Oracle
Primavera
Unifier Oracle Identity Manager (OIM) Configuration Guide

Version 20
December 2020

Contents

Using Oracle Identity Manager with Primavera Unifier 5
About Connecting Oracle Identity Manager to Primavera Unifier 5
Prerequisites Before Configuring OIM 6
Installing the OIM Application 6
Verifying System Properties 6
Updating Lookups 7
Creating a Sandbox for Non-Admin Users 7
Enabling Single Sign-On 9
Configuring OIM 9
Provisioning Users for OIM 10
Creating Users for Primavera Unifier 10
Modifying, Disabling, and Enabling OIM User's Access to Primavera Unifier 11
Setting up OIM for Bidder Integration 11
Copyright 16

Using Oracle Identity Manager with Primavera Unifier

This document assists administrators in configuring Oracle Identity Manager (OIM) to use with Primavera Unifier. OIM is an enterprise-level identity management system that centrally administers user accounts and access privileges. OIM manages the entire user identity life cycle to help your organization meet changing business and regulatory requirements and provides essential auditing, reporting, and compliance functionality.

About Connecting Oracle Identity Manager to Primavera Unifier

The OIM connector has three folders:

- **JavaTasks** has a jar file to communicate with Primavera Unifier.
- **Resources/XML** has xml files to import into OIM.
- **ThirdParty** has third party jars that the connector must use.

As an administrator, you can take advantage of the OIM connector to provision Primavera Unifier users. The OIM connector helps you administer the complete user identity life cycles of Primavera Unifier users. As a primary example, when you create a new user in OIM, it will also create a new user with the same user login name, email address, and personal name in the Primavera Unifier database.

The core attributes and operations supported by the connector are listed below.

Attributes

The following user attributes are managed:

> **Note**: OIM will provision all attributes except the password.

- Login Name
- Password
- First Name
- Last Name
- E-mail Address

Operations

The following operations are supported:

- Create User: Add a new user in Primavera Unifier via OIM.
- Modify User: Modify an attribute, such as an e-mail address, in Primavera Unifier via OIM.
- Disable User: Disable a user's access to the application via OIM.

- Enable User: Enable a user's access to the application via OIM.

Prerequisites Before Configuring OIM

Before you configure OIM with Primavera Unifier, you need to check the following in OIM:

1) Verify the System Properties.
2) Update the Lookups.
3) Create and publish a sandbox environment to hide the admin menu from non-admin users.

Installing the OIM Application

Follow the steps below to install OIM and the other applications needed to use OIM:

> **Note**: For the full list of system requirements, applications, and application version levels refer to the *Primavera Unifier Tested Configurations* in the Primavera Unifier Documentation Library.

1) Install Oracle Identity Manager (OIM). For details, refer to the *Oracle Fusion Middleware Online Documentation Library* available at: ***http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html*** (***http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html***)
2) After installing and configuring the Oracle Identity Manager Server for the first time, you must start the Oracle Identity Manager Managed Server. For details, refer to the *Oracle Fusion Middleware Online Documentation Library* available at: ***http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html*** (***http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html***)
3) Install Primavera Unifier:
   a. Verify the installation works.
   b. Open the Unifier Configurator.
   c. In the **Authentication** tab, in the User Authentication Type field, select **OIM/OAM**.

Verifying System Properties

To verify the system properties:

1) Login to **Identity System Administration** as an administrative user (for example, `xelsysadm`).
2) Depending on the OIM version that you are using, click **System Configuration** or **Configuration Properties**.
3) Locate **OIM.Provisioning** and ensure the **Value** field shows **ON**.
4) Locate **XL.EnableDisabledResources** and ensure the **Value** field shows **TRUE**.
5) Locate **XLUserResource.ProvisionMode** and ensure the **Value** field shows **JAVA**.
6) Change the default user name policy.

By default, OIM uses the email address as the user name, but Unifier does not accept special characters (like the @ symbol) in user names.

a. Locate **XL.DefaultUserNamePolicyImpl**:
b. In the **Value** field, change **oracle.iam.identity.usermgmt.impl.plugins.DefaultComboPolicy** to **oracle.iam.identity.usermgmt.impl.plugins.LastNameFirstInitialPolicy**.

