Lab 13: Configure Advanced Provisioning Infrastructure for Request based scenarios

Contents

Lab 13: Configure Advanced Provisioning Infrastructure for Request based scenarios ........................................... 1

1. Introduction .......................................................................................................................................................... 1

2. Contents ........................................................................................................................................................... 8

2.1. Configure few Important Parameters for Request oriented provisioning scenarios .................. 8

2.2. Import Request Dataset configuration into MDS ...................................................................................... 9

2.3. Setup Request UI Pre-population .................................................................................................................. 9

2.4. Setup In-line SoD check Request Validation Plugin .................................................................................... 9

2.5. Pre-Populate adapter missing when provisioning to DSEE Server ACME ........................................ 35

2.6. Setup Request Provisioning Use Case 1.2 - Contractor Requesting for DSEE Account and Role 40

2.7. Setup Request Provisioning use case 1.3 - Employee requesting for DSEE account and roles 76

2.8. Setup Request Provisioning use case 1.4 - Employee requesting for additional DSEE roles or changes to account on day 2100

2.9. Setup Request Provisioning use case 1.5 - Helpdesk Administrator requesting for DSEE account and roles 143

2.10. In-line SoD check using Request Validation ............................................................................................ 168

3. Conclusion ......................................................................................................................................................... 170

1. Introduction

This use case will cover the configurations and usage of OIM features to setup the real-life usage infrastructure for using OIM DSEE connector after it is installed, to cater to the advanced provisioning requirements for MEDICLAIM (ACME’s acquisition) Intranet user
management application, which is DSEE. The configurations would be mainly oriented around building the request based provisioning scenarios for DSEE servers of ACME. Once the infrastructure is deployed, various kinds of user communities like Employees, Contractors and their management will start using OIM driven provisioning services to request and approve accounts and entitlement in ACME DSEE instances.

Few more important facts relevant to the context:

- After acquisition MEDICLAIM has been reorganized as a BRANCH of ACME and named as Health Insurance Division. Further, this branch is divided in two - Group Insurance and Individual Insurance.

- Contractors (external users) as well as Employees (internal users) work in both these departments, and need to hold accounts in the DSEE based intranet repository. They can either use OIM self-service feature to raise requests or send emails to the IT administrators who can do it on their behalf. The IT department has a dedicated created a set of team which specially works for only handling the helpdesk calls of users of MEDICLAIM (Now ACME’s Health Insurance Division), in way affiliating them totally with this organization itself.

- MEDICLAIM (Now ACME’s Health Insurance Division) maintains THREE instances of DSEE application – DSEE Server, Johannesburg, DSEE Server, Prague and DSEE Server, Chicago.

The sections below describe the use cases to be achieved by the advanced provisioning configurations described in this lab:

1.1. Contractor requesting for DSEE account and roles

- Contractor (Assume he is already self registered, that is out of use case scope) logs into OIM self-service console and raises a request for DSEE account. While creating the request, she faces the following restrictions:

- They cannot request for others but only themselves
• Request can only be made for DSEE account (and only one resource object)

• Request can only be made for DSEE account in two DSEE instances (DSEE Server, Johannesburg and DSEE Server, Prague).

• Request dataset should not show some specific attributes (from the default dataset)

• While requesting DSEE account, only 25% DSEE roles are available in the input (instead of all which OIM would have already synched from DSEE using Lookup recon).

• Request will be routed to SOA suite. It will be assigned to an enterprise wide all-contractors’ manager. Once he approves, it moves forward. (In OIM language, this is more of a template level approval). No request level approvals, only operational levels in place.

• IF the request was filed for an account in DSEE Server, Johannesburg

• Request gets assigned to the contractor’s actual manager (as per reporting relationship stored in OIM). Manager logs in, views the request data and approves request.

• ELSE IF the request was filed for an account in DSEE Server, Prague

• Request gets assigned to the Resource Administrator (as defined in OIM). Once he logs in, can view the request data and approves request.

• Contractor gets DSEE account plus requested DSEE roles.

1.2. Employee requesting for DSEE account and roles

• Employee (Assume she/he is already in OIM, which is out of use case scope) logs into OIM self-service console and raises a request for DSEE account. While creating the request, she faces the following restrictions:
They cannot request for others but only themselves.

Request can only be made for DSEE account in two DSEE instances (DSEE Server, Johannesburg and DSEE Server, Chicago).

While requesting DSEE account, only 75% DSEE roles are available in the input (instead of all which OIM would have already synched from DSEE using Lookup recon). These would be the roles, which contractors cannot get access to and those roles which contractors can get, employees cannot.

- Request will be routed to SOA suite. No request level approvals, only operational levels in place.
- IF the request was filed for an account in DSEE Server, Johannesburg
  - Request gets assigned to the employee’s actual manager (as per reporting relationship stored in OIM). Manager logs in, views the request data and approves request.
- ELSE IF the request was filed for an account in DSEE Server, Chicago
  - Request gets assigned to the Resource Administrator (as defined in OIM). Once he logs in, can view the request data and approves request.
- Employee gets DSEE account plus requested DSEE roles.

1.3. Employee requesting for additional DSEE roles or changes to account on day 2.

- End-users Employees can log into OIM and request for additional roles on day 2, and will face restrictions as described in the two use cases mentioned above. The approval logic will be same as what was mentioned for the Employee user in the Employee use case mentioned above.
o They cannot request for others but only themselves. No request level approvals, only operational levels in place.

o Common Consideration mentioned in section 1.2 would apply.

o For 5 DSEE basic roles, which the employee should have requested the first day itself, if she is requesting on day 2, approver should request for more information before approving the request. She will then update the request to provide the requested information and then the request will get assigned back to the approver who should finally approve.

o If the approver would have requested for more information and is not satisfied with the requestor response, instead of continuing on the same loop of communication, she would delegate the approval to a specific person (OIM user) in their department, who perfectly knows how to deal with such situations and finally approve the request assessing if the need is genuine.

o If the need is found to be invalid, either the approver will reject the request or for some reasons would motivate the requestor to withdraw/close the request herself.

1.4. ACME Helpdesk Administrator requesting for DSEE account and roles

- End-users who are not confident to use the self-service can call up or send an email to the ACME Helpdesk administrators to create such requests for them.

- ACME Helpdesk administrators (special IT team formed for ACME’s Health Insurance Division) logs into OIM for creating requests for employees as well as contractors to arrange for them, DSEE account with roles. The only restriction they would face is:
- Request can only be made for DSEE account (and only one resource object).

- Bulk requests for one IT resource at a time

  - The rest of the restrictions are not in place as they are expected to know the function clearly without expecting the same from the end users.

  - To be productive, An ACME Helpdesk administrator would usually create a bulk request involving multiple users by requesting for them DSEE account plus a set of roles which are understood as the basic requirement by the business (and the intranet’s requirement). In the same request, the administrator should definitely be able to club members of both the different departments - Group Insurance and Individual Insurance.

  - Request will be routed to SOA suite. If the ACME Helpdesk administrator (Requester) is from country US then requests will be routed for Helpdesk administrator’s manager. If the ACME Helpdesk administrator is not from country US then requests will be routed for Request Level approval to DSEE Resource Administrator.

  - The logic of Operational level approvals will be actual manager of the beneficiary.

1.5. Compliant Access Request process by enforcing in-line SoD checks before Request submission

ACME employees can request a resource for themselves or for other employees. Resources are governed by Audit Objectives and Segregation of Duties (SOD) Policies.

The audit object and the resource dictate whether or not a SOD check is required and what the approval process should be if there is a violation.

ACME employees can request access to the Corporate Portal, which is driven by ODSEE. For Self, When users requests a resource for themselves, the following business rules hold true

<table>
<thead>
<tr>
<th>Resource Name</th>
<th>Audit Objective</th>
<th>SOD Required</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
In this lab, a Request Validation Plugin kicks in, when a request for resource for a user is being raised. When the user clicks on “Finish” button of the last form of Create Request Wizard from OIM Web Console, the control comes to Request Validation Plugin.

The Request Validation Plugin performs following steps to perform a SoD check:

1. Identifies whether SoD check is required or not. The decision whether SoD check is required or not is taken based on the following rules table:

<table>
<thead>
<tr>
<th>Resource Name</th>
<th>Audit Objective</th>
<th>SOD Check Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>ODSEE</td>
<td>GLB</td>
<td>Yes</td>
</tr>
<tr>
<td>Sales Dashboard</td>
<td>SOX</td>
<td>No</td>
</tr>
<tr>
<td>Secure Token</td>
<td>High Risk</td>
<td>Yes</td>
</tr>
</tbody>
</table>

2. If SoD check is required, the plugin performs the SoD check:
   a. Gets the resource name from the request data.
   b. Fetches associated Roles from the request data.
   c. Performs SoD check by verifying Role names in SoD Policies Lookup. SoD Policies lookup sample is shown below.

<table>
<thead>
<tr>
<th>Encode Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSEE Role A</td>
<td>DSEE Role B</td>
</tr>
<tr>
<td>DSEE Role A</td>
<td>DSEE Role C</td>
</tr>
<tr>
<td>DSEE Role D</td>
<td>DSEE Role C</td>
</tr>
</tbody>
</table>
2. Contents

2.1. Configure few Important Parameters for Request oriented provisioning scenarios

Purpose
This step describes the procedure to configure a pre-populate adapter on DSEE connector process form. In this procedure you will:

- Update DSEE connector resource object
- Update DSEE connector process definition

Steps

Update DSEE connector resource object

2.1.1. Launch Design console. Folder **Resource Management** → Form **Resource Object** → For the resource object **iPlanet User** → Check the checkboxes **Allow Multiple** and **Self Request Allowed** and click **Save** icon.

