ORACLE
Insurance

# Oracle Insurance Data Gateway

## Installation Guide

Version 1.0

Oracle Insurance Data Gateway Installation Guide

Release 1.0

Part # E93105-01

Library# E93054-01

January 2018

Contributing Authors: Kiran Yeruva, Mark Taylor, Vishal Pratap

ORACLE
Insurance

# CONTENTS


**Preface** ..... **5**
- **Audience** ..... **5**
- **Conventions** ..... **5**
- **Documentation Accessibility** ..... **5**
- **Customer Support** ..... **5**
- **Contact** ..... **6**
- **Follow Us** ..... **6**

**Getting Started** ..... **7**
- **Release Download** ..... **7**
- **System Prerequisites** ..... **7**
- **Database Configuration** ..... **8**
  - OIDG Database Schema Creation ..... 8
  - RCU (Infra) Schemas Creation ..... 8

**OIDG Installation Requirements** ..... **10**
- **Base Path and Java Home Update** ..... **10**
- **Folder Structure and Release Files Maintenance** ..... **10**
  - Folder structure: ..... 10

**Input Parameters for OIDG Installation** ..... **13**
- **OIDG Parameter Configuration Steps** ..... **13**
  - Linux User/Group Section ..... 13
  - Database Section ..... 14
  - Middleware Section ..... 15
  - Confirmation Section ..... 16
  - Credentials Section ..... 16
  - Confirmation ..... 17

**OIDG Pre-Script Installation** ..... **18**

**OIDG Installation Manual Steps** ..... **19**
- **Defining JNDI Providers** ..... **19**
- **Creating Security Policies** ..... **20**

**OIDG Post-Script Installation** ..... **23**

**Deploying ACORD_AML Libraries** ..... **24**

**OIDG Release Upgrade** ..... **26**
- **OIDG Release Upgrade Pre-Requisite** ..... **26**
  - OIDG Release Deployment / Un-Deployment Process ..... 27
  - OIDG Release Un-Deployment Process ..... 29
  - OIDG Release Deployment Process ..... 29

**Setting Up the Enterprise Scheduler Service Jobs ..... 31**
**Configuring Daily Error Log ..... 37**
**Updating OIDX.Properties file ..... 39**
**Email Configuration for Notifications ..... 40**
**Acquiring mail server SSL certificate ..... 40**
Importing the mail server SSL certificate into keystore ..... 41
Synchronizing certificates from central store to local file instance ..... 43
**Configuring Workflow Notification Properties ..... 43**
**Configuring Email Driver Properties ..... 45**
**Troubleshooting ..... 47**
Verifying Trust Keystore ..... 48
Reviewing the WebLogic start script ..... 48
**OIDG GnuPG Encryption and Decryption ..... 49**
**Verifying GnuPG-Agent ..... 49**
**Generating GnuPG Key ..... 49**
Exporting and Importing secret sub keys ..... 51
Trusting the keys ..... 52

ORACLE Insurance

# PREFACE

Welcome to the Oracle Insurance Data Gateway (OIDG) Installation Guide. This guide describes installation and configuration steps for the OIDG application.

## Audience

This guide is intended for users who will be deploying OIDG.

## Conventions

The following text conventions are used in this document:

| Convention | Description |
|---|---|
| **bold** | **Bold type indicates information you enter.** |
| ***italic*** | *Italic type indicates emphasis or placeholder variables for which you supply particular values.* |
| `monospace` | `Monospace type indicates commands, code in examples, and text that appears on the screen.` |

## Documentation Accessibility

This documentation may contain links to websites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Websites.

## Customer Support

If you have any questions about the installation or use of our products, please call +1.800.223.1711 or visit the My Oracle Support website:

http://www.oracle.com/us/support/index.html

Go to My Oracle Support to find answers in the Oracle support knowledge base, submit, update or review your service requests, engage the My Oracle Support Community, download software updates, and tap into Oracle proactive support tools and best practices.

Hearing impaired customers in the U.S. who need to speak with an Oracle Support representative may use a Telecommunications Relay Service (TRS). Information about TRS is available at http://www.fcc.gov/cgb/consumerfacts/trs.html

A list of phone numbers is available at http://www.fcc.gov/cgb/dro/trsphonebk.html. International hearing-impaired customers should use the TRS at 1.605.224.1837.

