

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

SIM Integration and Installation Guide

Release 10.1.4.1.0

E12618-01

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 SIM Integration and Installation	4
Audience.....	4
The v-GO PM SIM Connector.....	6
Component Modules	6
Installation Overview.....	8
Prerequisites	8
Installation Instructions	9
Local versus Remote Installation	9
Installing the Connectors.....	9
Configuration Options	11
Modify SIM Connector Configuration File.....	11
Appendix A: WorkflowRegistry.xml	15

About SIM Integration and Installation

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.



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

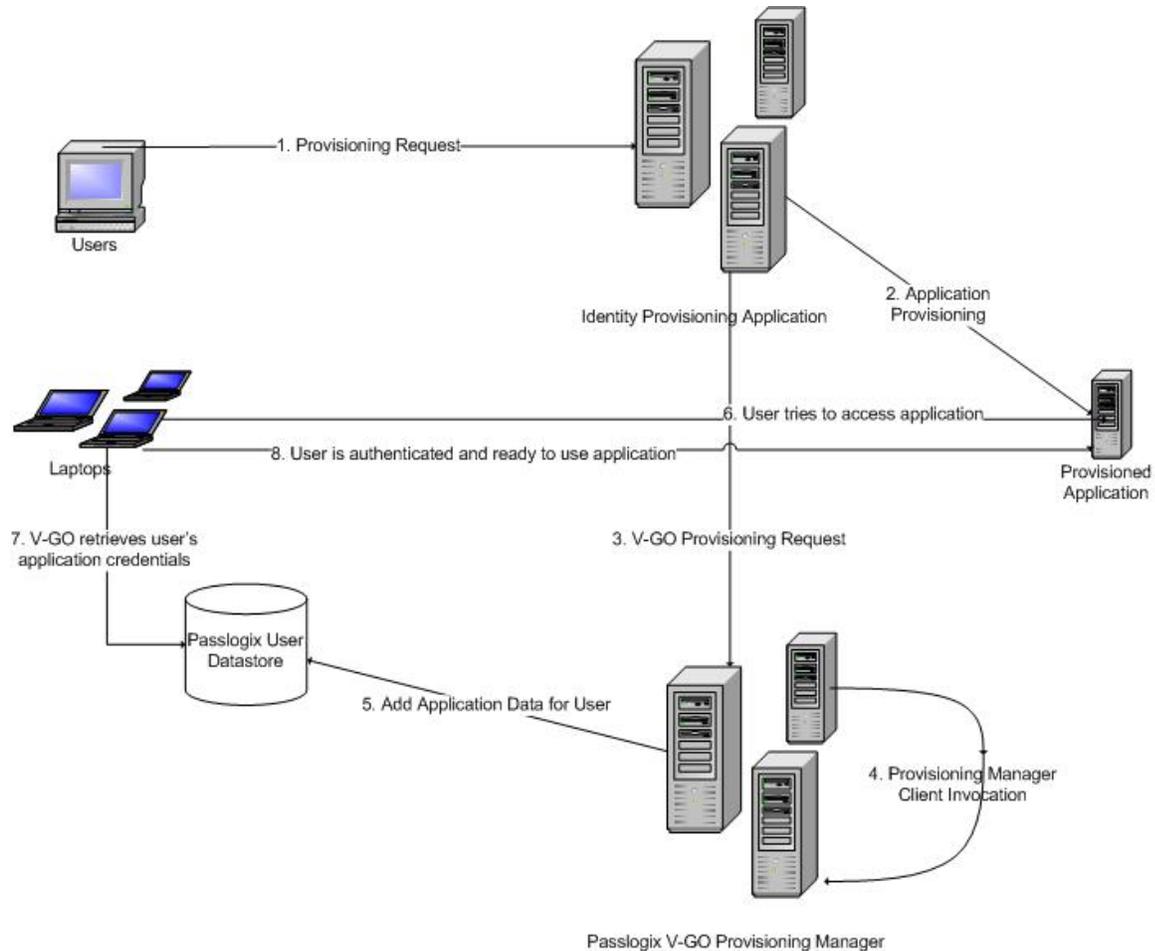
The SIM Connector is set up to work out-of-the-box in a local environment.

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

The ESSO-PG SIM 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:

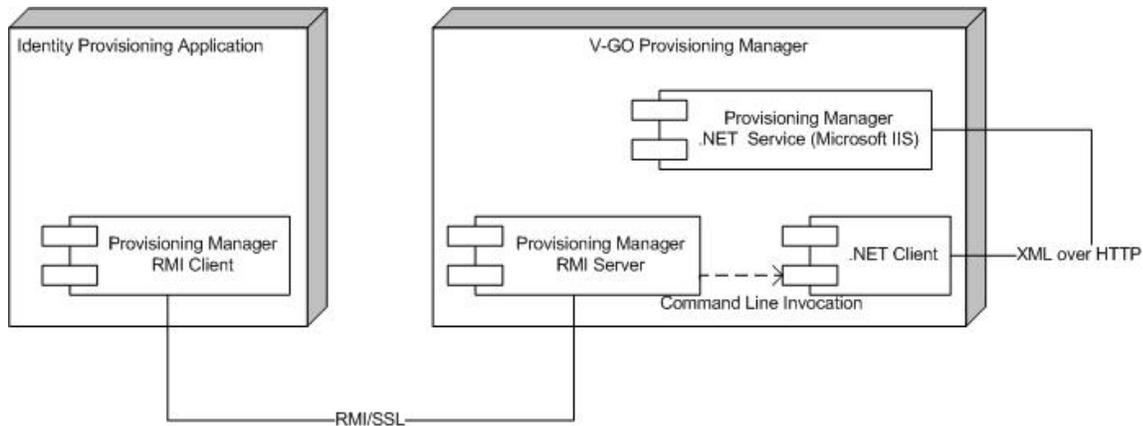


Component Modules

The CLI uses a client-server model. The CLI does not need to be installed on the same machine as SIM. If you use the Connector with RMI support (Remote Method Invocation), the CLI can exist on a Windows-based computer while SIM can run on any platform that is supported.

The RMI Connector consists of two components, the RMI Server and RMI Client. The RMI Client interfaces with SIM and sends provisioning instructions to the RMI Server via SSL (it can be disabled if needed). The RMI Server invokes the ESSO-PG CLI, which generates and executes the commands, returning the results to the caller.

Alternatively, if SIM is installed on the same machine, a local Connector can be used to communicate with the CLI. In this case, the Connector, CLI, and provisioning application must reside on the same machine. The diagram below shows the configuration of ESSO-PG CLI with an RMI Connector:



ESSO-PG RMI Client

This module resides on the same machine as the SIM provisioning application where it is invoked directly by SIM. The RMI client is a stub that passes the commands from SIM to the RMI Server over SSL. The information returned varies based on the command being invoked.

ESSO-PG RMI Server

The RMI server listens for commands from the RMI client. SSL is used to ensure secure communication between the two. Communications ports are configurable and certificates are managed through the use of certificate stores.

CLI (.NET Client)

The CLI is the .NET client for the ESSO-PG Web Service. The CLI is invoked by the RMI server. It sends the provisioning instructions to the ESSO-PG Web Service where the provisioning instructions are created and placed in the directory service. The CLI then returns the results to the RMI server, which sends a response back to the RMI client.

Installation Overview

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

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

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.

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. If you are using the remote connector, you have the option of deploying the CLI and Connector on the same system as the ESSO-PG server and v ESSO-PG Administrative Console or on a different system for separation and security. 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

Installation Instructions

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

Local versus Remote Installation

There are two types of installations for the connector:

- **Local:** In scenarios where the SIM server is deployed on a server running Microsoft® Windows® 2000 or 2003 operating system, it is possible to deploy the connector completely on that machine. In such a case the connector is deployed using the `PMCLIInvoker.jar` file, and the ESSO-PG CLI is installed on that same server.
- **Remote:** In scenarios where the SIM server is deployed on servers running an operating system other than Windows, the connector must be deployed in a distributed fashion with the `PMRMIClient.jar` file installed on the SIM server and the `PMRMIServerInvoker.jar` file, along with the ESSO-PG CLI, installed on a server running Microsoft Windows 2000 or 2003. To simplify deployment in some scenarios, this can be the same server hosting the ESSO-PG Server.

Installing the Connectors

1. Insert the ESSO-PG CD and open the `Libraries\TIM_SIM` directory, which contains the following three files:
 - `PMCLIInvoker.jar` - allows invocation of the ESSO-PG command locally.
 - `PMRMIClient.jar` - allows invocation of the ESSO-PG command locally and passes information to the RMI Server Invoker.
 - `PMRMIServerInvoker.jar` – the remote listener for the ESSO-PG RMI Client. This is installed on the same system as the CLI.
2. See the [configuration options](#) to set up the components to run in your environment.



The `PMCLIInvoker.jar` and `PMRMIClient.jar` cannot exist in the same environment. Use only one at a time for integration purposes. Otherwise, SIM might not function properly.

3. Copy the appropriate CLIENT Jar file to the `<SIM Staging Directory>\WEB-INF\lib` directory.

Perform this step *only* if you are installing the remote connector. On the machine hosting the CLI, copy the `PMRMIServerInvoker.jar` into the `v-GO PM\Client\CLI\DotNet` directory.

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\TIM_SIM\1.4\SIMUpgrade directory, into SIM using the **Configure > Import** menu options.

The SIM LDAP Resource definition must be configured to work in the specific environment you have setup. 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

The connector can be configured in both local and remote deployment scenarios via a properties file that is passed either on the command line or by the SIM provisioning application to the Connector.

```
conf_file <config_properties_filename>
```

Local Connector

The property file is passed as a name-value pair through the WorkflowContext object:

Name	Value
conf_file	<full path to SIM configuration file>

This object is passed to the SIM connector from the SIM provisioning application using the value "initializationParameter".

