

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

SIM Integration and Installation Guide using the Java CLI

Release 10.1.4.1.0

E12617-01

November 2008

Oracle Enterprise Single Sign-on Provisioning Gateway SIM Integration and Installation Guide using the Java CLI,
Release 10.1.4.1.0

E12617-01

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 SIM Installation Using Java CLI	4
Audience.....	4
ESSO-PG SIM Connector	5
Component Modules	5
Installation Overview.....	6
Prerequisites	6
Installation Instructions	7
Installing the Connectors.....	7
Configuration Options	8
Appendix A: WorkflowRegistry.xml	10


About SIM Installation Using Java CLI

This guide describes how Oracle Enterprise Single Sign-On Provisioning Gateway (ESSO-PG) receives and processes provisioning requests initiated by Sun Java System Identity Manager (SIM). The integration of ESSO-PG with SIM is accomplished through a workflow extension that SIM uses to communicate with the ESSO-PG Web Service.

This workflow extension has two components, the ESSO-PG Command-Line Interface (CLI) and the SIM 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 SIM. 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.

Audience

This guide is intended for experienced application programmers responsible for the development of the Sun Java System Identity Manager. Readers are expected to understand SIM 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.

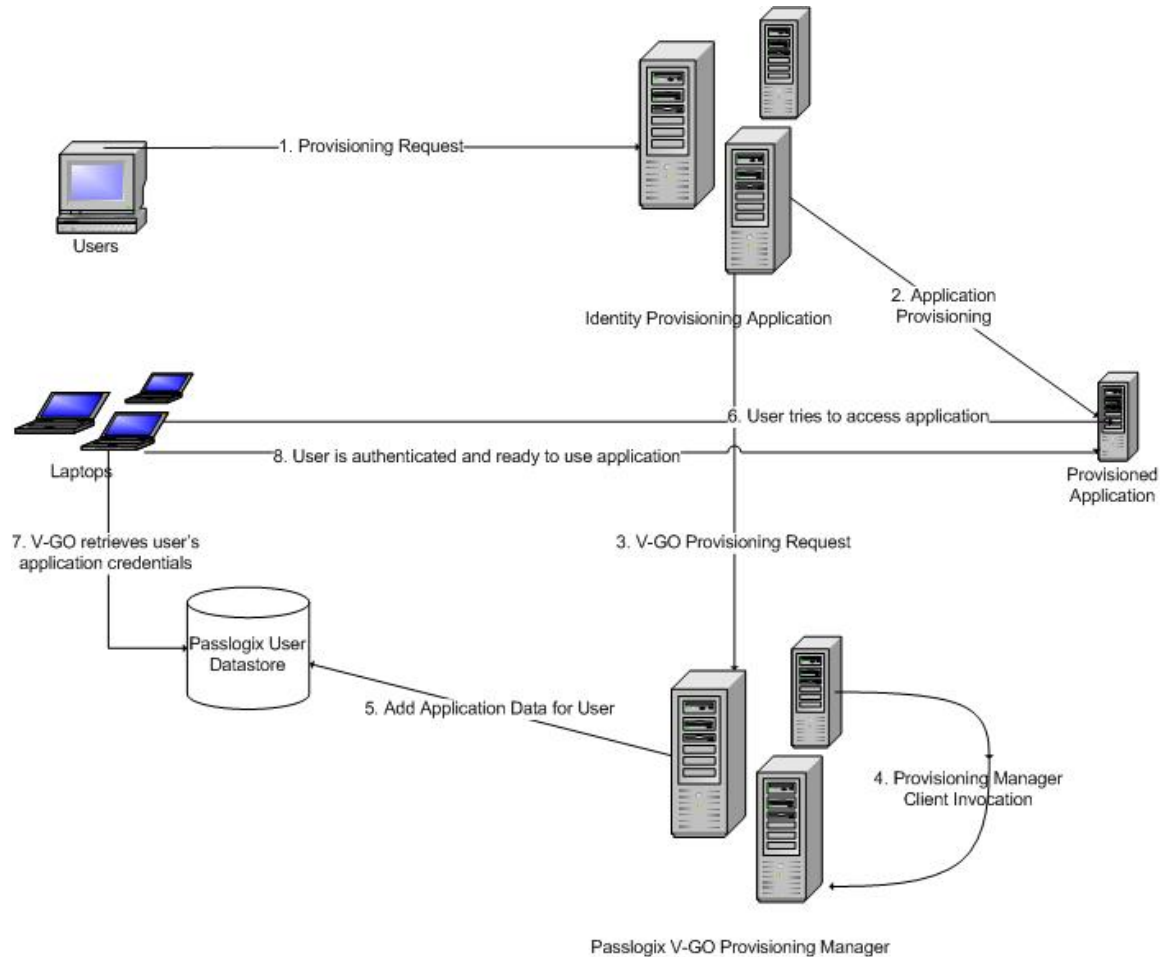
	The instructions in this guide provide an overview of the ESSO-PG SIM interface, installation instructions, and a sample integration scenario. Steps for integrating into your organization's specific workflow scenario can vary.
--	--

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

ESSO-PG SIM Connector

The ESSO-PG Java 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 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 Modules

CLI (Java Client)

The CLI is a Java-based client for the ESSO-PG Web Service. The CLI is the base component for the SIM connector. It sends the provisioning instructions to the ESSO-PG Web Service where the credentials are created and placed in the directory service. The results are then returned through the CLI to the SIM connector.