## Contact

USA: +1.800.223.1711
Canada: 1.800.668.8921 or +1.905.890.6690
Latin America: 877.767.2253

For other regions including Latin America, Europe, Middle East, Africa, and Asia Pacific regions:
Visit: http://www.oracle.com/us/support/contact/index.html

## Follow Us

 https://blogs.oracle.com/insurance

 https://www.facebook.com/oracleinsurance

 https://twitter.com/oracleinsurance

 https://www.linkedin.com/groups?gid=2271161

# GETTING STARTED

Please follow this document closely while installing or upgrading to the OIDG.

| NOTE | Any missing configuration may lead to an inappropriate setup. |
|---|---|

## Release Download

Download the OIDG release zip file from the Oracle Software Delivery Cloud and extract into a local folder.

## System Prerequisites

Following system setup is required before moving further with this documentation.

| Name | Version | Notes |
|---|---|---|
| **Oracle WebLogic Server** | 12.2.1.0.x | |
| **Oracle SOA Suite** | 12.2.1.0.x | |
| **Oracle Java SE 8** | 1.8.x | |
| **Oracle Database Server** | 12.1.0.2.0 | |
| **GnuPG** | 2.2.1 | https://www.gnupg.org/ |
| **Chef** | 12.6.0 | Download compatible Chef package for your Operating System from the below URL. https://downloads.chef.io/chef/stable/12.6.0 |
| **ACORD® AML libraries** | | Download ACORD AML libraries |

ORACLE Insurance

# Database Configuration

## OIDG Database Schema Creation

A database schema needs to be created on a new database when OIDG is installed for the first time.

Follow these steps to setup a new tenant database schema:

1. Connect to the OIDG DB or PDB with SYSDBA privilege.

2. Create a table space to hold data for the OIDG schema.

   SQL command:

   ```
   Create tablespace OIDX datafile '[filepath
   location/filename.dbf]' size 500M autoextend on;
   ```

3. Run **\AML Engine\Database\Installation\OIDG_PDB_SYSDBA.sql**
   Make sure to rename the schema owner name, password, and table space name before applying the script.

4. Connect as the schema owner user.

5. Run **\AML Engine\Database\Installation\SCI001_OIDG_B?_Schema.sql** to create the DB schema.

   **Note:** "?" Denotes the build number which needs to be installed.

Follow these steps to migrate the database schema for OIDX from previous builds to the current version:

1. Connect as the schema owner user and apply all the migration scripts in the **AML Engine\Database\Migration** folder to update the DB components **if the migration scripts have not been applied**. To see if a migration script has been applied or not, exam the rows in the DBHISTORY table.

   Make sure the scripts are applied in the order of the build numbers.
   For example, if the current OIDG build is 1, and has to be upgraded to build 3, then you should upgrade to **SCU00?_OIDG_B1ToB2.sql** and **SCU00?_OIDG_B2ToB3.sql**.

   **Note:** "?" Denotes the serial number of the script file.

## RCU (Infra) Schemas Creation

Create the pre-requisite Oracle SOA Infrastructure RCU schemas according to the product documentation provided with Oracle SOA Suite.

**Note**:

The RCU prefix, user, and common password defined during RCU setup will also be needed for OIDG product installation.

Do not use special characters **[!'@#\$%^\&*()**_**+*]** in the RCU prefix name.

Chapter – 2

# OIDG INSTALLATION REQUIREMENTS

This chapter includes following topics:

- Base Path and Java Home Update
- Folder Structure and Release Files Maintenance

## Base Path and Java Home Update

Please refer to the following steps for OIDG script update:

1. Go to the **OIDG-1.0-automation\chef\cookbooks\fsgbu_oidx_base\attributes** and update the following properties in **default.rb**
2. Update the user home base path for the Linux user (used for FMW installation)

   ```
   default['fsgbu_oidx_base']['base_home'] = '/scratch'
   ```

   ```
   # FSGBU base variables
   default['fsgbu_oidx_base']['base_home'] = '/scratch'
   ```

   This path is combined with the username you entered during installation. It will be recognized as the “user home base bath”, **Example**: /scratch/username (or) /u01/username

3. Update the JAVA home path

   ```
   default['fsgbu_oidx_base']['java_home'] = '/usr/java/jdk1.8.0_144'
   ```

   ```
   # Java attributes
   default['fsgbu_oidx_base']['java_home'] = '/usr/java/jdk1.8.0_144'
   ```

## Folder Structure and Release Files Maintenance

Create the following folder structure inside the user base path to maintain release files.