**Allow Multiple** flag is required if for the same OIM user we would want to provision more than one instances of resource object **iPlanet User**.

**Self Request Allowed** flag is required if for the we would want an OIM user to be able to request for resource object **iPlanet User** using OIM Self service console. Also additional relevant request templates could be configured as explained in lab <todo - provide hyperlink>
2.2 **Import Request Dataset configuration into MDS**

Collect the Request dataset package from `/odrive/dummydata/Lab 13/DSEERequestDatasets`. Open the jpr file in Jdeveloper and using “deploy” option, deploy the request dataset in OIM.

2.3 **Setup Request UI Pre-population**

Collect the Dataset Pre-population plugin package from `/odrive/dummydata/Lab 13/PrePopulationPlugins`. Open the jpr file in Jdeveloper and using “deploy” option, deploy the plugin in OIM.

2.4 **Setup In-line SoD check Request Validation Plugin**

2.4.1 **Deploy the request validation package**

Collect the In-line SoD check request validation plugin package from `/odrive/dummydata/Lab 13/ SodBasedRequestValidator`. Open the jpr file in Jdeveloper and using “deploy” option, deploy the plugin in OIM.

2.4.2 **Include in-line SoD check messages in the relevant resource bundle**

Add the below specified error messages along with the error codes in the following file:

`/odrive/oracle/oim11g_MWH/Oracle_IDM1/server/customResources/customResources_en.properties and customResources.properties`

The error messages should be added in the following format:

SODERR001=SoD Violation: {0}
SODERR002=Analyzer Class Load Error: {0}
SODERR003=OIM Read Error: {0}`
2.4.3 Verify Audit Objective

To work this asset, please verify the audit objective associated with “iPlanet User” resource. Follow the below steps to perform the same.

a) Log in into “Design Console”

![Oracle Identity Manager Design Console]

- User ID: xelsysadm
- Password: ********
- Version: 11.1.1.3.0.2.0

b) Go to “Resource Management” -> “Resource Object” and search for “iPlanet User”
c) Select “Resource Audit Objective” and verify the assign objective for resource.

d) To Assign the audit objective click on “Assign” button (Please refer above image)
e) In below image, select audit objective (Highlighted with number 1) e.g. SOX then add selected to “Assign Audit Objectives” List (Highlighted with number 2) and finally click on “Ok” button (Highlighted with number 3).

New audit objective can be added in lookup “Lookups.Resource Audit Objective.Type”
Oracle Identity Manager Design Console: connected to jdbc:oracle:thin:@orclfmw.e...

Lookup Definition

Code: Lookups.Resource Audit Objective.Type
Field: 

Lookup Type
Field Type
Required

Group

Lookup Code Information

<table>
<thead>
<tr>
<th>Code</th>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SOX</td>
<td>SOX (Hosts Financially)</td>
</tr>
<tr>
<td>2</td>
<td>HIPAA</td>
<td>HIPAA (Hosts Private)</td>
</tr>
<tr>
<td>3</td>
<td>CLB</td>
<td>CLB (Hosts Non-Public)</td>
</tr>
<tr>
<td>4</td>
<td>Quarterly Review</td>
<td>Requires Quarterly Re</td>
</tr>
<tr>
<td>5</td>
<td>Annual Review</td>
<td>Requires Annual Revi</td>
</tr>
</tbody>
</table>

Add | Delete
2.4.4 Modify Process Definition

Modify the iPlanet User Process Definition form. Follow the below steps to perform the same

a. Open design console

![Oracle Identity Manager Design Console]

b. In the “Process Management” select “Process Definition” as shown below
c. Now search for “iPlanet User” in the Process Definition form.
d. The following screen appears. In the iPlanet User form check the “Auto Save Form” option as shown below.
<table>
<thead>
<tr>
<th>Task Description</th>
<th>Default Assignee</th>
<th>Event Handler/Adaptor</th>
<th>Cond.</th>
<th>Required for Completion</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Email</td>
<td>adpi PLANETMODIFYUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change Middle Name</td>
<td>adpi PLANETMODIFYUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disable User</td>
<td>adpi PLANETMODIFYUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add Role To User</td>
<td>adpi PLANETAUTOLOGICAL</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>First Name Updated</td>
<td>adpi PLANETMODIFYUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Middle Name Updated</td>
<td>adpi PLANETMODIFYUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Attestation Event Occurred</td>
<td>adpi PLANETMODIFYUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reconciliation Insert Received</td>
<td>adpi PLANETMODIFYUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Department Updated</td>
<td>adpi PLANETMODIFYUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add User To Group</td>
<td>adpi PLANETMODIFYUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Common Name Updated</td>
<td>adpi PLANETMODIFYUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete User</td>
<td>adpi PLANETDELETEUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change User Password</td>
<td>adpi PLANETMODIFYUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change Username</td>
<td>adpi PLANETMODIFYUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remove User From Group</td>
<td>adpi PLANETMODIFYUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reconciliation Delete Received</td>
<td>adpi PLANETMODIFYUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable User</td>
<td>adpi PLANETMODIFYUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change First Name</td>
<td>adpi PLANETMODIFYUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location Updated</td>
<td>adpi PLANETMODIFYUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Move User</td>
<td>adpi PLANETMODIFYUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Account Changed</td>
<td>adpi PLANETMODIFYUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telephone Updated</td>
<td>adpi PLANETMODIFYUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization DN Updated</td>
<td>adpi PLANETMODIFYUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication Language Updated</td>
<td>adpi PLANETMODIFYUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Account Alert</td>
<td>adpi PLANETMODIFYUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Account Moved</td>
<td>adpi PLANETMODIFYUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resource Attestiation Event Occur</td>
<td>adpi PLANETMODIFYUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create User</td>
<td>adpi PLANETCREATEUSER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2.4.5 Import Lookup Codes & Request Templates

The lookup definition for the required lookup codes can be imported by importing the following file in the package using deployment manager.

- oim_objects/RequestValidationPlugin.xml
- oim_objects/RoleConflictRules.xml

Once this xml file has been imported through Deployment Manager, the following lookup codes and request templates will be created:

- Lookup.SoD.Check.Required - Lookup
- Request iPlanet User – request template
- Self Request iPlanet User – request template

To import the above files into OIM login to the advanced console of OIM and click on Import Deployment Manager File as shown below
2.4.6 Add required JAR files to project classpath

1. Open ContractorIDEventHandlerPostProc.jpr in JDeveloper.
2. Right click the project and click on Project Properties from the context menu.
3. Go to Libraries and Classpath section.

4. Add oimclient.jar file to the classpath.
5. **Oimclient.jar** is successfully added to the project.
2.4.7 Deploy the Sample

1. Open “SodBasedRequestValidator.jpr” in JDeveloper.
2. Please make sure you have OIM Customization Installer extension installed on this JDeveloper instance.
3. Select the project (SodBasedRequestValidator) in the Application Navigator.
4. Go to “Tools” -> OIM Customization Installer->Deploy
Note: Before trying to deploy any project, please make sure you have added the dependent JAR files in the project classpath and have good package folder structure in place.

2.4.8 Verify the Deployment of Lookup Codes
1. For "Lookup.Assets.Configuration"

This lookup will be used now and henceforth to maintain configuration values of various different assets.
   a. Select "Administration" -> "Lookup Definition"
b. Enter "Lookup.Assets.Configuration" and then click on search query/ binoculars in the menu bar.
c. Following search result will be displayed.
### d. Description about the table.

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>SoD.Check.Lookup.Name</td>
<td>Lookup.SoD.Check.Required</td>
</tr>
<tr>
<td>iPlanet User.SoD.Analyzers.Lookup.ClassName</td>
<td>oracle.iam.assets.sodanalyzers.OimLkuSoDAnalyzer</td>
</tr>
</tbody>
</table>
2. **For “Lookup.SoD.Check.Required”**

This lookup represents the list of Audit Objective for which SoD check is required. The LKU Code key represents the name of *Audit Objective* and LKU Decode represents the name of *Resource Object*.

Similar steps as mentioned above have to be performed, table description for this lookup is mentioned below

<table>
<thead>
<tr>
<th>Code key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>GLB</td>
<td>iPlanet User</td>
</tr>
<tr>
<td>High Risk</td>
<td>Secure Token</td>
</tr>
</tbody>
</table>


This lookup will be used to list all the SoD policies which will be used for SoD analysis. SoD policies will be nothing but conflicting roles and entitlements. Only this lookup will be used for listing all possible conflict combinations of roles/entitlements. For example, according to below example, *Group Insurance Members* Role and *Individual Insurance Members* Role are in a conflicting state and cannot be assigned together in a request.

Similar steps as mentioned above have to be performed; table description for this lookup is mentioned below

<table>
<thead>
<tr>
<th>CODE KEY</th>
<th>DECODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn=group insurance managers,ou=people, dc=mydomain, dc=com</td>
<td>cn=health information worker,ou=people, dc=mydomain, dc=com</td>
</tr>
<tr>
<td>cn=group insurance administrators,ou=people, dc=mydomain, dc=com</td>
<td>cn=group insurance claim inspectors,ou=people, dc=mydomain, dc=com</td>
</tr>
<tr>
<td>cn=group insurance administrators,ou=people, dc=mydomain, dc=com</td>
<td>cn=group insurance managers,ou=people, dc=mydomain, dc=com</td>
</tr>
<tr>
<td>cn=group insurance administrators,ou=people, dc=mydomain, dc=com</td>
<td>cn=group insurance members,ou=people, dc=mydomain, dc=com</td>
</tr>
<tr>
<td>cn=group insurance administrators,ou=people, dc=mydomain, dc=com</td>
<td>cn=group insurance administrators,ou=people, dc=mydomain, dc=com</td>
</tr>
<tr>
<td>cn=health information worker,ou=people, dc=mydomain, dc=com</td>
<td>cn=group insurance administrators,ou=people, dc=mydomain, dc=com</td>
</tr>
</tbody>
</table>
dc=mydomain, dc=com
dc=mydomain,dc=com

A row entry in this above lookup identifies two conflicting roles. If two conflicting roles are assigned together, the validation will fail and appropriate error messages will be displayed in-line.

