

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

TIM Integration and Installation Guide

Release 10.1.4.1.0

E12619-01

November 2008

Copyright © 2006-2008, 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.

Table of Contents


About TIM Integration and Installation	4
Audience.....	4
Using TIM for Integration and Installation.....	5
ESSO-PG TIM Connector	6
Component Module: CLI (Java Client)	6
Installation Overview.....	7
Prerequisites	7
Installation Instructions	8
Installing the Java CLI API libraries.....	8
Installing the Connector	8
Schema Attribute Meta-Values	13
Meta-Value Rules	13
Supported Meta-Value Tags	14

About TIM Integration and Installation

This guide describes how to install the IBM Tivoli Identity Manager (ITIM or TIM), version 6.1, and integrate it with Oracle Enterprise Single Sign-On Provisioning Gateway (ESSO-PG).

Audience

This guide is intended for experienced application programmers responsible for the development of the IBM Tivoli Identity Manager. 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.

	<p>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.</p> <p>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.</p>
---	---

Acronym or Abbreviation	Full Name
SSO Agent	ESSO-LM Agent
SSO Administrative Console	ESSO-LM Administrative Console
ESSO-LM	Oracle Enterprise Single Sign-On Logon Manager
ESSO-AM	Oracle Enterprise Single Sign-On Authentication Manager
ESSO-KM	Oracle Enterprise Single Sign-On Kiosk Manager
ESSO-PG	Oracle Enterprise Single Sign-On Provisioning Gateway
ESSO-PR	Oracle Enterprise Single Sign-On Password Reset
SSO	ESSO-LM
FTU	First Time Use
SSO Agent	ESSO-LM Agent

Using TIM for Integration and Installation

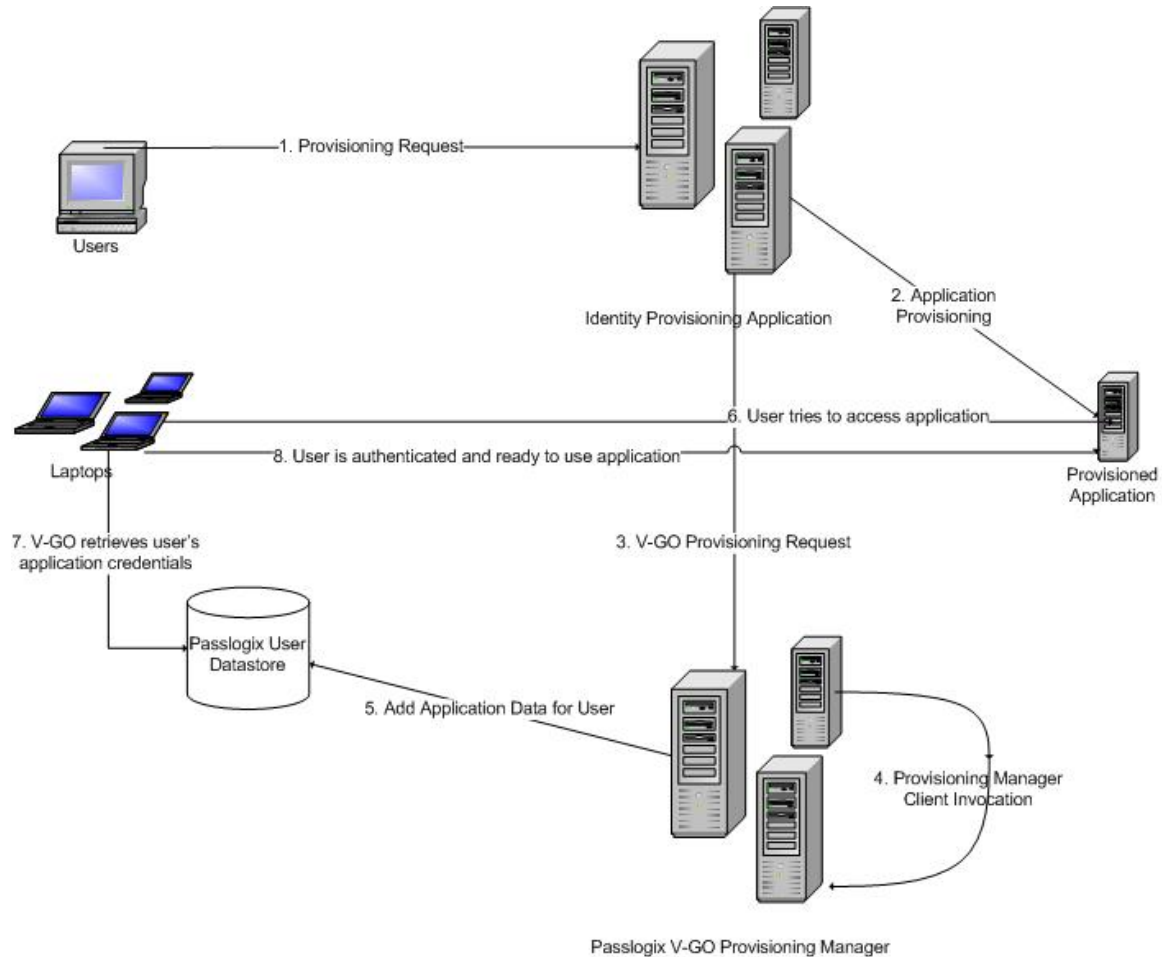
ESSO-PG can receive and process provisioning requests initiated by IBM Tivoli Identity Manager (ITIM or TIM). The integration of ESSO-PG with TIM is accomplished through a workflow extension that TIM uses to communicate with the ESSO-PG Web Service.