### Folder structure:

/<user home base>/Chef/OIDG_1.0/

#### Example:

/u01/Chef/OIDG_1.0/

Copy the following files from the OIDG release package to
**/<user home base>/Chef/OIDG_1.0/**

- /AdminView/AdminView.ear
- /AdminView/AdminView.properties
- /DataSrv/OIDX_POC_DSL.ear
- /Portal/IDXPORTAL.ear
- /PrcOrch/OIDX_PrcOrch_cfgplan.xml
- /PrcOrch/sca_OIDX_PrcOrch.jar
- /QuickView/QuickView.ear
- /QuickView/QuickView.properties
- /ResultProcessing/sca_ResultProcessing.jar
- /ResultProcessing/ResultProcessing_cfgplan.xml
- /SrvVirt/log4j-api-2.9.1.jar
- /SrvVirt/log4j-core-2.9.1.jar
- /SrvVirt/OSBCoreCustomizationFile.xml
- /SrvVirt/SVCore_SrvVirt.sbar

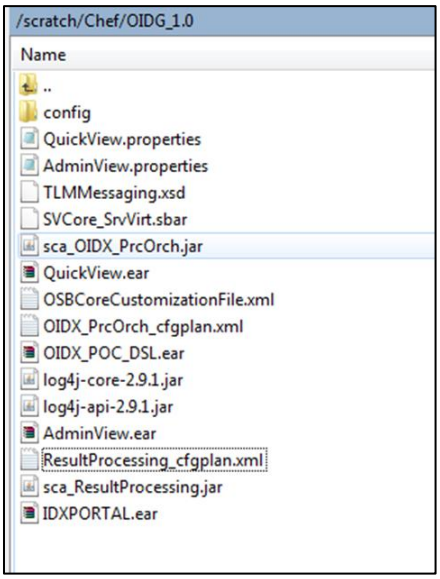



*Figure 1: OIDG release package folder structure*

Copy the following files from the release package to **/<user home base>/Chef/`OIDG_1.0/config`**

- /SrvVirt/adapter-oidx-cache-config.xml
- /DataSrv/configfilesecurity.key
- /DataSrv/OIDX.properties
- /DataSrv/oidx_cache_config.xml
- /DataSrv/oidx_dsl_log4j.xml
- /DataSrv/PIIConfig.xml

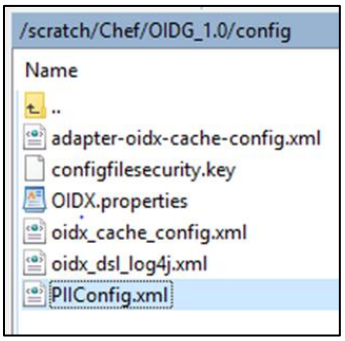



*Figure 2: OIDG release package folder structure*

Chapter – 3

# INPUT PARAMETERS FOR OIDG INSTALLATION

This chapter includes following topics:

- OIDG Parameter Configuration Steps
  - Linux User/Group Section
  - Database Section
  - Middleware Section
  - Confirmation Section
  - Credentials Section

## OIDG Parameter Configuration Steps

1. Go to the path **/OIDG-1.0-automation/chef/** and run**: sh oidg_config.sh** with root user

```
[root@HostName chef]# pwd
/scratch/Chef/scripts/OIDG-1.0/chef
[root@HostName chef]#
[root@HostName chef]# sh oidg_config.sh
```

2. Provide the required information for the following inputs

### Linux User/Group Section

1. **Linux Username**
   - Example: *oracle* (the user you installed Fusion Middleware with)

2. **FMW Products Installed Group**
   - Example: *oinstall* or *oracle* (the user group you installed Fusion Middleware with)

```
########################################
Application Name               : OIDG
########################################

Please read the instructions and provide the below required inputs for OIDG application installation

---------------------------
Linux User/Group inputs
---------------------------

Please provide the Linux Username/Groupname with which Oracle Fusion Middleware was installed

Linux Username (FMW Products installed) :
```

```
--------------------------
Linux User/Group inputs
--------------------------

Please provide the Linux Username/Groupname with which Oracle Fusion Middleware was installed

Linux Username (FMW Products installed) : testuser

Linux Groupname (FMW Products installed): testuser
```

## Database Section

### OIDG and RCU schemas are created in the same database instance.

```
IS OIDG Schema and RCU Infra Schemas were created on the Same
Database/Pluggable Database (y/n): y
```

```
--------------------
Database inputs
--------------------

IS OIDG Schema and RCU Infra Schemas were created on the Same Database/Pluggable Database (y/n)     : y
```

Enter the following values to proceed further:

```
Database hostname:          Database hostname
Database service name:      DB Instance name
Database port:              Listener port (Example: 1521)
Database OIDG User name:    OIDG schema name
RCU Infra Schema Prefix:    RCU Schema's Prefix
```

```
----------------------
Database inputs
----------------------

Note: OIDG Schema and RCU Infra Schemas needs to be created on the Same Database/Pluggable Database

Please provide the Database/Pluggable Database details where OIDG Schema and RCU Infra Schemas created

Database hostname               : test.us.test.com
Database service name           : testpdb.us.oracle.com
Database port                   : 1212

Please provide the OIDG Schema name

Database OIDG User name         : test

Please provide the Prefix of RCU Schemas

RCU Infra Schema Prefix         : DEV
```