**Note:** These roles are iPlanet Roles and not OIM Roles.

### 2.4.9 Verify the Deployment of Request Templates

1. Login to OIM Web Console

   ![OIM Web Console](image)
   
   **Sign In**
   
   User Login: xelsysadm
   
   Password: ********
   
   Sign In
   
   Forgot Password
   
   Register
   
   Track Registration

2. Go to Advanced section
iii. Click on Search Request Templates
iv. Search for the imported request templates
2.5 Pre-Populate adapter missing when provisioning to DSEE Server ACME

Note: (The pre-populate common adapter may have a problem during import. This is one way to fix it. Do this only if you run into this issue)

There might be an issue when running the provisioning in DSEE Server ACME. The Common Name field in the Custom Process Form ‘UD_IPNT_USR’ is mandatory
For any reason the adapter adpIPLANETCOMMONNAMEPPSTRING that is used to pre-populate the Common Name field is failing. Replace it with the PrepopulateFormField that we have created during a previous step for pushing the User Login value into the Common Name. For that:

2.1.2. Open the Design Console -> Development Tools -> Form Designer

2.1.3. Search "UD_IPNT_USR" Form

2.1.4. Create new Version

2.1.5. Go to Pre-Populate tab

2.1.6. Select **Common Name** and click on **Delete**

2.1.7. Click on **Add** and enter the values:

- **Field Name**: Common Name
- **Rule**: Default
- **Adapter**: PrepopulateFormField
2.1.8. Click on **Save**

2.1.9. Select the line in Adapter Variables and click on **Map**

2.1.10. Select:

- **Map To**: User Definition
- **Qualifier**: User Login

The screen should look like:

![Map Adapter Variables](image)

2.1.11. Click on **Save** and **Close**

The previous screen should look like:
2.1.12. Click on **Save** and **Close**

The Process Form should look like (don't consider the order of the lines):
Checkpoint

When executing the following Request-based use cases, the DSEE connector request dataset on the request creation UI should always get launched with pre-populated values for attributes, namely - <todo, specify the whole set here>.
2.6 Setup Request Provisioning Use Case 1.2 - Contractor Requesting for DSEE Account and Role

Purpose

In this use case, we will configure scenario described in use case 1.2. A Contractor user of ACME Health Insurance Division will use Self Service Feature and Request for DSEE Account and iPlanet Role. This use case will demonstrate the use “Self Request Resource” model and the approval levels of a request. We will demonstrate the use of template level approval and Operation level approval process for requests submitted by Contractors.

Pre-requisites

- OIM Contractor Role already exists and is called – “ACME Health Ins Contractor”
- OIM Contractor User already exists and is assigned with “ACME Health Ins Contractor” Role (CUSER1, CUSER2)
- Organization Structure for Health Insurance Division, Group Insurance, Individual Insurance already exists.
- DSEE Connector, DSEE Resource and IT Resources for 3 DSEE instances already installed and configured. DSEE Resource is “iPlanet User” and is of type LDAP Server. The 3 DSEE IT resources are “DSEE Server, Johannesburg”, “DSEE Server, Prague” and “DSEE Server, Chicago”. Creation of these IT resources has been explained in Lab 2- Install connector and extend it
- Custom workflow for “Universal Contractor Approver” called “ContractorApprovalForEBS” is already deployed and registered. This workflow assigns the approval task to pre-existing OIM user id who is the Universal Contractor Approver. The login id of Universal Contractor Approver is “CAPPROVER1” with password as “Abcd1234”.
Custom Workflow for Resource Administrator approver called “DSEEResourceAdminApproval” is already deployed and registered. This workflow assigns the approval task for DSEE Resource to a pre-existing user who is the DSEE Resource Administrator. The login id of this DSEE Resource Administrator is “RADMIN1” and password is “Abcd1234”.

Request Dataset XML file for provisioning operation on DSEE resource has been provided as part of the training environment. The file name is “ProvisionResourceiPlanet User.xml”.

In DSEE IT Resource, iPlanet Roles have been pre-populated.

Steps

Create Request Template

Create Request Template that will be used to submit Self Service Requests by Contractors for DSEE Account and Roles. We will use the “Self-Request Resource” request model to create this template and name our template as “Contractor DSEE Request”. We will use Template level approval to invoke the custom workflow that assigns the approval task to a “Universal Contractor Approver”.

2.2.1. Login in to OIM console as “xelsysadm” user or any other user that has permissions to create request templates.

2.2.2. Click Advanced to Open the OIM Advanced Administration page.

2.2.3. Click Configuration tab and then click Request Templates

2.2.4. On the left pane, from the Actions menu, select Create. Alternatively, you can click the “Create Request Template” icon on the toolbar.
2.2.5. Name the template – “Contractor DSEE Request” and choose model type as “Self-Request Resource”. For Approval process, we will use a Template level approval process and invoke a custom workflow called “ContractorApprovalForEBS”. Search and select the “ContractorApprovalForEBS” workflow. This workflow assigns the template level approval task to a “Universal Contractor Approver”. In our use case, the “Universal Contractor Approver” is a user with user id “CAPPROVER1”.
Set request template details:

**Request template basic information**

- **Request Template Name**: Contractor DSEE Request
- **Request Model Type**: Self-Request Resource
- **Description**: Request for DSEE by Contractors
- **Template Level Approval Process**: Default/Contractor Approval For EB

* = required field
2.2.6. On the “Select Allowed Resources” page, select “iPlanet User” as that is our DSEE Resource.
2.2.7. In the “Select Attributes to Restrict” page, restrict “Department”, “Server”, “NsuniqueID”.
2.2.8. On the “Set Attribute Restrictions” page, select “DSEE Server, Johannesburg” and “DSEE Server, Prague” as the 2 IT resources that Contractors can request access for.

Do not allow contractor users to enter value for “Department” and “NsuniqueID” attributes.

For server select values as shown below.
2.2.9. We will not restrict any Additional Attributes. Move to next page that is “Set Template User Roles”. In this step, we will select the role as “ACME Health Ins Contractor”. This is the role assigned to all contractors and will be used for this contractor template.
2.2.10. Review the Request Template Summary page and finish creating the request template for Contractor users.
Create Approval Policy for Request Level

Create Request Level Approval policy: We will create a Request Level policy for the “Contractor DSEE Request” request template that we created in the previous step. For this policy, we will set the approval process to “Auto Approval” as there are no request level approvals required in this use case. Refer to screen shots below for creation of this policy.

2.2.11. Go to OIM Advanced Administration page and click the “Policies” tab and then click “Approval Policies”.

2.2.12. Create a new request level policy and call it “Contr_DSEE_Pol_RL”. Set the Approval process to “Auto Approval”.
2.2.13. Add a simple approval rule called “\texttt{Contr_DSEE_Pol_RLRule}” that configures this policy for our Contractor request template. See screenshots below. Go to next page. Review the summary and finish creating this policy.
Create Operational Level Approval Policy for DSEE Johannesburg

Create Operational Level Approval Policy for DSEE Johannesburg IT Resource. Since there are 2 DSEE IT resources that a contractor can request an account for and each IT resource requires a different operation level approval, we will configure two operation level policies. This step covers the creation of operation level policy for DSEE Johannesburg IT resource.

2.2.14. Go to OIM Advanced Administration page and click the Policies tab, then click Approval Policies.

2.2.15. Create a new operational level approval policy and call it “Contr_DSEE_Pol_OL”. Select request model as “Self-Request Resource” and level as “Operation Level”. We will limit the scope to “iPlanet User” resource for this policy. Set the Approval Process to “BeneficiaryManagerApproval”.

![Create Approval Policy](image)
Create an Approval rule for this operation level policy. Add a simple rule with Entity as “Resource (New Instance data)” and Attribute “Server” equals “DSEE Server, Johannesburg”. You can name this rule as “Contr_DSEEPolRule OL”.

2.2.16. Create an Approval rule for this operation level policy. Add a simple rule with Entity as “Resource (New Instance data)” and Attribute “Server” equals “DSEE Server, Johannesburg”. You can name this rule as “Contr_DSEEPolRule OL”.
2.2.17. Review the Approval Policy information on the next screen and finish creating the policy.
Create Operational Level Approval Policy for DSEE Server, Prague

Create Operational Level Approval Policy for “DSEE Server, Prague” IT Resource. This will be the second operation level policy for contractors requesting accounts on “DSEE Server, Prague” IT resource.

2.2.18. Go to OIM Advanced Administration page and click the Policies tab, then click Approval Policies.

2.2.19. Create a new operational level approval policy and call it “Contr_DSEE_Pol2_OL”. Select request model as “Self-Request Resource” and level as “Operation Level”. We will limit the scope to “iPlanet User” resource for this policy. Set the Approval Process to “DSEEResourceAdminApproval”
2.2.20. Create an Approval rule for this operation level policy. Add a simple rule with Entity as “Resource (New Instance data)” and Attribute “Server” equals “DSEE Server, Prague”. You can name this rule as “Contr_DSEEPol2Rule2_OL”.
2.2.21. Review the Approval Policy information on the next screen and finish creating the policy. Make sure you have the Policy name, scope, approval process and rule correctly defined.