Installation Overview

This section describes installation and configuration requirements to integrate ESSO-PG with the Sun Java Systems Identity Manager:

- [Installing required prerequisites](#)
- [Installing the SIM Connector](#)
- [Configuring the v-GO PM to work with SIM](#)

Prerequisites

The ESSO-PG Server and Administrative 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 component must be installed on the system running the SIM Provisioning Workflow Interface (Connector). This will generally be the same machine that is running SIM. See the *ESSO-PG Installation and Setup Guide* for the instructions on how to install the CLI. Alternatively, components can be copied from the Libraries directory on the CD. There are two versions to provide support for Java Runtime, 1.4.2+ and 1.5.

To install the Connector, install the following components:

- Java Runtime 1.4.2 or higher
- ESSO-PG Java CLI

Installation Instructions

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

Installing the Connectors

1. Insert the ESSO-PG CD and open the `Libraries\JavaCLI` directory. There are two versions of the CLI. One for JDK 1.4.2+ and another for JDK 1.5.0+. Open the folder for the version you plan to use (1.4 or 1.5).

There are several files and folders in this directory. The main entry point is contained in `pmcli.jar` and can be started using `pmcli.bat`.

2. Copy all the jar files to the `<SIM Staging Directory>\WEB-INF\lib` directory. Files in the `Legal` directory contain the license agreements for each of these components and are not required to be copied.



All components, except `pmcli.jar`, are OSS libraries that have not been modified and can be downloaded from Apache and other OSS developers. If a version of these libraries already exists on your system, that version can be used; however, it is possible that some functionality might not work with some versions.



If you are using the Java CLI for JDK 1.4.2+, there will be an `endorsed` directory. Copy the contents of this directory to `<J2RE1.4.2_HOME>\lib\endorsed`.


3. Copy the connector, `pmsim.jar`, from the `Libraries\PMSIM` directory to the `<SIM Staging Directory>\WEB-INF\lib` directory. The version of PMSIM must be the same as the CLI version chosen.
4. Make the changes to `workflowRegistry.xml` as directed in [Appendix A](#).
5. Upload the `PasslogixUpgrade.xml` file, located on the ESSO-PG CD in the `Libraries\PMSIM\SIMUpgrade` directory, into SIM using the **Configure > Import** menu options.
6. Configure the SIM LDAP Resource definition to work in your specific environment; check values such as hostname, Bind-dn, and password.
7. Follow the [Configuration Option](#) instructions in the next section to complete setup of the SIM Connector.


Configuration Options

The SIM Connector is configured by defining the keys listed in the table below in a file named `pmsim.properties`. If values are not defined, the default value is used from the `default.properties` file stored in the `pmsim` library. This file can be extracted from the jar file and used as a template for configuration options.

To use SSL:

1. Set the `pmsim.serviceurl` key to refer to an https URL.
2. Add the SSL public certificate to the application server's trusted keystore.

	<p>If the application server (or runtime driving the connector) does not use a keystore, instead of Step 2, perform the following steps:</p> <p><i>(Warning: These steps will modify the global keystore and default hostname handler at runtime and should not be done unless you are certain it will not affect other applications running in the same instance.)</i></p> <ol style="list-style-type: none">1. Create a <code>pmcli.properties</code> file (if one does not already exist).2. Set the <code>rmi.ssl.trust.keystore.location</code> key to point to the keystore containing the SSL certificate. Refer to the <i>ESSO-PG Client CLI Guide</i> for more information on setting up SSL for the Java CLI.
---	--

	<p>The <code>rmi.ssl</code> property does not need to be set when using the Java CLI as part of the connector. Rather, the controlling Java application sets it and ensures that the SSL certificate is in the keystore. If the controlling application does not have a keystore, the <code>rmi.ssl</code> property should be set to use SSL.</p>
---	---

When using properties files, place them in a directory that is defined on the Classpath for SIM. Do not define the full path to the properties file in the Classpath, only the path to the directory it is in. The directory path name cannot contain any spaces or the classloader will not be able to find this file.

Configuration Properties	Description
<code>pmsim.serviceurl</code>	Specifies the URL for the ESSO-PG Web service. By default this is a URL on localhost. It might need to be changed for your environment.
<code>pmsim.executiontime</code>	The execution time for the instruction. This can be provided at runtime or set here for global use. If not set, the default is Now.
<code>pmsim.username</code>	The user ID needed to authenticate to the ESSO-PG Web service.
<code>pmsim.password</code>	The password that is used to authenticate to the ESSO-PG Web service.
<code>pmsim.agent</code>	The name of the service client used by the .NET client to authenticate to the v ESSO-PG Web service. This value is optional.