### OIDG and RCU Schemas are created in Different database instances.

```
IS OIDG Schema and RCU Infra Schemas were created on the Same
Database/Pluggable Database (y/n): n
```

```
----------------------
Database inputs
----------------------

IS OIDG Schema and RCU Infra Schemas were created on the Same Database/Pluggable Database (y/n)     : n
```

## Enter the DB inputs:

| | |
|---|---|
| RCU Database hostname: | Database hostname |
| RCU Database service name: | DB Instance name |
| RCU Database port: | Listener port (Example: 1521) |
| RCU Infra Schema Prefix: | RCU Schema's Prefix |
| OIDG Database User name: | OIDG schema name |
| OIDG Database hostname: | OIDG Database hostname |
| OIDG Database service name: | OIDG DB Instance name |
| OIDG Database port: | OIDG Listener port (Example: 1521) |

```
----------------------
Database inputs
----------------------

IS OIDG Schema and RCU Infra Schemas were created on the Same Database/Pluggable Database (y/n)     : n

Please provide the Database/Pluggable Database details where OIDG Schema and RCU Infra Schemas created

RCU Database hostname              : test.us.test.com
RCU Database service name          : testpdb.us.test.com
RCU Database port                  : 1212

Please provide the Prefix of RCU Schemas

RCU Infra Schema Prefix        : DEV

Please provide the OIDG Schema name and Database Details

Database OIDG User name          : OIDG
OIDG Database hostname           : test2.us.test.com
OIDG Database service name       : testppdb.us.test.com
OIDG Database port               : 1212
```

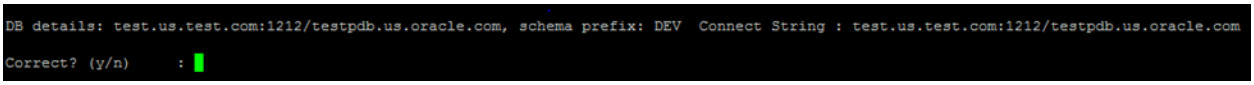
# Middleware Section

- OIDG Fusion Middleware HOME Path:
  - Enter the middleware home path including **Oracle_Home**

```
-----------------------------
Middleware Home inputs
-----------------------------

Please provide the Oracle Middleware Home path: Ex- /u01/fmw1221/Oracle/Middleware/Oracle_Home

OIDG Fusion Middleware HOME path        :
```

# Confirmation Section

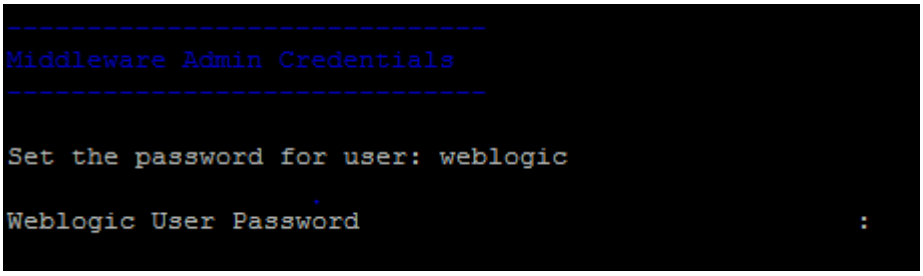
```
Correct? (y/n) :  (y/n)
```




# Credentials Section

## WebLogic Credentials

- Set the WebLogic User Password
  - You have to use this password for WebLogic login after domain creation.



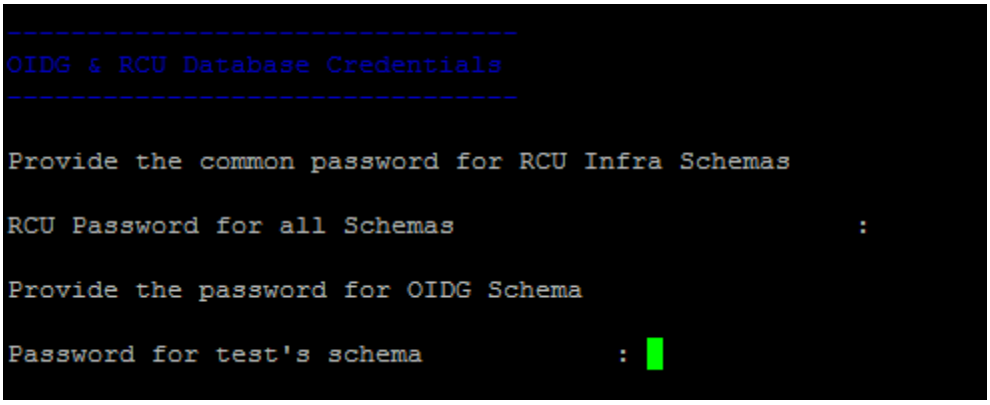

## Database Credentials

- Set the RCU Password for all Schemas

```
Provide the common password used for the RCU Infra Schemas
```