Execution of the use case - Contractor 1

*Pre-seeded data elements:* Org “Group Insurance” has a Contractor User “cuser1” (Contractor1 User1). Contractor user “cuser1” has a manager whose user id is “jdoe” (John Doe). Role for contractor user “cuser1” is “ACME Health Ins Contractor”. Password is “Abcd1234” for all users.

Contractor user **CUSER1** creates a request for account and role on “DSEE Server, Prague” IT Resource. The approval requests for all contractors have a template level approval. The template level approval is sent to Universal Contractor Approver with login id **CAPPROVER1**. Once the request is approved by **CAPPROVER1**, the request is sent for Operation level approval to DSEE Resource Administrator user with login id **RADMIN1**

2.2.22. Login to OIM console as **CUSER1**. Go to **Self Service** and click **Create Request**
2.2.23. On next screen for selecting beneficiary, select radio button **Request for Me** and click **Next** (if you select **Request for Others**, you will get a message “You are not permitted to raise request for Others”)

2.2.24. On next screen for selecting request template, select **Request Template** as **Contractor DSEE Request** and click **Next**
2.2.25. On next screen for selecting resource, put a wild card * in **Resource Name** and click Right Arrow button. **iPlanet User** appears in **Available Resources**. Select it and click right arrow to drag it to **Selected Resource**.
2.2.26. Click Next button and enter the details for the user in Resource Details as shown. Fill in all the mandatory fields. Use the Add button under Actions to add DSEE one role (group insurance members role). Pick DSEE Server, Prague (shows up as Server # 5 because of a bug) as the Server.

2.2.27. Click Next.

2.2.28. You can add justification and date information on the next page and click submit to create the request. Upon successful submission, you will get a request ID. Keep a note of this request ID.
Note: If you find any error in submitting the request (if request status is Failed), verify the following entry in approval process login in EM.

- Login to EM([http://oracle.example.com:7001/em](http://oracle.example.com:7001/em)) as weblogic/abcd1234.
- Navigate SOA \(\rightarrow\) soa-infra(Admin Server) \(\rightarrow\) default, open “ContractorApprovalForEBS[1.0]”
Click on SOA Composite, open “CallbackService_2” as shown above.

Go to “Policies” tab, open “oracle/wss11_saml_token_with_message_protection_client_policy” under “Directly Attached Policies”.

Verify “keystore.recipient.alias” value in Security Configuration Details. If the value is different from “xell”, update the value shown below.
Follow the above steps to verify other approval process “DSEEResourceAdminApproval[1.0]”.

2.2.29. Click on Request ID link to view the request details of the submitted request. Note the Contractor requests have to go through a template level approval and will always be assigned to user id CAPPROVER1 who is the Universal Contractor Approver.
2.2.30. Log out as **CUSER1** and log back in as the Universal Contractor Approver using **CAPPROVER1** log in id and “Abcd1234” as the password. Click the Tasks tab after logging in as **CAPPROVER1** user. You should see the request ID that was submitted by contractor user **CUSER1** assigned as a task.
2.2.31. Select the Request. Click **Open Task Detail**. Review and approve the request. This completes the template level approval.
2.2.32. Once Universal Contractor Approver **CAPPROVER1** has approved the request, it will be assigned to the Resource Administrator of DSEE Server Prague. The DSEE Resource Administrator user id is **RADMIN1** and password for this user is “Abcd1234”. Log in as user **RADMIN1** and check the Tasks tab. You should see the task assigned to this user.

2.2.33. Open the Request details, review it and approve it. This should complete the approval process.
2.2.34. Log back in as contractor user **CUSER1** to verify that request is completed and DSEE Resource has been provisioned.
Execution of the use case - Contractor 2

**Pre-seeded data element:** Org “Group Insurance” has a Contractor User “cuser2” (Contractor2 User2). Contractor user “cuser2” has a manager whose user id is “jdoe” (John Doe). Role for contractor user “cuser1” is “ACME Health Ins Contractor”. Password is “Abcd1234” for all users.

Contractor user **CUSER2** creates a request for account and role on “DSEE Server, Johannesburg” IT Resource. The approval requests for all contractors have a template level approval. The template level approval is sent to Universal Contractor Approver with login id **CAPPROVER1**. Once the request is approved by **CAPPROVER1**, the request is sent for Operation level approval to Contractor’s Actual Manager. In this use case, the manager of contractor user is John Doe and has a log id of **JDOE**.

2.2.35. Login to OIM console as **CUSER2**. Go to **Self Service** and click **Create Request**
2.2.36. On next screen for selecting beneficiary, select radio button Request for Me and click Next (if you select Request for Others, you will get a message “You are not permitted to raise request for Others”)

2.2.37. On next screen for selecting request template, select Request Template as Contractor DSEE Request and click Next
2.2.38. On next screen for selecting resource, put a wild card * in Resource Name and click Right Arrow button. iPlanet User appears in Available Resources. Select it and click right arrow to drag it to Selected Resource.
2.2.39. Click **Next** and enter the details for the user in **Resource Details** as shown. Fill in all the mandatory fields and use the Add button to add DSEE one role (group insurance members role). Pick DSEE Server, Johannesburg (shows up as Server # 4 because of a bug) as the Server. Click **Next**.

![Image of Resource Details form](image)

2.2.40. You can add justification and date information on the next page and click submit to create the request. Upon successful submission, you will get a request ID. Keep a note of this request ID.
2.2.41. Click on Request ID link to view the details of the submitted request. Select the request and click Open request Detail. The request should be assigned to user id CAPPROVER1 for template level approval.
2.2.42. Log out as CUSER2 and log back in as the Universal Contractor Approver using CAPPROVER1 login id and “Abcd1234” as the password. Click the Tasks tab after logging in. You should see the request ID that was submitted by contractor user CUSER2 assigned as a task.

![Image of the Task Management Screen]

2.2.43. Select the Request. Click **Open Task Detail**. Review and approve the request. This completes the template level approval.
2.2.4. Once Universal Contractor Approver has approved the request, it will be assigned to the actual manager of Contractor user **CUSER2**.

The actual manager of this contractor user has a user id **JDOE** and password for this manager is “Abcd1234”. Log in as user **JDOE** and check the Tasks tab. You should see the task assigned to this manager.
2.2.45. Open the Request details, review it and approve it. This should not complete the approval process.

2.2.46. Log back in as contractor user **CUSER2** to verify that request is completed and DSEE Resource has been provisioned.
Checkpoint
This completes configuration steps for use case described in Section 1.1. Verify that you have successfully and properly created the Request Template, Request Level Approval Policy and the two Operation Level Approval policies.

2.7 Setup Request Provisioning use case 1.3 - Employee requesting for DSEE account and roles

Purpose
In this use case, we will configure scenario described in Section 1.3. An Employee user of ACME Health Insurance Division will use Self Service Feature and Request for DSEE Account and iPlanet Role. This use case will demonstrate the use “Self Request Resource” model and the approval levels of a request. The approval process for employees is simpler and is implemented only at operation level. In this procedure, you will:

- Create Request Template that will be used to submit Self Service Requests for DSEE Account and Roles
- Create Request Level Approval Policy
- Create Operation Level Approval Policy for “DSEE Server, Johannesburg” IT Resource

Pre-requisites

- OIM Employee Role already exists and is called “ACME Health Ins Employee”
● OIM Employee User already exists and is assigned with “ACME Health Ins Employee” Role

● Organization Structure for Health Insurance Division, Group Insurance, Individual Insurance already exists.

● DSEE Connector, Resource and IT Resources for 3 DSEE instances already installed and configured

● DSEE Request Dataset XML file has already been loaded into MDS.

● Custom Workflow for “Resource Administrator” called “DSEEResourceAdminApproval” is already deployed and registered. This workflow assigns the approval task for DSEE Resource to a pre-existing user with user id “radmin1” and password “Abcd1234”.

● DSEE Roles have already been pre-populated.

**Steps**

Create Request Template that will be used to submit Self Service Requests for DSEE Account and Roles

We will use the “Self-Request Resource” request model to create this template and name our template as “Employee DSEE Request”.

2.3.1. Login in to OIM console as “xelsysadm” user or any other user that has permissions to create request templates.

2.3.2. Click Advanced to Open the OIM Advanced Administration page.

2.3.3. Click Configuration tab and then click Request Templates
2.3.4. On the left pane, from the **Actions** menu, select **Create**. Alternatively, you can click the “Create Request Template” icon on the toolbar. Name the template – “**Employee DSEE Request**” and choose model type as “**Self-Request Resource**”. We do not need a template level approval for this use case.

![Create Request Template](image)

2.3.5. On the “**Select Allowed Resources**” page, select “**iPlanet User**” as that is our DSEE Resource.
2.3.6. On the Attributes to Restrict page, select “Server”, “NsuniqueID”. 
2.3.7. On the “Set Attribute Restrictions” page, select “DSEE Server, Johannesburg” and “DSEE Server, Chicago” as the 2 IT resources that Employees can request access for. Do not allow employee users to enter value for “NsuniqueID” attribute.
2.3.8. We will not restrict any Additional Attributes and move to next page. On the "Set Template Users Role" page, select the role that all employees will be assigned to and this role is called “ACME Health Ins Employee”.
2.3.9. Review the summary page and finish creating the template.