This workflow extension has two components, the ESSO-PG Command Line Interface (CLI) and the TIM Provisioning Workflow Interface (Connector). The CLI accepts requests from the Connector and communicates them 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 allows the Connector to reside on platforms that are currently not supported by the ESSO-PG CLI. In the remote case, SSL is used to secure communications between machines.

ESSO-PG TIM Connector

The ESSO-PG Client CLI makes it possible to use other provisioning solutions to communicate with the ESSO-PG Web Service. For more information on the CLI syntax and usage, refer to the *ESSO-PG Client CLI Guide*.

The following diagram shows the sequence of events that takes place during the provisioning of a ESSO-PG -enabled application for a user after the application has been deployed:



Component Module: CLI (Java Client)

The Java CLI is the command-line-based client interface for ESSO-PG Server. For the Connector to work properly, the CLI must be installed on the same machine as TIM. The CLI becomes responsible for sending the provisioning instructions to the ESSO-PG Web Service. From there, the ESSO-PG server stores the instructions on the backend Directory Server for later execution and management. Any results are returned to TIM via the invoked CLI operation. The Connector and CLI are supported on any platform that supports the Java Runtime Environment (1.4.2).

Installation Overview

This section describes installation and configuration requirements to integrate ESSO-PG with the IBM Tivoli Identity Manager.

- [Install required prerequisites](#)
- [Install the TIM Connector](#)
- [Configure v-GO PM to work with TIM](#)

Prerequisites

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

The ESSO-PG Java CLI components must be installed on the system running the TIM Provisioning Workflow Interface (Connector). See the *ESSO-PG Installation and Setup Guide* for the installation and configuration of the ESSO-PG CLI.

To install the Connector the following components must be installed:

- Java 1.4.2 or higher
- ESSO-PG 10.1.4.1.0 Java CLI
- IBM TIM 4.6 / IBM TIM Express 4.6

Installation Instructions

This section describes how to install the TIM connector and integrate it into the TIM workflow.

Installing the Java CLI API libraries

1. Insert the ESSO-PG CD and run setup. Select **Install ESSO-PG Client CLI/SDK** to install the ESSO-PG Java CLI for JDK 1.42 (select **Custom** option).
2. Add the following installed files (usually under Program Files) as shared libraries using the procedure described at:

ITIM 4.6:

http://publib.boulder.ibm.com/infocenter/wasinfo/v5r1//index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/ae/tcws_sharedlib.html

ITIM Express 4.6:

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.express.doc/info/exp/ae/tcws_sharedlib.html

```
pmcli.jar  
axis.jar  
bcprov-jdk13-128.jar  
dom.jar  
jaxp-api.jar  
jaxrpc.jar  
opensaml-1.0.1.jar  
sax.jar  
wss4j.jar  
xalan.jar  
xercesImpl.jar  
xmlsec-1.3.0.jar
```

3. Using the WebSphere Admin Console, set the server Classloader Policy to **Single** and the WAR Classloader Policy for **ITIMx** to either **Module** or **Application**.

Installing the Connector

1. Insert the ESSO-PG CD and open the Libraries\TIM_SIM directory, which contains the following file:

PMAPIInvoker-6.1.jar. TIM Provisioning Workflow Interface (Connector)

See the [configuration options](#) for information on how to set up the Connector to run in your environment.

2. Copy the Connector to the following location:

```
$WAS_HOME/installedApps/<cell>/enRole.ear
```


3. **ITIM 4.6:** Add the Connector to IBM Websphere's manifest file located at:
\$WAS_HOME/installedApps/<cell>/enRole.ear/app_web.war/META-INF/MANIFEST.MF.
ITIM Express 4.6: Add the library file as a shared library using the procedure described at:
http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.express.doc/info/exp/ae/tcws_sharedlib.html
4. Modify the library configuration file in PMAPIInvoker-6.1.jar. The keys that must be modified are:

javaCLI.serviceurl

Change to the full URL of the ESSO-PG Server. Example: http://<host address of PM Server>/v-GO PM Service/UP.asmx

javaCLI.serviceuser

Change to the Administrative userid of ESSO-PG Server. If the v ESSO-PG Server is configured to speak with an Active Directory server, the format should be <DOMAIN>\\<USERNAME>.

javaCLI.serviceuserpassword

Change to the Password for the serviceuser set in javaCLI.serviceuser.

5. Back up the workflowextenstions.xml file located in the \$ITIM_HOME/data folder.

ITIM 4.6: overwrite the workflowextensions.xml file with the TIM46V3.workflowextensions.xml file located on the ESSO-PG CD under the Libraries\TIM_SIM\Extensions folder.