- Set the password for OIDG's schema:

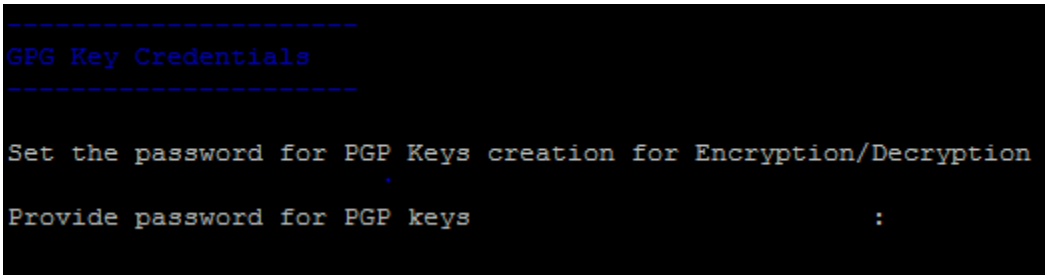
```
Provide the password for the OIDG db schema
```




## GnuPGCredentials

- Set the password for PGP keys

```
Set the password for PGP Key creation for Encryption/Decryption
```




## Security Realm user Credentials

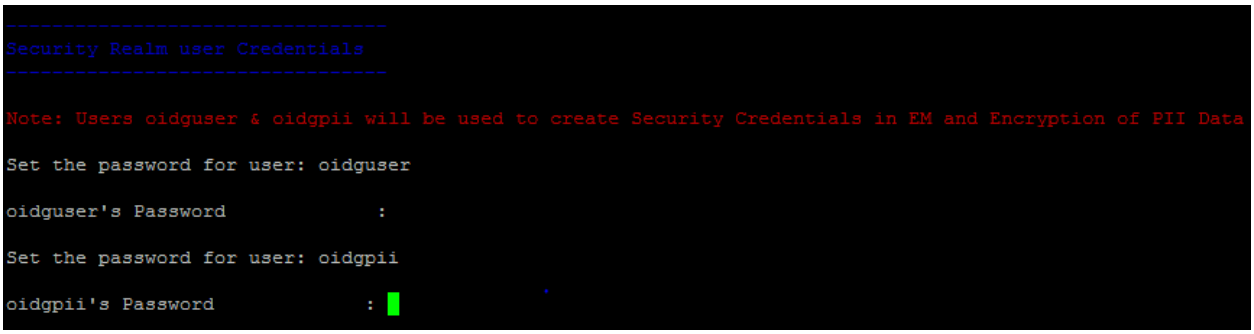
**Note**: Users **oidguser** and **oidgpii** are created for configuring Security Credentials in EM and Encryption of PII Data

- oidguser's Password:

  ```
  Set the password for user: oidguser
  ```

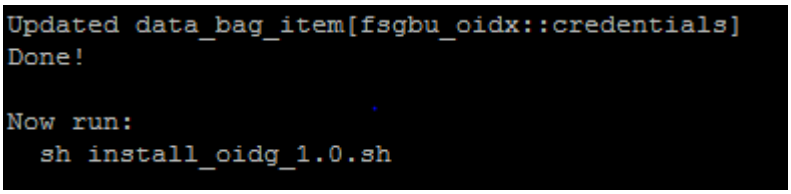
- oidgpii's Password:

  ```
  Set the password for user: oidgpii
  ```




# Confirmation

Please verify and resolve any errors that have occurred before running **sh install_oidg_1.0.sh**



# OIDG PRE-SCRIPT INSTALLATION

1. Go to the path **/OIDG-1.0-automation/chef/** and run: **sh install_oidg_1.0.sh** from root.

```
[root@HostName chef]# sh oidg_config.sh
```

2. Please check the status of Chef Script: Finished (or) failed.

```
Running handlers:
Running handlers complete
Chef Client finished, 31/35 resources updated in 05 minutes 55 seconds
[root@HostName chef]#
```

   **Note**: Script execution takes about 30 – 40 minutes.

3. Upon the completion of the **install_oidg_1.0.sh** script, please refer to Chapter 5.

**Follow these steps in case of pre-script execution failures:**

1. Drop and Re-create the RCU Schema.

2. Delete the middleware user_projects folder and domain_registry.xml.
   **Example**: /FMW_HOME/Oracle/Middleware/Oracle_Home/user_projects

3. Delete the OIDG folder.
   **Example**: /FMW_HOME/Oracle/Middleware/oidg

4. Delete ora_stage folder.
   **Example**: /FMW_HOME/oraStage

5. Kill all the running WebLogic processes if there are any.

6. Re-run from the input parameters for OIDG Installation chapter with new RCU Schemas.

# OIDG INSTALLATION MANUAL STEPS

This chapter includes following topics:

- Defining JNDI Providers
- Creating Security Policies

## Defining JNDI Providers

JNDI Provider resources are required by OSB components to locate and communicate with Enterprise Java Beans (EJB) components.