Create Request Level Approval Policy

We will create a Request Level policy for the “Employee DSEE Request” request template that we created in the previous step. We will call this request level policy as “Emp_DSEE_Pol_RL” and the type will be “Self-Request Resource”. For this policy, we will set the approval process to “Auto Approval” as there are no request level approvals required in this use case.
2.3.10. Go to OIM Advanced Administration page and click the Policies tab and then click Approval Policies.

2.3.11. Create a new request level policy and call it “Emp_DSEE_Pol_RL”. Set the Approval process to “Auto Approval”.

2.3.12. Add a simple approval rule called “Emp_DSEE_Pol_RLRule” that configures this policy for our Employee request template. The rule will look like what is shown in screen shot below.
2.3.13. Review the Summary page for the Request level policy and finish creating the policy.
Create Operation Level Approval Policy for “DSEE Server, Johannesburg” IT Resource

Since there are 2 DSEE IT resources that an employee can request an account for and each IT resource requires a different operation level approval, we will configure two operation level policies. This step covers the creation of operation level policy for DSEE Johannesburg IT resource.

2.3.14. Go to OIM Advanced Administration page and click the Policies tab, then click Approval Policies.

2.3.15. Create a new operation level policy and call it “Emp_DSEE_Pol_OL”. Request Type is “Self-Request Resource” and level is “Operation Level”. Select Resource as “iPlanet Resource” for scope. Approval Process will be “BeneficiaryManagerApproval”.

![Image of Create Approval Policy page]
2.3.16. On the next page, create a Rule with name as “Emp_DSEE_Pol_OLRule” and add a simple rule as shown in the screen shot below.
2.3.17. Review the summary page and finish creating the first operation level policy.
Create a second operational level approval policy

Name it “Emp_DSEE_Pol2 OL”. This second policy is being created for requests that are submitted for “DSEE Server, Chicago” IT Resource.

Go to OIM Advanced Administration page and click the Policies tab, then click Approval Policies.

Create a Operation Level Approval Policy and name it as “EMP_DSEE_Pol2 OL”. Request Type is “Self-Request Resource” and Level is “Operation Level”. Scope is “iPlanet User” resource. Approval Process for this policy is “DSEEResourceAdminApproval” which is our custom workflow.
2.3.18. On the next page, create a Rule name – “Emp_DSEE_Pol2_OLRule”. Add a simple rule for “DSEE Server, Chicago” as shown below.
2.3.19. Review the Approval Policy Summary page and finish creating the policy.

![Image of Create Approval Policy screen]

**Execution of the use case - Employee 1**

*Pre-seeded data elements:* Org “Group Insurance” has Users “euser1” (Employee1 User1). Employee user “euser1” has a manager whose user id is “jdoe” (John Doe). Role for employee user “euser1” is “ACME Health Ins Employee”. Password is “Abcd1234” for all users.

Employee user EUSER1 requesting DSEE Server, Chicago account and role. The approval process is simple in case of requests raised by employees. Only operation level approval process is used. The approval requests submitted by employees for Chicago DSEE server instance are sent for approval to DSEE Resource Administrator with log in id **RADMIN1**.
2.3.20. Login to OIM console as EUSER1. Go to Self Service and click Create Request

2.3.21. On next screen for selecting beneficiary, select radio button Request for Me and click Next (if you select Request for Others, you will get a message “You are not permitted to raise request for Others”)
2.3.22. On next screen for selecting request template, select **Request Template** as **Employee DSEE Request** and click **Next**.

![Select Request Template](image1)

2.3.23. On next screen for selecting resource, put a wild card * in **Resource Name** and click Right Arrow button. **iPlanet User** appears in **Available Resources**. Select it and click right arrow to drag it to **Selected Resource**.

![Select Resources](image2)

2.3.24. Click **Next** button and enter the details for the user in **Resource Details** as shown. Fill in the mandatory fields. Add a DSEE Role. Server to be picked up is Server #6 (DSEE Server, Chicago). Click **Next**.

![Resource Details](image3)
2.3.25. You can enter justification if any and click **Finish**. Successful submission of request is confirmed and a Request ID is generated.
2.3.26. Click on Request ID link to view the submitted request. Select the request and click Open request Detail. You can further click Approval tasks to see where the request has gone. In this case since we selected server 6 (Chicago), the request went to DSEE Resource Admin RADMIN1.

2.3.27. Click on Profile -> My Profile -> Resources and see that this user has access to no resource yet.
2.3.28. Log off as **EUSER1** and Log back in as **RADMIN1**. Click on **Tasks** -> **My Tasks** -> **Approvals** and you will see the request created previously is waiting here for approval. Select the request and click **Approve Task**. Alternatively you can click Open tasks Detail, review the details and then decide to approve or take any other action.

![Task Approval Interface](image)

2.3.29. Log off as **RADMIN1** and Log back in as **EUSER1**. Click **Requests** -> **My Requests** and you will see that your request is now completed.

![Request Details](image)
2.3.30. Also Click on Profile -> My Profile -> Resources and you will see resource iPlanet User is provisioned to the user EUSER1.

Execution of the use case - Employee 2

Employee user EUSER2 will be requesting for DSEE Server, Johannesburg account and role. Only difference in this case from previous is that the request goes to the requester’s (same as beneficiary in this case) actual manager and not to Resource Administrator. The manager in this use case is John Doe with login id JDOE
2.3.31. Repeat the above process from 3.2.1 by logging in as EUSER2. Submit a Request using Employee DSSE Request template. In the Resource Details section, fill in the mandatory fields and request for access to Server #4 (DSEE Server, Johannesburg). Request for a DSEE Role. See screen shot below.
2.3.32. After submitting the request you will see in Request Detail that request went to JDOE in this case who is the manager of the requester (beneficiary). In 3.2.1 it went to RADMIN1

![Request Details](image)

2.3.33. Log off as EUSER2 and login as JDOE to approve the request.
2.3.34. Login as **EUSER2** user to verify the provisioning request has been completed.
Checkpoint

This completes configuration steps for use case described in Section 1.2. Verify that you have successfully and properly created the Request Template, Request Level Approval Policy and the two Operation Level Approval policies.

2.8 Setup Request Provisioning use case 1.4 - Employee requesting for additional DSEE roles or changes to account on day 2

Purpose

In this use case, we will configure use case described in 1.3. One Day 2, one Employee user of ACME Health Insurance Division will use Self Service Feature and Request for additional changes to his/her DSEE Account and iPlanet Role. In this use case, we will use the “Self Modify Provisioned Resource” Request Model. Since this is a different Request Model, we will need a new XML request dataset file for the DSEE resource. We will use a request dataset file called “ModifyResource|Planet User.xml” that is created for modify provisioned resource operation. Since there are 2 IT resources that an employee can request changes for, we will create two separate Request Templates one for each IT resource and then corresponding Request and Operation level policies.

Pre-requisites

- OIM Employee Role already exists and is called – “ACME Health Ins Employee”

- OIM Employee User already exists and is assigned with “ACME Health Ins Employee” Role

- Organization Structure for Health Insurance Division, Group Insurance, Individual Insurance already exists.

- DSEE Connector, Resource and IT Resources for 3 DSEE instances already installed and configured
- DSEE Request Dataset XML file “ModifyResourceiPlanet User.xml” for modify provisioned resource will be provided in training environment.

- OIM user with DSEE IT Resource provisioned already exists.

- Custom Workflow for “Resource Administrator” called “DSEEResourceAdminApproval” is already deployed and registered. This workflow assigns the approval task for DSEE Resource to a pre-existing user with user id “radmin1” and password “Abcd1234”.

**Steps**

Upload DSEE Request dataset file “ModifyResourceiPlanet User.xml”.

This dataset XML file for DSEE resource will be provided to you in your training environment.

**NOTE:** The steps below to upload dataset may not be needed if you already have finished uploading both the Request dataset files for DSEE resource in Section 2.4.1. Perform the steps below only if you have not imported both the request dataset files as part of Section 2.4.1.

2.4.1. The import location from where MDS utility will import the XML file is defined as “metadata_from_loc” property in “OIM_ORACLE_HOME/server/bin/weblogic.properties” file. Under this import location, you have to create a directory structure as required by the utility to place the request dataset XML files. In our example, copy the DSEE Request dataset XML file to “/home/oracle/reqdata/custom/iplanet/” directory. Refer to screen shots below.
2.4.2. Set environment variable **OIM_ORACLE_HOME**. In our environment, we will set it as follows:

```bash
export OIM_ORACLE_HOME=/odrive/oracle/oim11g_MWH/Oracle_IDM1
```

2.4.3. Run the import utility “**weblogicImportMetadata.sh**” to import the dataset into MDS. The import utility will prompt you to enter the username, password and OIM Admin Server t3 URL. Enter the user name as “weblogic” and this user’s password.
Create Request Template that will be used to submit Self Modify Provisioned Requests for DSEE Account and Roles.

We will use the "Self-Modify Provisioned Resource" request model to create this template and name our template as “Modify DSEE Johannesburg Account”.

2.4.4. Login in to OIM console as “xelsysadm” user or any other user that has permissions to create request templates.

2.4.5. Click Configuration tab and then click Request Templates

2.4.6. On the left pane, from the Actions menu, select Create. Alternatively, you can click the “Create Request Template” icon on the toolbar. Name the template – “Modify DSEE Johannesburg Account”.
2.4.7. On Select Allowed Resources page, select “iPlanet User”.
2.4.8. On Select Attributes to Restrict page, select “Server”, “NSuniqueID” as the attributes.
2.4.9. Restrict the IT resources by just selecting “DSEE Server, Johannesburg” IT Resource as we are creating template for this resource only.
2.4.10. On Set Template User Roles page, select “ACME Health Ins Employee” role.
2.4.11. Review the Request Template summary and finish creating the Request template for Johannesburg Resource.
Create a second Request Template that will be used to submit Self Modify Provisioned Resource for DSEE Account and Roles.

