Adapter is running, and Port is the Port configured during AD Adapter installation; the default is 45580. Refer to the AD Adapter Installation Guide for more information.

**\*User ID:**

Configured during AD Adapter installation. The default is "agent."

**\*Password:**

Configured during AD Adapter installation; the default is "agent."

**\*Base Point DN**

As configured in AD. This is optional.

**\*Administration User Account:**

AD Administrative Account.

**\*Administration User Password**

AD Administrative Account password.

**\*Owner:**

Optional.

**\*Service Prerequisite**

Optional.

**\*vgoapplicationdescriptionmeta**

Optional.

**\*vgoapplicationidmeta**

AD Server 2003(this is used in case the service is the root service).

**\*vgocredattribute1meta**

<STRING|MYDOMAIN\><ACCOUNT|eruid>

Here, MYDOMAIN is the domain name where the server is hosted.

**\*vgocredattribute2meta**

**\*vgossouseridmeta**

<OWNER|uid>

**\*vgoadminid**

MYDOMAIN\Administrator

**\*vgoadminpwd**

The password (This is configured as a "Password"-type field, and should not appear in clear text.)

**\*vgoserver**

The URL of the v-GO PM Web service

(for example, <http://192.168.120.163/v-GO%20PM%20Service/UP.asmx>)

The service is ready; a role is created. In ITIM, accounts can be provisioned to users only through Roles that are associated with a provisioning policy.

## Creating the Service for AD (ITIM 4.6)

Follow these steps to create the service for AD.

### Configure the Service Form



This scenario assumes that Active Directory stores the user's SSO credentials.

1. Locate the form.
  - For ITIM 4.6, click **Configuration -> Form Customization**.
  - ITIM Express 4.6: Click **Configure System -> Design Forms**.
2. Select the Service folder and then ADProfile from the tree view. (Install ADAgent and import ADProfile.jar if necessary). Service profile names might differ from environment to environment.
3. Create a new tab and add the following ESSO-LM attributes on this tab:
  - vgoapplicationdescriptionmeta
  - vgoapplicationidmeta
  - vgoapplicationuseridmeta
  - vgocredattribute1meta
  - vgocredattribute2meta
  - vgossouseridmeta
  - vgoadminid
  - vgoadminpwd (**Password Field**)
4. Save the form.
5. Repeat these steps for all services that need to sync with ESSO-PG.

### Configure the Person Form

This pertains to ITIM 4.6 only.

1. Select the **Person** folder and then **Person** from the tree view.
2. Add the uid attribute to the first tab.

### *Enter ESSO-PG Data on the Services for ITIM 4.6*

1. Click **Provisioning -> Manage Services**.
2. Select **AD Service** and click **Detailed Information**.

3. On tab 2, add the following:

- vgoapplicationidmeta: \*Application Template Name
- vgossouseridmeta: <OWNER|uid>

where Application Template Name is the name of the Application Template to provision for with an asterisk(\*) prefixed. The asterisk is unique to an AD ESSO-PG repository and is not needed for all services.

You have the option to fill in the following fields with text values:

- vgoapplicationdescriptionmeta
- vgocredattribute1meta
- vgocredattribute2meta

The vgoapplicationuseridmeta field must be set with the userid of the credentials to inject. An example value could follow this format:

<STRING|DOMAIN\><ACCOUNT|eruid>

where DOMAIN is replaced with the actual name of the domain where the credential exists.

- vgoadminid  
Example : MyDomain\Administrator

- vgoadminpwd  
The password(it should not appear in clear as it is a Field of type "Password ")

4. Save your changes.

5. Repeat these steps for all other services that need to sync with ESSO-LM.

**For ITIM Express 4.6:**

1. Click **Manage Users**.
2. Select **Create -> Active Directory Profile**.
3. Fill out the required attribute values on the first page and click **Next**. (At this point, you can test the connection before continuing to verify the values.)
4. On tab2, add the following:

- vgoapplicationidmeta: \*Application Template Name
- vgossouseridmeta: <OWNER|uid>

where Application Template Name is the name of the Application Template to provision for with an asterisk(\*) prefixed. The asterisk is unique to an Active Directory Oracle repository and is not needed for all services.

You have the option to fill in the following fields with text values if needed:

- vgoapplicationdescriptionmeta
- vgocredattribute1meta
- vgocredattribute2meta

Additionally, the vgoapplicationuseridmeta field must be set with the userid of the credentials to inject. An example value could follow this format:

<STRING|DOMAIN\><ACCOUNT|eruid>

where DOMAIN is replaced with the actual name of the domain where the credential exists.

- vgoadminid  
Example : MyDomain\Administrator

- vgoadminpwd  
The password(it should not appear in clear as it is a Field of type "Password ")

5. Click **Next**. Set the reconciliation schedule and click **Finish**.
6. If there are additional services that need to sync with ESSO-LM, select **Create another service instance** and repeat these steps.