Remote Connector

Client

The property file is passed as a name-value pair through the WorkflowContext object:

Name	Value
conf_file	<full path to SIM configuration file>

This object is passed to the SIM connector from the SIM provisioning application using the value "initializationParameter".

Server

Start the RMI server using:

```
java -jar PMRMIServerInvoker.jar conf_file "<path to conf file>"
```

Replace *<path to conf file>* with the path.

The values specified in the `conf_file` override the default configuration properties specified under the `com.passlogix.integration.provision.conf` namespace in `PMRMIClient.jar` and `PMRMIServerInvoker.jar` class libraries.

The following table lists the properties that must be overridden in a typical deployment.

 The RMI.* configuration properties are only required in remote deployments.

Configuration Properties	Description
logger.level	<p>Used to set the level of messages that the system generates. All messages are generated on standard output by default.</p> <p> Used in ALL deployments</p>
rmi.registry.host	<p>Used to specify the hostname of the server on which the RMI registry is running. This is typically the name of the server on which RMI Server is running.</p> <p> This property needs to change in remote deployments. This is used by the RMI Client.</p>
rmi.ssl.server.keystore.location	<p>The RMI over SSL requires the availability of public or private keys that are used to set up a secure channel. The Jar files are shipped with a default key store (server.jks), but this property can be used to specify the full path of the key file, in JKS format, that is used by the client/server to establish secure SSL.</p> <p> This property needs to change in remote deployments. This is used by the RMI Client and Server.</p>
rmi.ssl.server.keystore.password	<p>The password that is used to read the key information from the store.</p> <p> This property must change in remote deployments. This is used by the RMI Client and Server.</p> <p>Specifying the value in clear text is a potential security issue. This can be addressed by passing the value at runtime through the Workflow interface.</p>

Configuration Properties	Description
<code>rmi.ssl.trust.keystore.location</code>	<p>The RMI over SSL requires the availability of trusted certificates that are used to setup a secure channel. The Jar files are shipped with a default trusted certificate store (trust.jks), but this property can be used to specify the full path of the certificate store, in JKS format, that is used by the client/server to establish secure SSL.</p> <div data-bbox="636 499 1268 627" style="border: 1px solid black; padding: 5px;">  <p>This property must change in remote deployments. This is used by the RMI Client and Server.</p> </div>
<code>rmi.registry.enabled</code>	<p>True on the RMI Server. False on the RMI client</p> <div data-bbox="636 695 1268 806" style="border: 1px solid black; padding: 5px;">  <p>This is used by the RMI Client and Server.</p> </div>
<code>rmi.ssl.trust.keystore.password</code>	<p>The password that is used to read the information from the store.</p> <div data-bbox="636 905 1268 1226" style="border: 1px solid black; padding: 5px;">  <p>This property must change in remote deployments. This is used by the RMI Client and Server.</p> <p>Specifying the value in clear text is a potential security issue. This can be addressed by passing the value at runtime through the Workflow interface.</p> </div>
<code>commandLine.serviceurl</code>	<p>The URL of the Provisioning Gateway .NET Service which is invoked by the .NET Client. This URL can be found in the server configuration file.</p> <div data-bbox="636 1360 1268 1472" style="border: 1px solid black; padding: 5px;">  <p>This property must change. This is used by the RMI Server or Local Client.</p> </div>
<code>commandLine.serviceuser</code>	<p>The user ID needed to authenticate to the Provisioning Gateway .NET Service for provisioning the ESSO-PG user.</p> <div data-bbox="636 1602 1268 1707" style="border: 1px solid black; padding: 5px;">  <p>This property must change. This is used by the RMI Server or Local Client.</p> </div>

Configuration Properties	Description
<code>commandLine.serviceuser password</code>	<p>The password that is used to authenticate to the Provisioning Gateway .NET Service for provisioning the user.</p> <div data-bbox="636 369 1268 627" style="border: 1px solid black; padding: 5px; background-color: #ffffcc;">  <p>This property must change.</p> <p>Specifying the value in clear text is a potential security issue. This can be addressed by passing the value at runtime through the Workflow interface.</p> </div>
<code>commandLine.serviceclient</code>	<p>The name of the service client used by the .NET client to authenticate to the Provisioning Gateway service.</p> <div data-bbox="636 758 1268 871" style="border: 1px solid black; padding: 5px; background-color: #ffffcc;">  <p>This is used by the RMI Server or Local Client.</p> </div>
<code>commandLine.serviceclient executable</code>	<p>The location of the .NET Command Line Executable that is invoked by the Server for the purpose of provisioning to the Provisioning Gateway.</p> <div data-bbox="636 999 1268 1165" style="border: 1px solid black; padding: 5px; background-color: #ffffcc;">  <p>This property must change only if the ESSO-PG CLI is not installed to the default installer location. This is used by the RMI Server or Local Client.</p> </div>

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 Passlogix 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 Passlogix 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 Passlogix 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>
```