We will use the “Self-Modify Provisioned Resource” request model to create this template and name our template as “Modify DSEE Chicago Account”.

2.4.12. Login in to OIM console as “xelsysadm” user or any other user that has permissions to create request templates.

2.4.13. Click Configuration tab and then click Request Templates

2.4.14. On the left pane, from the Actions menu, select Create. Alternatively, you can click the “Create Request Template” icon on the toolbar. Name the template – “Modify DSEE Chicago Account”.

![Create Request Template](image.png)
2.4.15. On Select Allowed Resources page, select “iPlanet User”.

2.4.16. On Select Attributes to Restrict page, select “Server”, “NSuniqueID” as the attributes.
2.4.17. Restrict the IT resource by selecting “**DSEE Server, Chicago**” IT Resource as we are creating template for this resource. Limit the roles by selecting all except for 4 roles as shown in the screen shot below.
2.4.18. On Set Template User Roles page, select “ACME Health Ins Employee” role.
2.4.19. Review the Request Template summary page and finish creating the Request template for Chicago Resource.

Create Request Level Policy for “Modify DSEE Johannesburg Account” request template
2.4.20. Go to OIM Advanced Administration page and click the Policies tab, then click Approval Policies.

2.4.21. Create a new request level policy and call it “Modify_DSEE_Joh_Pol_RL”. Request Type is “Self Modify Provisioned Resource” and level is “Request Level”. Select Resource as “iPlanet Resource” for scope. Approval Process will be “Auto Approval”.

2.4.22. Create a Simple Rule called “Modify_DSEE_Joh_Pol_RLRule” like shown below.
2.4.23. Review the Approval Policy summary page and finish creating the policy.
Create Operation Level Policy for “Modify DSEE Johannesburg Account” request template.

2.4.24. Go to OIM Advanced Administration page and click the Policies tab, then click Approval Policies.

2.4.25. Create a new operation level policy and call it “Modify_DSEE_Joh_Pol_OL”. Request Type is “Self Modify Provisioned Resource” and level is “Operation Level”. Select Resource as “iPlanet Resource” for scope. Approval Process will be “BeneficiaryManagerApproval”.

![Image of Create Approval Policy interface]

- In the Search and Select: Approval Process section, select the appropriate approval process.
- In the Basic Information section, enter the following details:
  - Policy Name: Modify_DSEE_Joh_Pol_OL
  - Request Type: Self Modify Provisioned Resource
  - Level: Operation Level
- Set the Resource as iPlanet Resource.
2.4.26. Create a Simple Rule as shown below and call it “Modify_DSEE_Joh_Pol_OLRule”
2.4.27. Review the Approval Policy summary page and finish creating the policy.
Create Request Level Policy for “Modify DSEE Chicago Account” request template.

2.4.28. Go to OIM Advanced Administration page and click the Policies tab, then click Approval Policies.

2.4.29. Create a new request level policy and call it “Modify_DSEE_Chicago_Pol”。 Request Type is “Self Modify Provisioned Resource” and level is “Request Level”. Select Resource as “iPlanet Resource” for scope. Approval Process will be “Auto Approval”.

2.4.30. Create a Simple Rule called “Modify_DSEE_Chicago_Pol_Rule” as shown below.
2.4.31. Review the Approval Policy summary page and finish creating the policy.
Create Operation Level Policy for “Modify DSEE Chicago Account” request template.

2.4.32. Go to OIM Advanced Administration page and click the Policies tab, then click Approval Policies.

2.4.33. Create a new operation level policy and call it “Modify_DSEE_Chicago_Pol OL”. Request Type is “Self Modify Provisioned Resource” and level is “Operation Level”. Select Resource as “iPlanet Resource” for scope. Approval Process will be “DSEEResourceAdminApproval” which is a custom workflow.
2.4.34. Create a Simple Rule called “Modify_DSEE_Chi_PolOLERule” as shown below.
2.4.35. Review the Approval Policy summary page and finish creating the policy.
Execution of the use case - Employee 1

Pre-seeded data elements: Org “Group Insurance” has a Employee User “euser1” (Employee User1). Employee user “euser1” has a manager whose user id is “jdoe” (John Doe). Role for employee user “euser1” is “ACME Health Ins Employee”. Password is “Abcd1234” for all users.

Employee user EUSER1 already has a DSEE account on DSEE Server, Chicago and 1 role as part of use case 3.2. Employee user EUSER1 now creates a request using “Modify DSEE Chicago” request template. This template is used for requesting changes to an existing account. The user requests for one additional DSEE role. The request will go for approval and approver will request for more information from the requester. The requester EUSER1 will provide that information and request will be resubmitted to Approver. Approver will look at the information provided and approve the task. Employee user EUSER1 will log back in and verify additional role has been assigned.

Login to OIM console as EUSER1. Go to Self Service and click Create Request
2.4.36. On next screen for selecting beneficiary, select radio button **Request for Me** and click **Next** (if you select **Request for Others**, you will get a message "You are not permitted to raise request for Others")

2.4.37. On next screen for selecting request template, select **Request Template** as **Modify DSEE Chicago Account** and click **Next** button.
2.4.38. On next screen for selecting resource, put a wild card * in **Resource Name** and click Right Arrow button. **iPlanet User** appears in **Available Resources**. Select it and click right arrow to drag it to **Selected Resource**.

2.4.39. Click **Next** and the details for the user in **Resource Details** will be already populated as shown since **EUSER1** already has an account.

Click **Add** button and add 1 more DSEE Role. See screen shot below. Click **Next**.
2.4.40. You can add justification and date information on the next page and click submit to create the request. Upon successful submission, you will get a request ID. Keep a note of this request ID.

2.4.41. Click on **Request ID** link to view the request details of the submitted request. The request is sent to Resource Administrator with user id **RADMIN1** for approval.
2.4.42. Log out as EUSER1 and log back in as user RADMIN1 and “Abcd1234” as the password. Click the Tasks tab after logging in as RADMIN1 user. You should see the request ID that was submitted by EUSER1 assigned as a task.
2.4.43. Open the task details and click the **Request More Information** link. In the **Request More Information** window, fill in the Details and request for more information from **Requester**. Submit the Request. The task is sent back to Requester for additional information.
2.4.44. Log out as **RAADMIN1** and log back in as **EUSER1**. Look under Tasks tab and you should see the request for more information assigned to **EUSER1**.

2.4.45. Select the task and click **Open Task Detail** link. In the Additional Request Information section, enter the Response. Use the **Submit to Approver** button to re-submit the request to Approver.
2.4.46. The request with the additional information submitted by USER1 is sent back for approval to RADMIN1. Logout and then back in as RADMIN1 user and check the Request Comments tab of the request. At this point, RADMIN1 will accept and approve the request.
2.4.47. Log out as **RADMIN1** and log back in as **EUSER1** and verify that request to modify account has completed.
2.4.48. Click the **Open Resource Details** link under **My Profile -> Resources** section to verify that second DSEE role has now been added.

**Execution of the use case - Employee 2**
**Pre-seeded data elements:** Org “Group Insurance” has a Employee User “euser2” (Employee2 User2). Employee user “euser2” has a manager whose user id is “jdoe” (John Doe). Role for employee user “euser2” is “ACME Health Ins Employee”. Password is “Abcd1234” for all users.

Employee user **EUSER2** already has a DSEE account on **DSEE Server, Johannesburg** and 1 role as part of use case 3.2. Employee user **EUSER2** now creates a request using **“Modify DSEE Johannesburg”** request template. This template is used for requesting changes to an existing account. The user requests for one additional DSEE role. The request will go for approval to Employee Manager **JDOE**. Employee Manager **JDOE** will look at the information provided and re-assign the task to another user with login id **JFISHER**. The task will be re-assigned and now show up in tasks list of user **JFISHER**. The new Approver **JFISHER** will reject the task and provide the information to requester. Employee user **EUSER1** will log back in and see that request for additional role has been rejected with reason for rejecting the request.

2.4.49. Login to OIM console as **EUSER2**. Go to **Self Service** and click **Create Request**
2.4.50. On next screen for selecting beneficiary, select radio button **Request for Me** and click **Next** (if you select **Request for Others**, you will get a message “You are not permitted to raise request for Others”)

2.4.51. On next screen for selecting request template, select **Request Template** as **Modify DSEE Johannesburg Account** and click **Next**
2.4.52. On next screen for selecting resource, put a wild card * in Resource Name and click Right Arrow button. iPlanet User appears in Available Resources. Select it and click right arrow to drag it to Selected Resource.

2.4.53. Click Next and the details for the user in Resource Details will be already populated as shown since EUSER2 already has an account. Click Add button and add 1 more DSEE Role. See screen shot below. Click Next.

2.4.54. You can add justification and date information on the next page and click submit to create the request. Upon successful submission, you will get a request ID. Keep a note of this request ID.

2.4.55. Click on Request ID link to view the request details of the submitted request. The request is sent to Employee Manager with user id JDOE for approval.
2.4.56. Log out as EUSER2 and log back in as user JDOE and “Abcd1234” as the password. Click the Tasks tab after logging in as JDOE user.

You should see the request ID that was submitted by EUSER2 assigned as a task.
2.4.57. Open the task details and click the **Re-Assign** link.