Updating Lookups

To update lookups:

Click **Lookups**.

Updating **Lookup.USR_PROCESS_TRIGGERS**

1) In the **Search** window, enter **Lookup.USR_PROCESS_TRIGGERS** and click **Search**.
2) Select **Lookup.USR_PROCESS_TRIGGERS** and click on the **edit** icon.
3) In the **Edit Lookup Type** window:
   a. Click **Create Lookup Code**.
   b. In the **Meaning** field, enter **Change Email**.
   c. In the **Code** field, enter **USR_EMAIL**. Ensure it's in all caps.
   d. In the **Enabled** field, select the enabled option.
   e. Click on **Save**.

Updating **Lookup.Users.Role**

1) In the **Search** window, enter **Lookup.Users.Role** and click **Search**.
2) Select **Lookup.Users.Role** and click on the **edit** icon.
3) In the **Edit Lookup Type** window:
   a. Click **Create Lookup Code**.
   b. In the **Meaning** field, enter **Unifier Standard**.
   c. In the **Code** field, enter **Unifier Standard**.
   d. In the **Enabled** field, select the enabled option.
   e. Click on **Save**.
   f. Click **Create Lookup Code**.
   g. In the **Meaning** field, enter **Unifier Poral**.
   h. In the **Code** field, enter **Unifier Poral**.
   i. In the **Enabled** field, select the enabled option.
   j. Click on **Save**.

Click **OK** to close Lookups.

Creating a Sandbox for Non-Admin Users

The administrative user needs to hide the Administration menu from non-admin users in the Identity Self Service portal.

To hide the Administration menu:

1) Login to the Identity System Administration portal as an administrative user.
2) Select **Sandboxes**.
3) In the **Manage Sandboxes** tab, select the **Create Sandbox**.
4) In the **Create Sandbox** dialog box:
   a. In the **Sandbox Name** field, enter a name for the sandbox to identify its purpose.
   b. In the **Description** field, enter a description of the sandbox.
   c. In the **Activate Sandbox** field, select the option.
   d. Click **Save and Close**.
   e. On the confirmation message, click **OK**.
5) Logout of the Identity System Administration portal.
6) Login to the Identity Self Service portal as an administrative user.
7) Click **Sandboxes**.
8) Select the sandbox you created.
9) Select **Activate Sandbox**.

   When the sandbox activates, the sandbox link in the top right corner will show the name of the sandbox you created.
10) Select **Customize** in top right corner.
11) Go to Home Page and select **Manage** option.
12) Click the **Structure** tab from top left-corner.
13) Click on the center of the page in the **Home** tab.
14) In the **Confirm Task Flow Edit** dialog box, select **Edit**.
15) Click the **Edit** icon (Show the properties of `pgl1`) from the right-side pane.
16) In the **Component Properties: pgl1** dialog box:
   a. In the **Show Component** field, click the arrow.
   b. Select **Expression Builder**….
17) In the **Edit** dialog box:
   a. Select **Type a Value or expression**.
   b. Enter `#{oimcontext.currentUser.roles['SYSTEM ADMINISTRATORS'] != null}`.
18) Click **OK**.
19) Click **OK** again to close the **Component Properties: pgl1 dialog box**.
20) Click **Close** from top right to close the **Editing Page Identity Self Service** toolbar.
21) Select your sandbox and click on **Publish Sandbox**.
22) Click **Yes** in confirmation window.

    Your sandbox will disappear from **Manage Sandboxes**.
23) Logout of the Identity Self Service portal.
24) Login to the Identity System Administration portal as a non-admin user.
25) Verify that the Administration section is not visible.

Enabling Single Sign-On

To use OIM, ensure you have enabled Single Sign-On (SSO) and have Oracle Access Manager (OAM) and Oracle HTTP Server/Webgate managing SSO. Refer to the *Unifier Installation Guide* for more information.

Configuring OIM

Complete these steps before you begin connecting OIM and Primavera Unifier.