1. Log on to the Service Bus console (http://hostname:port/sbconsole), where "**hostname:port**" are the host name and port of your administration server.

2. In the project explorer, navigate to All Projects → System → JNDI Providers.
   Verify that **DataServices_JNDIProvider** is defined.
   If it is defined, skip steps 3-7. If not, continue with the rest of the steps.

3. In the upper left corner of the page, click Create to begin a new update session.

4. Right-click the JNDI Providers folder to display the context menu, then click Create → Create JNDI Provider.

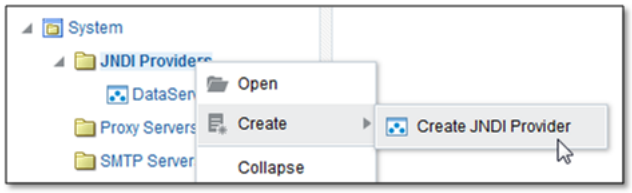



*Figure 3: Create JNDI Provider*

5. In the Create JNDI dialog, enter "DataServices_JNDIProvider" for Resource Name. Click Create.

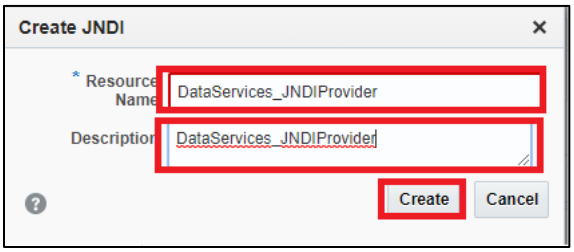



*Figure 4: Create JNDI dialog*

6. On the JNDI Definition page, fill in the following fields:
   a. **Provider URL** – the host name or IP and port of the managed server to which OIDX_POC_DSL is targeted (Example: “t3://hostname:port”) i.e. ‘AML Server’.
   b. **Initial Context Factory** – select “weblogic.jndi.WLInitialContextFactory”
   c. **User Name, New Password, and Confirm Password** – the login credentials for the server. Usually credentials are the same as administration server login credentials.