2.4.58. In the **Re-Assign Task** window, search for user **John Fisher**. Select **John Fisher** as the User to whom the task will be re-assigned. Click **Re-Assign** button.
2.4.59. Log out as JDOE and log back in as JFISHER. Look under Tasks tab and you should see the request from EUSER2.
2.4.60. Select the Task and click **Reject Task** link. This will open up the Reject Task window. Enter the reason for rejecting the task. Click **Reject** button.
Log out as JFISHER and log back in as EUSER2 and check the requests tab. The request for additional role will be in a status of “Operation Approval Rejected” and the Request Comments tab will show the comments why the task was rejected.
Checkpoint

This completes configuration steps for use case described in Section 1.1.3. Verify that you have successfully and properly created the Request Template, Request Level Approval Policy and the two Operation Level Approval policies.
2.9 Setup Request Provisioning use case 1.5 - Helpdesk Administrator requesting for DSEE account and roles

Purpose
In this use case, we will configure scenario described in Section 1.4. This use case will demonstrate the bulk provisioning capability by Helpdesk Administrators using Provision Resource model. Request level approvals will be based on country of the Helpdesk Administrator. If Helpdesk Administrator submitting the request is from US, the request will be routed to Organization Administrators for approval. If the Helpdesk Administrator is from a country other than US, the requests level approval will be sent to DSEE Resource Administrator.

Pre-requisites
- OIM Helpdesk Role already exists and is called “ACME Help Desk Administrators”
- OIM Organization Administrators for Group Insurance already exists – “Group Ins Org Administrators”
- OIM Organization Administrators for Individual Insurance already exists – “Individual Ins Org Administrators”
- OIM Users assigned to above three roles already exist.
- DSEE Connector, Resource and IT Resources for 3 DSEE instances already installed and configured
- DSEE Request Dataset XML file for modify provisioned resource will be provided
- Custom Workflow for “Resource Administrator” called “DSEEResourceAdminApproval” is already deployed and registered. This workflow assigns the approval task for DSEE Resource to a pre-existing user with user id “radmin1” and password “Abcd1234”.
Steps
Create Request Template that will be used by ACME Helpdesk Administrators to submit Provisioning Requests for DSEE Account and Roles.

We will use the “Provision Resource” request model to create this template and name our template as “ACME Help Desk DSEE Provision”.

2.5.1. Login in to OIM console as “xelsysadm” user or any other user that has permissions to create request templates. Click Configuration tab and then click Request Templates.

2.5.2. On the left pane, from the Actions menu, select Create. Alternatively, you can click the “Create Request Template” icon on the toolbar. Name the template – “ACME Help Desk DSEE Provision” and use model as “Provision Resource”. There is no Template level Approval process needed for this use case.
2.5.3. On “Select Allowed Resources” page, search and select “iPlanet User” resource.

2.5.4. On the “Select Attributes to Restrict” page, restrict “Server” and “NsuniqueID” attributes.
2.5.5. On the “Set Attribute Restrictions” page, select all 3 DSEE IT resources as the Helpdesk administrators can submit requests for both contractors and employees. There are no additional attributes on “Set Additional Attributes” page.
2.5.6. Since Helpdesk Administrators belong to “ACME Health Desk Administrators” role, we will select this role on the “Set Template User Roles” page.
2.5.7. Review the Request Template Summary page and finish creating the Request template.
Create Request Level Policy

This use case requires 2 Request level policies. We will create the first request level policy in this step and call it “Helpdesk_DSEE_Pol1_RL”

2.5.8. Go to OIM Advanced Administration page and click the Policies tab, then click Approval Policies.

2.5.9. Create a new request level policy and call it “Helpdesk_DSEE_Pol1_RL”. Request Type is “Provision Resource” and level is “Request Level”. Approval Process will be “RequestorManagerApproval!1.0”.
2.5.10. Create a Simple Rule on “Set Approval Rule and Component” page. Name the rule as “Helpdesk_DSEE_Pol1_RLRule”. The rule will for requester’s (Helpdesk Admin) Country attribute to find whether the country is US or not.
2.5.11. Review the Approval Summary page and finish creating the first request level policy.
Create Second Request Level Policy

This use case requires 2 Request level policies. We will create the first request level policy in this step and call it “Helpdesk_DSEE_Pol2_RL”.

2.5.12. Go to OIM Advanced Administration page and click the Policies tab, then click Approval Policies.

2.5.13. Create a new request level policy and call it “Helpdesk_DSEE_Pol2_RL”. Request Type is “Provision Resource” and level is “Request Level”. Approval Process will be “DSEEResourceAdminApproval”.

2.5.14. Create a Simple Rule on “Set Approval Rule and Component” page. Name the rule as “Helpdesk_DSEE_Pol2_RLRule”. The rule will for requester’s (Helpdesk Admin) Country attribute to find whether the country is US or not.
2.5.15. Review the Approval Summary page and finish creating the first request level policy.

Create Operation Level Policy – For this use case, at operation level we will send the approval to Beneficiary Manager.

We will use the OOTB workflow for this. We will create the first request level policy in this step and call it “Helpdesk_DSEE_Pol OL”
2.5.16. Go to OIM Advanced Administration page and click the Policies tab, then click Approval Policies.

2.5.17. Create a new operation level policy and call it “Helpdesk_DSEE_Pol OL”. Request Type is “Provision Resource” and level is “Operation Level”. Approval Process will be “BeneficiaryManagerApproval” and Scope = iPlanet User.

2.5.18. Create a Simple Rule on “Set Approval Rule and Component” page. Name the rule as “Helpdesk_DSEE_Pol_OLRule”. The rule will check the Request template name.
2.5.19. Review the Approval Summary page and finish creating the first request level policy.

2.7.5 Execute Use Case - Helpdesk IT Admin from US
**Pre-seeded data elements:** Following users have been pre-seeded to be used in the execution of this use case

<table>
<thead>
<tr>
<th>First Name</th>
<th>Last Name</th>
<th>User ID</th>
<th>Manager</th>
<th>Organization</th>
<th>User Type</th>
<th>Role</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Helpdesk1</td>
<td>Manager1</td>
<td>hmanager1</td>
<td>ACME CAPITAL</td>
<td>Full-Time Empl oyee</td>
<td></td>
<td></td>
<td>US</td>
</tr>
<tr>
<td>Helpdesk1</td>
<td>User1</td>
<td>huser1</td>
<td>hmanager1</td>
<td>ACME CAPITAL</td>
<td>Full-Time Empl oyee</td>
<td>ACME Help Desk Administrators</td>
<td>US</td>
</tr>
<tr>
<td>GrpInsurance1</td>
<td>User1</td>
<td>GIuser1</td>
<td>JDOE</td>
<td>Group Insurance</td>
<td>Empl oyee</td>
<td>ACME Health Ins Employee</td>
<td></td>
</tr>
<tr>
<td>IndInsurance1</td>
<td>User1</td>
<td>IIuser1</td>
<td>JDOE</td>
<td>Individual Insurance</td>
<td>Empl oyee</td>
<td>ACME Health Ins Employee</td>
<td></td>
</tr>
</tbody>
</table>

Helpdesk Administrator **huser1** will raise a bulk request for users **GIuser1** and **IIuser1**, to get them provisioned with the DSEE server account (plus few DSEE roles). As the country of **huser1** is **US**, the whole bulk request will go to **hmanager1** for approval, as
he is huser1’s manager. Once approved, the request will break down into child requests and which will then be queued up for Operational level approvals to JDOE, who is the manager of the actual beneficiaries Gluser1 and IIuser1.

Similar behavior would be witnessed when the huser2 will raise a bulk request for users Gluser2 and IIuser2. The only difference observed would be the request level approval, which will get assigned to DSEE Resource administrator radmin1 because huser2 country is not US but UK.

2.5.20. Login to OIM console as HUSER1. Go to Self Service and click Create Request

2.5.21. On next screen for selecting beneficiary, select radio button Request for others and click Next (you will not get a message “You are not permitted to raise request for Others” as obtained on all previous request self service use cases because as a helpdesk
administrator, you have the role **ACME Help Desk Administrators** which is having the privileges over the Request template **ACME Help Desk DSEE Provision** that is based on a **Provision Resource** request model).

2.5.22. On next screen for selecting request template, select **Request Template** as **ACME Help Desk DSEE Provision** and click Next button.

2.5.23. On next screen for selecting users, specify a search filter **First Name Equals *insurance*+ and click Search.
2.5.24. From the search results, choose the users as shown in the screenshot below. Finally click Next.

**Note:** If help desk user may not be able to search users, fix is provided in Appendix 3.
2.5.25. On next screen for selecting resource, click Right Arrow button. **iPlanet User** appears in **Available Resources**. Select it and click right arrow to drag it to **Selected Resource**.

2.5.26. Click **Next**. **Resource Details** screen would be launched with the request dataset. As you can see that unlike the previous cases of requesting for iPlanet Resource account through self service, on this page very few fields will be available. None of the single user context specific fields like **First Name**, **Password** etc are shown. The reason is the request datasets, which we are using have all such fields marked as **available-in-bulk = "false"**. The fields which are shown here are only those which have **available-in-bulk = "true"** in the request dataset. So all the user context related information (like **First Name**, **Password** etc) will be pre-populated directly (by the already configured pre-populate adapters) in the process form before provisioning kicks off.
2.5.27. Fill in the data as shown in the screenshot, including the DSEE roles that should get assigned to both the users.

2.5.28. Click Next.

![Screenshot of request form]

2.5.29. Leave out justification and date information on the next page and click submit to create the request. Upon successful submission, you will get a request ID. Keep a note of this request ID.