1) Download the current version of the **Primavera Unifier Tools** file from the Oracle Software Delivery Cloud (https://edelivery.oracle.com/).
2) Copy **OIMConnector.zip** to a local drive where you are planning to install and configure the OIM Connector.
3) Unzip the file to a local folder (this doc will use **CONNECTOR_HOME**).
4) Copy the **primavera-unifier-oim-connector.jar** (in **CONNECTOR_HOME/ JavaTasks/**) to **OIM_HOME/server/JavaTasks/**.
5) Copy all the jars from in **CONNECTOR_HOME>/ThirdParty/** to **OIM_HOME/server/ThirdParty/**.
6) Login to **Identity System Administration** as an admin user.
7) Click **Import**.
8) In the **Import Configuration** window pane on the right, click on the browser button for File To be Imported field:
   a. Go to **CONNECTOR_HOME/Resources/XML/**.
   b. Select **configuration_data.xml**.
   c. Click **Open**.
   d. Click **Next**.
9) Select the appropriate Import options for the fields: :
   a. User References
   b. Role References
   c. If Object Exists
   d. Verify the details and click on **Add File**.
   e. On the Substitution screen, click **Next**.
   f. In the **Provide IT Resource Instance Data** screen, enter the details for Primavera Unifier IT Resource and click **Next**.
   g. If you do not have any other instances, click on **Skip**.
   h. In the **Confirmation** screen, click **View Selections**.
   i. Verify the details and click **Import**.
   j. (Required) In the **Success** dialog box, click **OK** at success window and restart OIM (or the server).
   k. Close the import screen.

10) Click **Next** and review the configuration import details in the **Summary** page. If all the details are correct, click **Import**.
11) Under **Configuration**, click **Application Instances**.
12) Click the **Create** icon to create new application instance.
13) In the **Create Application Instance** screen:
    a. In the Name field, enter a name for the Primavera Unifier instance.
    b. In the Display Name field, enter the name you want to display for the Primavera Unifier instance.
    c. In the Resource Object field, select a resource object for Primavera Unifier.
    d. In the IT Resource Instance, select an IT resource instance for Primavera Unifier.
    e. Click **Save**.
14) Ensure the Catalog Synchronization job runs automatically. If it doesn't, run it manually.
15) Once the application instance completes, go to the Organization tab and add organizations to the instance if needed.

Once you have configured OIM and Unifier, you will need to provision *users* in OIM. See the following section.

Provisioning Users for OIM

Provisioning users will ensure you can manage (create, disable, modify) user's profiles through both OIM and Primavera Unifier. For more information on provisioning, see the documentation included with OIM.

> **Note**: Administrators cannot provision, update, disable, or enable *bidders* in OIM.

Creating Users for Primavera Unifier

To create users from OIM for Primavera Unifier:

1) Create an administrative user in OIM to match the Primavera Unifier administrator:
    a. Log in to OIM.
    b. Create an organization with the name **Site**.
    c. Create an Administrator user in OIM.
2) Sign in to Unifier as the Administrator that you created.
    a. Create the **ootb** company.
    b. Give the company a short name and authentication code.
3) Return to OIM:
    a. Update the **IT Resource** in OIM with the ootb information.
    b. Create an organization with the ootb short name.
    c. Create a non-admin user and assign the user to the ootb organization.

d. In the **Accounts** tab, click **Request Accounts** to provision.
e. Select the Primavera Unifier application instance you created.
f. Add the instance to the cart.
g. Click **Checkout** to provision.

Modifying, Disabling, and Enabling OIM User's Access to Primavera Unifier

Refer to the *Oracle Fusion Middleware Online Documentation Library* available at: ***http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html*** (***http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html***) for more information on creating, modifying, and removing users.

To modify or delete an OIM user's access to Primavera Unifier, follow the steps below.

To modify an account:

1) Select the user you want to modify.
2) In **User Details** page:
   a. Click **Modify User**.
   b. Update the first name, last name, user name, user type, and email address.
   c. Click **Submit**.

> **Note:** You must first change the user name in Unifier before making the change in OIM.