## Schema Attribute Meta-Values

Several attributes have been added to the LDAP schema to support ESSO-PG and ITIM integration requirements. These attributes require meta-values to work properly. This section describes how to define these values. The following table displays the attributes and their required values:

| Attribute                        | Required Value                                    |
|----------------------------------|---|
| vgoApplicationIDLiteral          | string value (can contain root service indicator) |
| vgoApplicationDescriptionLiteral | string value                                      |
| vgoSSOUUserIDMetaMeta-           | Value   |
| vgoAtt1MetaMeta-                 | Value   |
| vgoAtt2MetaMeta-                 | Value   |
| vgoApplicationUserIDMetaMeta-    | Value   |

## Meta-Value Rules

Meta-Values follow these guidelines:

- Meta-Values consist of a tag and a value separated by a “|” (pipe) character. The tag specifies the object class from which to pull the appropriate data. The value specifies the attribute within that object class from which to pull the appropriate data.
- Meta-Values are enclosed in angle brackets (< and >), which is common in HTML and other markup languages.
- Multiple meta-values in a single erServiceItem attribute are concatenated to form a single return value.
- The attribute referenced by any meta-value is assumed to be a single string value. Support is not provided for multiple values or binary attribute data.
- If a value does not exist in the v-GOApplicationIDMeta attribute of the current service item, all subsequent ESSO-PG processing is skipped, and an indicator is set to avoid further processing.
- If the first character of the v-GOApplicationIDMeta attribute of the current service is an asterisk (\*), it is read as ESSO-PG’s Root Service. The asterisk is normally removed to read the true Application ID, but some operations process the attribute differently when a root service is identified.
- If a meta-value cannot be parsed successfully, a null value is used for the account attribute in question.

## Supported Meta-Value Tags

The following table describes the supported meta-value tags and describes how to parse each to derive the appropriate value.

| Tag Name | Description                                 | How To Parse  | Examples  |
|----------|---|---|---|
| SERVICE  | References the current service object       | The value is the name of an attribute in the current service object | <SERVICE v-GO><br><i>Parsed as:</i><br>The value of the v-GO attribute in the current service object    |
| ACCOUNT  | References the current account object       | The value is the name of an attribute in the current account object | <ACCOUNT eruid><br><i>Parsed as:</i><br>The value of the eruid attribute in the current account object. |
| OWNER    | References the current user's Person object | The value is the name of an attribute in the owner's Person object  | <OWNER uid><br><i>Parsed as:</i><br>The value of the uid attribute in the owner's Person object         |
| STRING   | The value is treated as a string literal    | The value is treated as a string literal                            | <STRING cn=><br><i>Parsed as:</i><br>cn=  |

# Configuring Workflows

To configure the workflows for ITIM 5.0 (or 5.1) and ITIM 4.6, log on to the ITIM Administrative console.

- **For ITIM 5.0 or 5.1:** Select **Configure System -> Manage Operations**. Under **Operation Level**, select **Entity Level**. From the Entity drop-down list, select **AD Account**. Click **Add**. The page for configuring the workflow opens.
- **For ITIM 4.6:** Select **Configure System -> Manage Operations**. Operations are added for the Entity Configuration where operations are added for AD Service that is created.

Workflows are configured in ITIM 4.6 exactly as they are in ITIM 5.0.

## Configuring the WorkFlow for the Add Operation

When the **Add** option is selected, name the operation "add."

Script files can be found in the Scripts folder of the Release Package.

- The "add\_ssoid" script can be found in the "add\_ssoid.txt" text file, located in the Scripts folder of the Release Package.
- The "checkSSO" script can be found in the "add\_checkss0.txt" text file, located in the Scripts folder of the Release Package.

## Configuring the WorkFlow for the Change Password Operation

When the **Add** option is selected, name the operation "changePassword."

The "checkSSO" script can be found in the "changepassword\_checkss0.txt" text file, located in the Scripts folder of the Release Package.

## Configuring the WorkFlow for the Delete Operation

When the **Add** option is selected, name the operation "delete."

- The "CheckRootService" script can be found in the "deleteCheckRootService.txt" text file, located in the Scripts folder of the Release Package.
- The "checkSSO" script can be found in the "deleteCheckSSO.txt" text file, located in the Scripts folder of the Release Package.

## Configuring the WorkFlow for the Modify Operation

When the **Add** option is selected, name the operation "modify."

The "checkSSO" script can be found in the "modifyCheckSSO.txt" text file, located in the Scripts folder of the Release Package.

## Configuring the WorkFlow for the Restore Operation

When the **Add** option is selected, name the operation "restore."

- The "checkPWDChg" script can be found in the "restorecheckPWDChg.txt" text file, located in the Scripts folder of the Release Package.
- The "checkSSO" script can be found in the "restorecheckSSO.txt" text file, located in the Scripts folder of the Release Package.

## Upgrading to the New Connector

1. Replace the existing " PMAPIInvoker\_6.0.jar," present in the location: "(drive name):\Program Files\IBM\Web Sphere\AppServer\profiles\AppSrv01\installedApps\sena-prrqNode01Cell\ITIM.ear" with the jar present in the location Release Folder\5.0.lib.
2. Ascertain that the service has been modified to include the attributes **vgoadminid**, **vgoadminpwd**, and **vgoserver**, as described in the section [Extend the ITIM Schema to Include ESSO-PG Attributes](#) and the section [Creating the Service for Active Directory](#), and that the values for these attributes are populated when the service is created.

## **Uninstalling ITIM**

Steps for uninstalling the connector are available on the IBM Web site.