2.5.30. Click on Request ID link to view the request details of the submitted request. The request is sent to Heldesk Administrator with user id HMANAGER1 for approval. This is exactly as we had configured in the request level approval policy for Helpdesk administrators with country US.
2.5.31. Log out as **HUSER1** and log back in as user **HMANAGER1** and “Abcd1234” as the password. Click the Tasks tab. You should see the request ID that was submitted by **HUSER1** assigned as a task. The beneficiary details will show **Multiple Users**, which is what you get in the case of a bulk request.
2.5.32. Clicking on the Request ID will show more details about the beneficiaries, resource data requested etc. At this point, **HMANAGER1** will accept and approve the request by clicking **Approve Task**.

2.5.33. Log out as **HMANAGER1** and log back in as **HUSER1** and verify that the original parent request is now in state Operation Initiated and new child requests have been spawned with state Obtaining Operational Approval. Request level approval has completed plus operational level approvals have been kicked off for the new child requests created for each of the beneficiaries. Feel free to open the new request instances and check the relevant data elements involved.
2.5.34. If you check both the child requests, they will be assigned for operational level approval to the beneficiaries’ manager for each of the case, which is JDOE for both. This is exactly as we had configured in the operational level approval policy.
2.5.35. Logout as HUSER1 and log in as JDOE. You would find both the approvals in the Tasks tab. Approve both these requests by selecting them one by one and clicking Approve Task.
2.5.36. Logout as JDOE and log in as HUSER1. Try to Search Requests. The parent bulk as well child individual requests should be in a state Request Completed.

2.7.6 Execute Use Case - Helpdesk IT Admin from UK

*Pre-seeded data elements*: Following users have been pre-seeded to be used in the execution of this use case.
<table>
<thead>
<tr>
<th>First Name</th>
<th>Last Name</th>
<th>User ID</th>
<th>Password</th>
<th>Manager</th>
<th>Organization</th>
<th>User Type</th>
<th>Role</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource1</td>
<td>Admin1</td>
<td>RADMIN1</td>
<td>Abcd1234</td>
<td></td>
<td>ACME CAPITAL</td>
<td>Full-Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Helpdesk2</td>
<td>User2</td>
<td>huser2</td>
<td>Abcd1234</td>
<td></td>
<td>ACME CAPITAL</td>
<td>Full-Time</td>
<td></td>
<td>UK</td>
</tr>
</tbody>
</table>
Detailed steps with screenshots have not been provided for execution of this use case because the procedure is exactly same as above (section 2.7.5). Helpdesk Administrator huser2 will raise a bulk request for users GIuser2 and IIuser2, to get them provisioned with the DSEE server account (plus few DSEE roles). As the country of huser1 is UK, the whole bulk request will get assigned to DSEE Resource administrator radmin1 because huser2 country is not US but UK. It is unlike the previous case where the request level approval was assigned to hmanager1 (huser1’s manager). Once approved, the request will break down into child requests and which will then be queued up for Operational level approvals to JDOE, who is the manager of the actual beneficiaries GIuser2 and IIuser2.

**Checkpoint**
This completes configuration steps for use case described in Section 1.5. Verify that you have successfully and properly created the Request Template, 2 Request Level Approval Policies and one Operation Level Approval policy.

### 2.10 In-line SoD check using Request Validation

Below screen appears if conflicting roles (highlighted in Section 2.4, *Lookup.SoD.iPlanet User.Conflict.Rules*) are requested by the user.
3. Conclusion

In this lab, you accomplished the following:

- Learnt how to import request dataset thru MDS
- Learnt how to create request configurations - Request templates, Approval Policies
- Learnt how to create requests and approve them

Product Features that you have learnt

- Access Policies
- Request Datasets with pre-population
- Request templates
- Approval Policies

Related features that you should explore further

- Attach notifications to various Request stages
Appendix:

1. Create Access Policy UI behaves strangely (Page 24). This was observed in OIM 11gR1.
   - Use “Skip All forms” button and then at the end iPlanet User shows twice. Just reverify DSEE Server ACME was set and “Save”.

2. Follow the steps below to make sure Server names instead of server ids show up when users request a resource. This is accomplished by editing the IT Resource (example, Manage IT Resource>DSEE Server ACME> Click Edit) and provide Read access for the IT Resource to the various ACME* Roles used in the labs.

   The first screenshot shows what you have to end up with. The second screenshot onwards shows the detailed steps. Repeat these for all DSEE Server instances.
### IT Resource Administration - Update Permissions

You can view additional information about this IT resource: Administrative Roles.

**IT Resource Name:** [Oracle Server, Pingdom]

Filter by Role Name: Filter Role

<table>
<thead>
<tr>
<th>Administrative Role</th>
<th>Display Name</th>
<th>Read Access</th>
<th>Write Access</th>
<th>Delete Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>REPORT ADMINISTRATORS</td>
<td>REPORT ADMINISTRATORS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PLUGIN ADMINISTRATORS</td>
<td>PLUGIN ADMINISTRATORS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SPM1_App_Role</td>
<td>SPM1_App_Role</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SOD ADMINISTRATORS</td>
<td>SOD ADMINISTRATORS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>USER_NAME_ADMINISTRATORS</td>
<td>USER_NAME_ADMINISTRATORS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ACME Health Plan Coordinator</td>
<td>ACME Health Plan Coordinator</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Update | Reset | Next | Last

Back to Search Results
OIM 11g Workshop - Lab 5
### Results 1 to 8 of 8

<table>
<thead>
<tr>
<th>Administration Role</th>
<th>Display Name</th>
<th>Read Access</th>
<th>Write Access</th>
<th>Delete Access</th>
<th>Assign</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACME Help Desk Administrators</td>
<td>ACME Help Desk Administrators</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>OPERATORS</td>
<td>OPERATORS</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>ALL DEPART</td>
<td>ALL DEPARTS</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>SHEL OPERATORS</td>
<td>SHEL OPERATORS</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>ACME Help Inc Contractor</td>
<td>ACME Help Inc Contractor</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>ACME Help Inc Employee</td>
<td>ACME Help Inc Employee</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Health Information Worker</td>
<td>Health Information Worker</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Mid Worker</td>
<td>Mid Worker</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
</tr>
</tbody>
</table>

Assign
### IT Resource Administrative Roles

You can view additional information about the IT resource: Administrative Roles.

**IT Resource Name:** USER server, Images

**Filter By Role Name:**

Results 1-10 of 26

<table>
<thead>
<tr>
<th>Administrative Role</th>
<th>Display Name</th>
<th>Read Access</th>
<th>Write Access</th>
<th>Delete Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Administrators</td>
<td>System Administrators</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Identity User Administrators</td>
<td>Identity User Administrators</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Identity Organization Administrators</td>
<td>Identity Organization Administrators</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Role Administrators</td>
<td>Role Administrators</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Records Administrators</td>
<td>Records Administrators</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Reconciliation Administrators</td>
<td>Reconciliation Administrators</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Attestation Event Administrators</td>
<td>Attestation Event Administrators</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Access Policy Administrators</td>
<td>Access Policy Administrators</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Approval Policy Administrators</td>
<td>Approval Policy Administrators</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Attestation Configuration Administrators</td>
<td>Attestation Configuration Administrators</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Administrative Role</td>
<td>Display Name</td>
<td>Read Access</td>
<td>Write Access</td>
<td>Delete Access</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------------</td>
<td>-------------</td>
<td>--------------</td>
<td>---------------</td>
</tr>
<tr>
<td>SYSTEM ADMINISTRATORS</td>
<td>SYSTEM ADMINISTRATORS</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>IDENTITY USER ADMINISTRATORS</td>
<td>IDENTITY USER ADMINISTRATORS</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>IDENTITY ORGANIZATION ADMINISTRATORS</td>
<td>IDENTITY ORGANIZATION ADMINISTRATORS</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>ROLE ADMINISTRATORS</td>
<td>ROLE ADMINISTRATORS</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>REQUEST ADMINISTRATORS</td>
<td>REQUEST ADMINISTRATORS</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>RECONCILIATION ADMINISTRATORS</td>
<td>RECONCILIATION ADMINISTRATORS</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>ATTESTATION EVENT ADMINISTRATORS</td>
<td>ATTESTATION EVENT ADMINISTRATORS</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>ACCESS POLICY ADMINISTRATORS</td>
<td>ACCESS POLICY ADMINISTRATORS</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>APPROVAL POLICY ADMINISTRATORS</td>
<td>APPROVAL POLICY ADMINISTRATORS</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>ATTESTATION COMPLIANCE ADMINISTRATORS</td>
<td>ATTESTATION COMPLIANCE ADMINISTRATORS</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Administrative Role</td>
<td>Regular Name</td>
<td>Read Access</td>
<td>Write Access</td>
<td>Delete Access</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------</td>
<td>-------------</td>
<td>--------------</td>
<td>---------------</td>
</tr>
<tr>
<td>REPORT ADMINISTRATORS</td>
<td>REPORT ADMINISTRATORS</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>PLUG-IN ADMINISTRATORS</td>
<td>PLUG-IN ADMINISTRATORS</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>CNM_APP Role</td>
<td>CNM_APP Role</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>SOC ADMINISTRATORS</td>
<td>SOC ADMINISTRATORS</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>USER NAME ADMINISTRATOR</td>
<td>USER NAME ADMINISTRATOR</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>ACME Health Ins Controller</td>
<td>ACME Health Ins Controller</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

Results 21 of 26

Update  Cancel

Back to Search Results
3. ACME Help desk users when they want to request resources for others may not be able to search for the other users. This is fixed by creating the appropriate Authorization Policy as shown below.