To disable an account:

1) Select the user you want to disable.
2) In **User Details** page, go to the **Accounts** tab.
3) Select the **Application Instance** you want to disable.
4) Click **Disable**.

To enable an account:

1) Select the user you want to enable.
2) In **User Details** page, go to the **Accounts** tab.
3) Select the **Application Instance** you want to enable.
4) Click **Enable**.

Setting up OIM for Bidder Integration

Since OIM is an enterprise-level identity management system that centrally administers user accounts and access privileges, OIM must also authenticate bidders.

Similar to Unifier users in an OIM-integrated environment, bidders can no longer change their passwords using the Unifier application interface. Bidders can only change their passwords from the OIM server, if the administrator has provided the OIM URL.

> **Note**: If an Administrator or a bidder changes the first name, last name, or email address of a *bidder* in OIM, the records will not be updated in Unifier.

During bid invitation, Unifier creates bidders in OIM regardless of the bidders status (new or existing).

> **Notes:**
>
> - Administrators cannot provision bidders in OIM.
> - Administrators cannot update, disable, or enable bidders in Unifier through OIM.

Workflow

a) Prerequisites
b) Reinstall and Reconfigure OIM Connector
c) Disable Email Uniqueness Validation in OIM
d) Import Configuration XML to create Scheduler Task
e) Create Scheduler Job and specifying parameters

Prerequisites

Ensure that you have:

- OIM and Unifier installed and configured properly.
- The latest version of OIM Connector.
- Configured OIM and imported OIM Connector.

Reinstall and Reconfigure OIM Connector

> **Note**: If you are installing the connector for the first time, you do not need to reinstall and configure the OIM connector. To continue, go to the "Disable Email Uniqueness Validation in OIM" section below.

1) Stop the **OIM** Server. (For example: WebLogic OIAMDmain - Oracle_IDM2)
2) Copy `OIMConnector.zip` to the local drive (on your PC or Server). The local drive is where you install and configure the OIM Connector
3) Unzip the zip file to local driver and name the folder (For example: `CONNECTOR_HOME`)
4) Copy `CONNECTOR_HOME/JavaTasks/primavera-unifier-oim-connector.jar` and paste to `OIM_HOME/server/JavaTasks/`
5) Copy all the `jars` from `CONNECTOR_HOME/ThirdParty/` and paste to `OIM_HOME/server/ThirdParty/`
6) Start the **OIM** Server (For example: WebLogic OIAMDmain - Oracle_IDM2)
7) Log in to Identity System Administration with admin user's credentials
8) Click **Import**.

9) Select **configuration_data.xml** (`CONNECTOR_HOME>/Resources/XML/configuration_data.xml`) to import

When the Deployment Manger - Import window opens:

1) Verify details displayed under File Preview and click **Add File**
2) Verify details displayed under Substitution and click **Cancel Substitution**
3) Verify details displayed under Primavera Unifier IT Resource and click **Cancel IT Resource Modification**
4) Verify details displayed under Current Selections

   Note: You may need to expand Primavera Unifier Resource Object and Primavera Unifier Process selections.
5) Right-click **UD_PU_USERS** and click **Remove**
6) Ensure that you see the UD_PU_USERS file in the Objects Removed From Import section on the top right-hand corner of the Deployment Manger - Import window
7) Click **Import,** wait until you see the confirmation message, and click **OK**
8) Close the Deployment Manger - Import window

Disable Email Uniqueness Validation in OIM

By default, OIM prevents two users to have the same email address (email uniqueness). To change the default setting for email uniqueness, follow these steps:

1) Log in to **Oracle Identity System Administration**
2) Depending on the OIM version that you are using, click **System Configuration** or **Configuration Properties**.
3) In the **Search System Properties** field enter ***email*** (include the asterisks, or stars)
4) Press **Enter** on your keyboard or click the right-arrow icon to begin search

If property keyword `OIM.EmailUniqueCheck` is not defined:

1) Click **Actions** and select **Create** to open the Create System Property window.
2) Provide the required system information to define a new property as follows:

- Property Name: **Whether or not email should be validated for uniqueness**
- Keyword: **OIM.EmailUniqueCheck**
- Value: **FALSE**

1) When finished, click **Perform**

If property keyword `OIM.EmailUniqueCheck` is defined:

1) In the System Configuration pane (Search System Properties) click the keyword: **OIM.EmailUniqueCheck**
2) Verify the information presented in the System Property Detail window to ensure that the Value is set to **FALSE**.
3) Click **Save** to complete changing the default setting for email uniqueness

Update Email Notification Template to Support Internationalization (Optional)

1) Log in to **Oracle Identity System Administration**.

