Oracle® Enterprise Single Sign-on Provisioning Gateway

SIM Integration and Installation Guide

Release 11.1.1.5.0

E20985-01

March 2011

ORACLE

Oracle Enterprise Single Sign-on Provisioning Gateway SIM Integration and Installation Guide, Release 11.1.1.5.0

E20985-01

Table of Contents

Abbreviations and Terminology

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

Abbreviation or Terminology	Full Name
Administrative Console	ESSO-LM Administrative Console
Agent	ESSO-LM Logon Manager Agent
FTU	First Time Use Wizard
ESSO Anywhere	Oracle Enterprise Single Sign-on Anywhere
ESSO-PG	Oracle Enterprise Single Sign-on Provisioning Gateway
ESSO-LM	Oracle Enterprise Single Sign-on Logon Manager
ESSO-PR	Oracle Enterprise Single Sign-on Password Reset
ESSO-UAM	Oracle Enterprise Single Sign-on Universal Authentication Manager

Preface

This guide describes how the Oracle Enterprise Single Sign-on Provisioning Gateway (ESSO-PG) can receive and process 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.

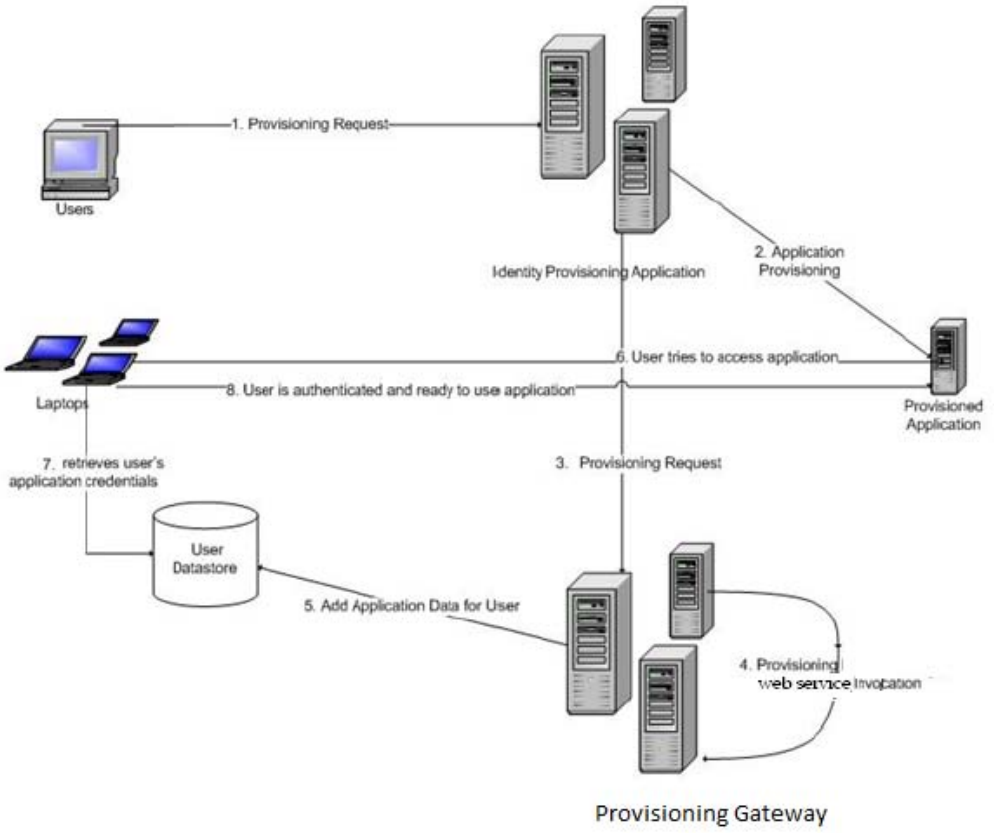
Note: The instructions in this guide provide an overview of ESSO-PG's SIM interface, installation instructions, and sample integration scenario. The steps for integration with your organizaton's specific workflow scenario may vary.

This guide is intended to serve purely as an example of how to integrate SIM 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 SIM Connector is set up to work out-of-the-box in a local environment.

Component Modules

The API Invoker uses a client-server model. The CLI does not need to be installed on the same machine as SIM. The API Invoker makes a web service call to the ESSO-PG Server and receives the response.