Appendix A: WorkflowRegistry.xml

Add the following information to the workflowRegistry.xml file, which is located in the %SIM Staging Directory%\config directory.

Add this information just above the line containing `</WorkflowRegistry>`

```
<!--
=====
  Passlogix Applications
=====-->
<WorkflowApplication name='Passlogix Credential Addition'
  class='com.passlogix.integration.provision.sim.SIMWorkflowInterface'
  op='add_credential'>
  <Comments>
    Adds an application's credential for the Passlogix SSO User.
  </Comments>

  <ArgumentDefinition name='sso_userid'>
    <Comments>
      The Passogix SSO User ID for which credential needs to be added.
    </Comments>
  </ArgumentDefinition>

  <ArgumentDefinition name='sso_application'>
    <Comments>
      The application for which account information would be added to Passlogix.
    </Comments>
  </ArgumentDefinition>

  <ArgumentDefinition name='sso_description'>
    <Comments>
      An optional description of the account.
    </Comments>
  </ArgumentDefinition>

  <ArgumentDefinition name='sso_app_userid'>
    <Comments>
      Account's User ID that will be used for authentication with the application.
    </Comments>
  </ArgumentDefinition>

  <ArgumentDefinition name='sso_password'>
    <Comments>
      Account's password that will be used for authentication with the application.
    </Comments>
  </ArgumentDefinition>

  <ArgumentDefinition name='sso_other1'>
    <Comments>
      Additional information about the account required during Login.
    </Comments>
  </ArgumentDefinition>

  <ArgumentDefinition name='sso_other2'>
    <Comments>
      Additional information about the account required during Login.
    </Comments>
  </ArgumentDefinition>

  <ResultDefinition name='command_id'>
```

```
<Comments>The Command GUID returned for the submitted command.</Comments>
</ResultDefinition>

</WorkflowApplication>

<WorkflowApplication name='Passlogix Credential Deletion'
class='com.passlogix.integration.provision.sim.SIMWorkflowInterface'
op='delete_credential'>
  <Comments>
    Deletes the application's credential for the Passlogix SSO User.
  </Comments>

  <ArgumentDefinition name='sso_userid'>
    <Comments>
      The Passogix SSO User ID for which credential needs to be deleted.
    </Comments>
  </ArgumentDefinition>

  <ArgumentDefinition name='sso_application'>
    <Comments>
      The application for which account information would be deleted from Passlogix.
    </Comments>
  </ArgumentDefinition>

  <ArgumentDefinition name='sso_app_userid'>
    <Comments>
      Account's User ID that will be used for authentication with the application.
    </Comments>
  </ArgumentDefinition>

  <ResultDefinition name='command_id'>
    <Comments>The Command GUID returned for the submitted command.</Comments>
  </ResultDefinition>

</WorkflowApplication>

<WorkflowApplication name='Passlogix Credential Modification'
class='com.passlogix.integration.provision.sim.SIMWorkflowInterface'
op='modify_credential'>
  <Comments>
    Modifies the application's credential information for the Passlogix SSO User.
  </Comments>

  <ArgumentDefinition name='sso_userid'>
    <Comments>
      The Passogix SSO User ID for which credential needs to be modified.
    </Comments>
  </ArgumentDefinition>

  <ArgumentDefinition name='sso_application'>
    <Comments>
      The application for which account information would be modified in Passlogix.
    </Comments>
  </ArgumentDefinition>

  <ArgumentDefinition name='sso_description'>
    <Comments>
      An optional new description of the account.
    </Comments>
  </ArgumentDefinition>

  <ArgumentDefinition name='sso_app_userid'>
    <Comments>
```

```
    Account's User ID that will be used for authentication with the application.
  </Comments>
</ArgumentDefinition>

<ArgumentDefinition name='sso_password'>
  <Comments>
    New Account's password that will be used for authentication with the application.
  </Comments>
</ArgumentDefinition>

<ArgumentDefinition name='sso_other1'>
  <Comments>
    New Additional information about the account required during Login.
  </Comments>
</ArgumentDefinition>

<ArgumentDefinition name='sso_other2'>
  <Comments>
    New Additional information about the account required during Login.
  </Comments>
</ArgumentDefinition>

<ResultDefinition name='command_id'>
  <Comments>The Command GUID returned for the submitted command.</Comments>
</ResultDefinition>

</WorkflowApplication>

<WorkflowApplication name='Passlogix User Deletion'
  class='com.passlogix.integration.provision.sim.SIMWorkflowInterface'
  op='delete_user'>
  <Comments>
    Deletes the Passlogix SSO User.
  </Comments>

  <ArgumentDefinition name='sso_userid'>
    <Comments>
      The Passogix SSO User ID that must be deleted.
    </Comments>
  </ArgumentDefinition>

  <ResultDefinition name='command_id'>
    <Comments>The Command GUID returned for the submitted command.</Comments>
  </ResultDefinition>

</WorkflowApplication>
>
```