2) Depending on the OIM version that you are using, click **System Configuration** or **Configuration Properties**.
3) Navigate to **Notification**.
4) Select a notification template you want to modify.
5) Click **Actions** >**Open** to open the template.
6) Select a language tab and modify the template for that language.
7) Click **Save**.

Import Configuration XML to create Scheduler Task

1) Log in to **Oracle Identity System Administration**
2) From the left-hand pane, click **Import** to open the Deployment Manager - Import window

At this point, the file selector window opens allowing you to select the XML file for import, by default.

> **Note**: If the file selector window does not open, click **Add** File.

1) Select the XML file to import (For example: `CONNECTOR_HOME/Resources/XML/Primavera_Unifier_Reconciliation_Task.xml`)
2) Review the details of the file that you want to import
3) Click **Add** File to add the file to the Current Selections window (For example: `Primavera_Unifier_Reconciliation_Task.xml`)
4) Click **Import** and if prompted, confirm your selection
5) When finished, click **OK** to complete the import process and close the Deployment Manager - Import window

Create Scheduler Job and specifying parameters

1) Log in to **Oracle Identity System Administration**
2) Click **Scheduler**
3) In the Search Scheduled Jobs field enter ***** (asterisk or star) and click the right-arrow icon to see the existing Scheduled Jobs
4) Click **Actions** and select **Create** to open the Create Job window
5) Enter a name in the Job Name field (For example: `Primavera_Unifier_Reconciliation_Job`)
6) Click the magnifying glass (in front of the Task field) to open the Search and Select: Scheduled Task window
7) In the Search field enter ***** (asterisk or star) and click the right-arrow icon to search and retrieve a list of all tasks
8) Click to select your desired task (For example: `Primavera_Unifier_Reconciliation_Task`) and click **Confirm** to open the Create Job window
9) Review the contents of the **Create Job** window.

Note: The Create Job window has an additional section: *Parameters*.

10) Complete the fields under Job Information, Job Periodic Settings, and Parameters, as follows:

- Start Date: Click the calendar icon and select a date (For example: `March 20, 2014 12:00:00 AM PDT`)
- Retries: (For example: `0`)
- Schedule Type: Select a desired option (For example: `Periodic`)
- Run Every: Enter a time period (For example: 5 mins)
- OIM Installation Location: (For example: `/apps/Oracle/Middleware/Oracle_IDM2`)
- OIM Server URL: (For example: `t3://slc05etq.us.oracle.com:14000`)
- OIM Admin User Name: (For example: `xelsysadm`)
- OIM Admin User Password: (For example: <password for xelsysadm user>)
- Unifier Server Protocol: (For example: `http`)
- Unifier Server Host: (For example: `host-pc2`)
- Unifier Server Port: (For example: `7001`)
- Unifier Admin Comp Short Name: (For example: `pcc`)
- Unifier Admin Comp Auth Code: (For example: <authentication code for pcc company>)

  Note: The values of the following fields are the same values as in Primavera Unifier IT Resource.

  - Unifier Server Protocol
  - Unifier Server Host
  - Unifier Server Port
  - Unifier Admin Comp Short Name
  - Unifier Admin Comp Auth Code

1) Click **Apply** to complete creating a scheduler job

Copyright

Oracle Primavera Unifier Oracle Identity Manager (OIM) Configuration Guide

Copyright © 1999, 2020, Oracle and/or its affiliates. All rights reserved.
Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software or hardware and documentation may provide access to or information on content, products and services from third-parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.