Installation Overview

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

Prerequisites

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

The ESSO-PG CLI components must be installed on the system that is running the SIM Provisioning Workflow Interface (Connector). If you are using the local connector, you must install SIM on the same system. See the *ESSO-PG Installation and Setup Guide* for the installation and configuration of the ESSO-PG CLI.

To install the Connector, you must install the following components:

- Java 1.4.2 or higher
- ESSO-PG CLI
- SIM 7.0 or 8.0

Installation Instructions

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

Release Structure and Package Contents

Document: contains all documents for installation.

Libraries: contains workflow extensions and schema modifications.

Scripts: contains all the scripts needed to create the sample workflow.

Resources: contains the key used in the installation.

SIM Jars: contains all the .jar files needed.

Installing the Connectors

Open the Release Package directory, which contains the following files in the SIM .jar file directory:

- axis-1.2.1.jar
- activation.jar
- axis-ant-1.2.1.jar
- bcprov-jdk13-128.jar
- commons-discovery-0.2.jar
- commons-logging-1.0.4.jar
- EncryptionTool.jar
- jaxp-api.jar
- jaxrpc.jar
- mail.jar
- opensaml-1.0.1.jar
- PMAPIInvoker_6.0.jar
- PMCLI.jar
- saaj.jar
- wss4j.jar
- wsdl4j_1.5.1.jar
- xalan.jar
- xercesImpl.jar
- xmlsec-1.3.0.jar

Note: Application server should not contain any of the files mentioned above. If it does, it should not be overridden.

Copy the .jar files listed above to the `<SIM Staging Directory>\WEB-INF\lib` directory. (The section Configuration Options should be completed before moving the .jar files.)

If the application server is **Jboss**, the following .jar files should not be copied, as they are already present in the server:

- activation.jar
- commons-logging-1.0.4.jar
- mail.jar
- xalan.jar
- xmlsec-1.3.0.jar

If the application server is **Apache Tomcat**, the following .jar files should not be copied, as they are already present in the server:

- activation.jar
- commons-logging-1.0.4.jar
- mail.jar

To complete installation, follow these steps:

1. Make the changes to `workflowRegistry.xml` as directed in Appendix A. A sample modified file is present in the Release Package/Resources folder.
2. To encrypt the VGO admin User Password, go to %SIM Staging Directory%\bin directory through command prompt. Type "lh console" and and press **Enter**. Now type "encrypt {password}" for example "encrypt sena@120". Copy the encrypted string that is returned.
3. Open the `PasslogixUpgrade.xml` file, located in the `Libraries\TIM_SIM\Extensions\SIMUpgrade` directory, using an XML reader. Replace the following values (this file is used to import the LDAP Resource that can be used to test the connector):

   vgoadmiID: Locate the following lines (**there are multiple lines**):
   <Argument name='vgoAdminID' value='OIM2\administrator'/>.
   Replace the string "OIM2\administrator" with the vgoAdminID (note that it should be in single quotes exactly as in the xml file and all instances should be replaced.

   vgoadmin Password: Locate the following lines (**there are multiple lines**):
   <Argument name='vgoadminpwd' value='EC08B38CE58D5511:-34DB4FDA:121F2228071:-7FFB|lv8F4I66e+o='/>
   Replace the string "EC08B38CE58D5511:-34DB4FDA:121F2228071:-7FFB|lv8F4I66e+o=" with the vgoAdminID Password that was obtained as in above..(Note it should be in single quotes exactly as in the xml file.

   vgoSSOApplication: Locate the word "AD Server One"(there are more than one instance).
   Replace the string "AD Server One " with the vgoSSOApplication.(Note it should be exactly as in the xml file and all instances should be replaced.
4. The LDAP resource that is imported must be configured to work in the specific environment you have set. Check the configuration information, such as hostname, Bind-dn, and password.

Follow the configuration option instructions in the next section to complete setup of the SIM Connector.

Configuration Options

This section describes how to configure ESSO-PG to work with SIM.

Modify SIM Connector Configuration File

1. Open the jar PMAPIInvoker_6.0 (located in the SIM Jars folder) and unzip it using Winzip or Winrar.
2. Go to the location `\com\passlogix\integration\provision\conf` and modify the file PMClientConfiguration.properties to add the location of the ESSO-PG server. A sample file is present in the Resources folder.
3. Compress the file again and create the .jar file with the same name (PMAPIInvoker_6.0.jar).
4. Modify the following attributes.

   javaCLI.serviceurl
   example:
   javaCLI.serviceurl=http://192.168.120.28:80/v-GO PM Service/UP.asmx

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>
```