ITIM 4.6 Express: overwrite the workflowextensions.xml file with the TIMXV3.workflowextensions.xml file located on the ESSO-PG CD under the Libraries\TIM_SIM\Extensions folder.



This only has to be done if the existing workflowextensions.xml file has not been modified already. If the original has been modified, add all Passlogix ACTIVITY IDs, defined in the extensions file that is on the CD, to the ITIM extensions file.

6. Extend the ITIM schema to include the E-SSO (**vgo***) attributes:
 - a. Back up C:\idsslapd-ldapdb2\etc\v3.modifiedschema. This location will be different on non-Windows platforms.
 - b. Add the **vgo*** attribute lines from the:

ITIM 4.6: TIM46V3.modifiedschema file (located under Libraries\TIM_SIM\Extensions) to the v3.modifiedschema file.

ITIM Express 4.6: TIMXV3.modifiedschema file (located under Libraries\TIM_SIM\Extensions) to the v3.modifiedschema file.

- c. 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 reapply the changes in conjunction with these changes.

- d. Add the attribute indexes to `v3.modifiedschema` from the appropriate `modifiedschema` file on the CD.
 - e. Save `v3.modifiedschema` and restart IDS.
7. Import the integration operations. Download an LDAP Browser. A default browser can be downloaded from this location:

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

Configure the LDAP Browser to connect to the IBM Directory Server.



The `SSOperations.ldif` contains the Add, Delete, ChangePassword, and Restore operations. These are required for all deployments. The `SSMODOperation.ldif` file contains the Modify operation, which might or might not apply to the user environment. For this reason, the Modify operation is packaged separately and has the option of being installed.

- a. Backup current operations by exporting the following objects:




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


```
erglobalid=0000000000000000022,ou=operations,ou=itim,ou=ibm,DC=COM
erglobalid=0000000000000000023,ou=operations,ou=itim,ou=ibm,DC=COM
erglobalid=0000000000000000024,ou=operations,ou=itim,ou=ibm,DC=COM
erglobalid=0000000000000000025,ou=operations,ou=itim,ou=ibm,DC=COM
erglobalid=0000000000000000027,ou=operations,ou=itim,ou=ibm,DC=COM
```

- b. Edit the `SSOperations.ldif` and `SSMODOperation.ldif` located under the `Libraries\Extensions` folder to match the DNs used to back up the current operations in the previous step (a).
- c. Delete the current operation objects.
- d. Import the operation objects from the `SSOperations.ldif` file (and optionally the `SSMODOperation.ldif` file).

8. Start ITIM.
9. Configure the Service form following these steps:

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

- a. **ITIM 4.6:** Click **Configuration > Form Customization**.
- b. **ITIM Express 4.6:** Click **Configure System > Design Forms**.
- c. 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.
---	---

- d. Create a new tab and add all ESSO-LM attributes on this tab as text fields.
 - e. Save the form.
 - f. Repeat steps (a) to (d) for all services that need to sync with ESSO-PG.
10. **ITIM 4.6 Only:** Configure the Person form following these steps.
 - a) Select the Person folder and then Person from the tree view.
 - b) Add the **uid** attribute to the first tab.

11. Enter ESSO-PG data on the Services.

ITIM 4.6:

- a. Click **Provisioning > Manage Services**.
- b. Select **AD Service** and click **Detailed Information**.
- c. 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 AD ESSO-PG repository and is not needed for all services. See the [Schema Attribute Meta-Values](#) section of this document for more information.

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

vgoapplicationdescriptionmeta

vgocredattributelmeta

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 the credential exists on.

- d. Save changes.
- e. Repeat steps (a) to (d) for all other services that need to sync with ESSO-LM.

ITIM Express 4.6:

- a. Click **Manage Users**.
- b. Select **Create > Active Directory Profile**.
- c. 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.)
- d. 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 ESSO-PG repository and is not needed for all services. Please see the [Schema Attribute Meta-Values](#) section of this document for more information.

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

```
vgoapplicationdescriptionmeta
vgocredattributelmeta
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 the credential exists on.

- e. Click **Next**. Set the reconciliation schedule and click **Finish**.
- f. If there are additional services that need to sync with ESSO-LM, select **Create another service instance** and repeat steps (a) to (d).



ITIM and ITIM Express: For more information on the meta-value tags described in tab2, see [Schema Attribute Meta-Values](#).

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
vgoApplicationID	Literal string value (can contain root service indicator)
vgoApplicationDescription	Literal string value
vgoSSOUserIDMeta	Meta-Value
vgoAtt1Meta	Meta-Value
vgoAtt2Meta	Meta-Value
vgoApplicationUserIDMeta	Meta-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 `vGOApplicationIDMeta` 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 `vGOApplicationIDMeta` 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 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 vgo> <i>Parsed as:</i> The value of the vgo 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> <i>Parsed as:</i> 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> <i>Parsed as:</i> 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=> <i>Parsed as:</i> cn=