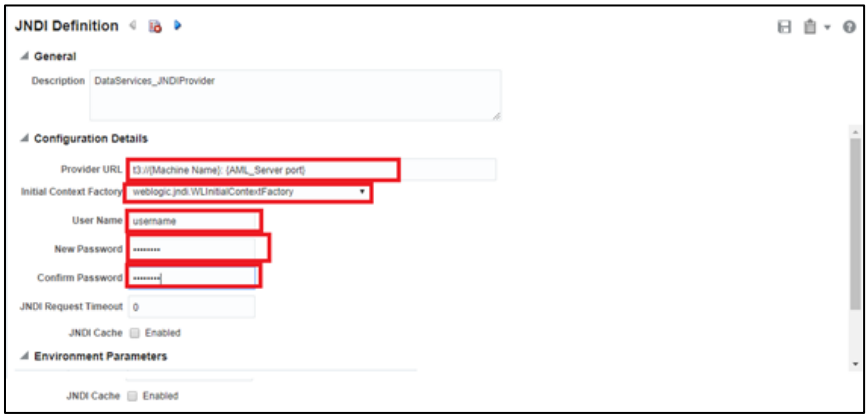



*Figure 5: JNDI Definition*

7. Click Save located on the upper-right corner of the page.

*Figure 6: Save icon*

# Creating Security Policies

1. Login to the WebLogic Enterprise Manager (<hostname>:> :< Admin Server Port Number>/em) with WebLogic credentials.

2. WebLogic Domain → Security → System Policies.

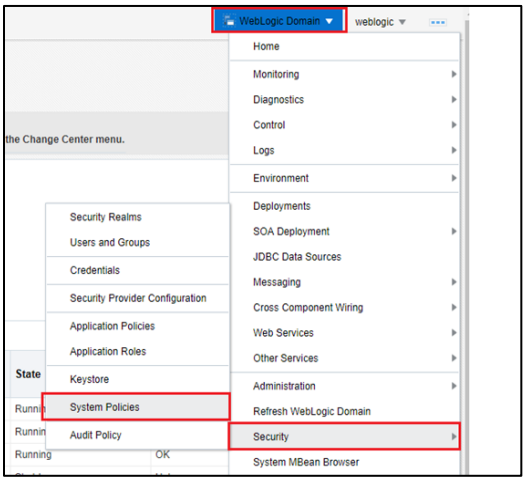



*Figure 7: WebLogic Enterprise*

3. Under Search section, select Name as Includes.

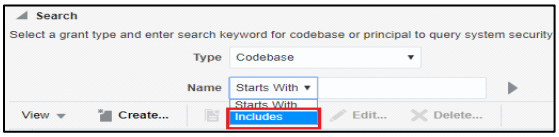



*Figure 8: Search section*

4. Type “OIDX_POC_DSL” in the search box, and click the arrow icon.

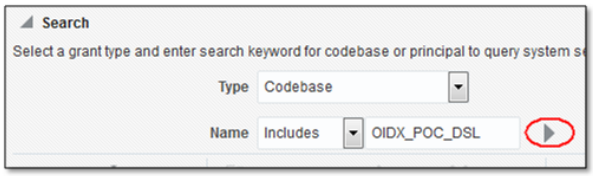



*Figure 9: Search box*

5. Check to see if the search results include a row as shown below.

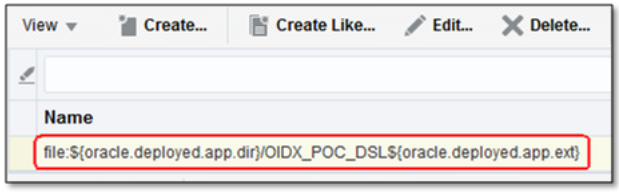



*Figure 10: Search result area*

6. If this policy does not exist, create it by following these steps:

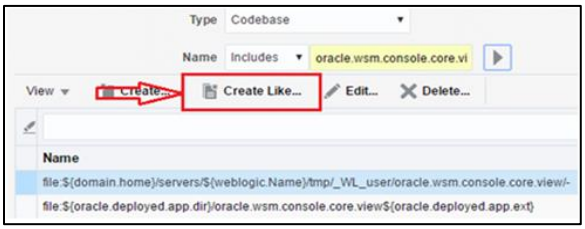



*Figure 11: Create Like*

a. Select the row that includes the text **oracle.wsm.console.core.view**, and then click Create Like.
b. On the Create System Grant Like page, change the text in the Codebase box to the following:
**file:${oracle.deployed.app.dir}/OIDX_POC_DSL${oracle.deployed.app.ext}**
c. Select the **CredentialAccessPermission** row in the Permission Class table and click Edit.
d. In the Edit Permission dialog change Permission Actions from **read,write,delete,update** to just **read**. Click Ok.
e. Click Ok again.

# OIDG POST-SCRIPT INSTALLATION

1. After completing the steps in Chapter 5, go to the path **/OIDG-1.0-automation/chef/** and run the following command from root to complete the installation

   `Command: sh install_oidg_1.0_post.sh  (from root)`

   ```
   [root@HostName chef]# sh install_oidg_1.0_post.sh
   ```

2. Please check the status of Chef Script: **Finished (or) failed**

   ```
   Running handlers:
   Running handlers complete
   Chef Client finished, 31/35 resources updated in 05 minutes 55 seconds
   [root@HostName chef]#
   ```

   **Note**: Script execution usually takes about 20-30 minutes to complete all the deployments.

# DEPLOYING ACORD_AML LIBRARIES

Follow these steps:

1. Log into the Service Bus Console (<hostname>:<Admin Server port number>/sbconsole).

2. Create a new update session by clicking Create.

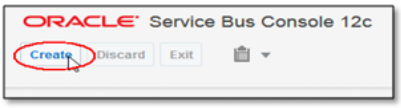



*Figure 12: Oracle Service bus console*

3. Click Import.

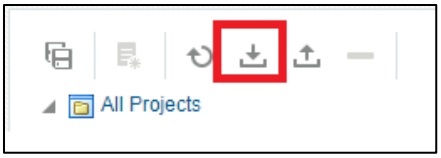



*Figure 13: Import*

4. Click Choose File and upload the file.

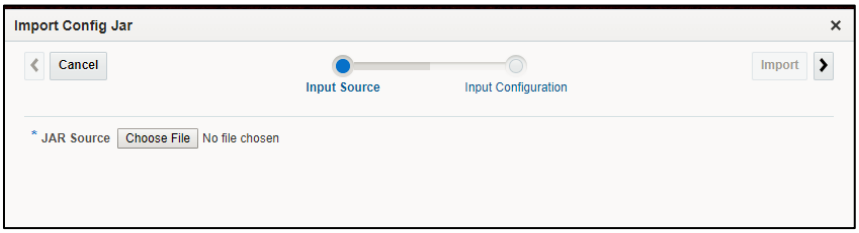



*Figure 14: Choosing and uploading file*

5. Click Next (right arrow).

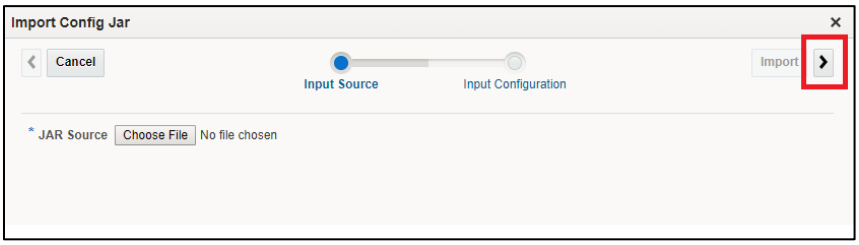



*Figure 15: Next button*

6. Click Import.

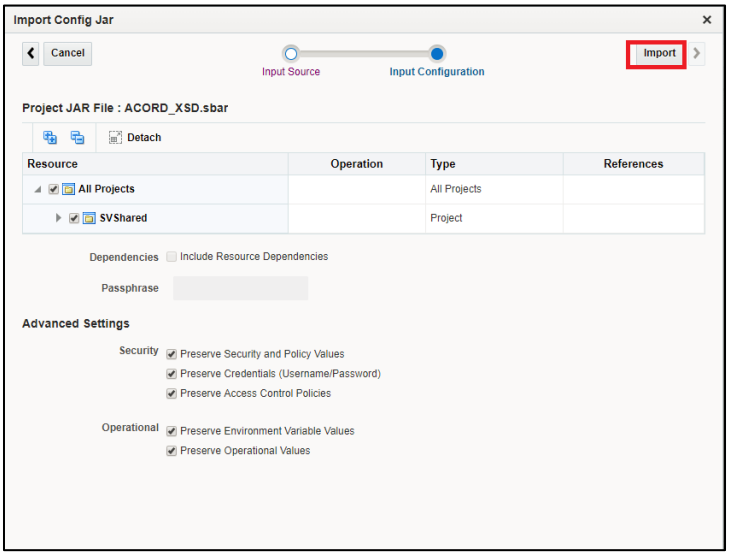



*Figure 16: Import button*

7. Click Close.


*Figure 17: Close button*

# OIDG RELEASE UPGRADE

This chapter includes following topics:

- OIDG Release Upgrade Pre-Requisite
- OIDG Release Deployment / Un-Deployment Process
- OIDG Release Un-Deployment Process
- OIDG Release Deployment Process

## OIDG Release Upgrade Pre-Requisite

Delete old files from the following locations and replace them with the new release files:

1. Copy the following files from the OIDG release package to **/<user home base>/Chef/OIDG_1.0**
    - AdminView.ear
    - AdminView.properties
    - log4j-api-2.9.1.jar
    - log4j-core-2.9.1.jar
    - OIDX_POC_DSL.ear
    - OIDX_PrcOrch_cfgplan.xml
    - OSBCoreCustomizationFile.xml
    - QuickView.ear
    - IDXPORTAL.ear
    - sca_ResultProcessing.jar
    - ResultProcessing_cfgplan.xml
    - QuickView.properties
    - sca_OIDX_PrcOrch.jar
    - SVCore_SrvVirt.sbar

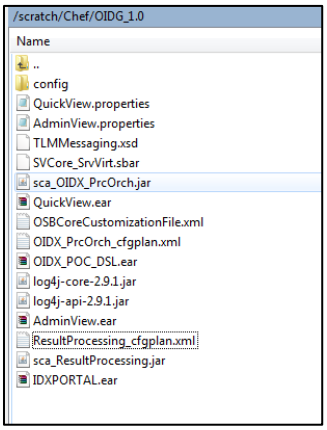



*Figure 18: OIDG release package*

2. Copy the files below from the OIDG release package to **/user home base/Chef/OIDG_1.0/config**
    - adapter-oidx-cache-config.xml
    - configfilesecurity.key
    - OIDX.properties
    - oidx_cache_config.xml
    - oidx_dsl_log4j.xml
    - PIIConfig.xml

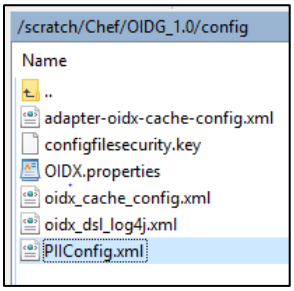


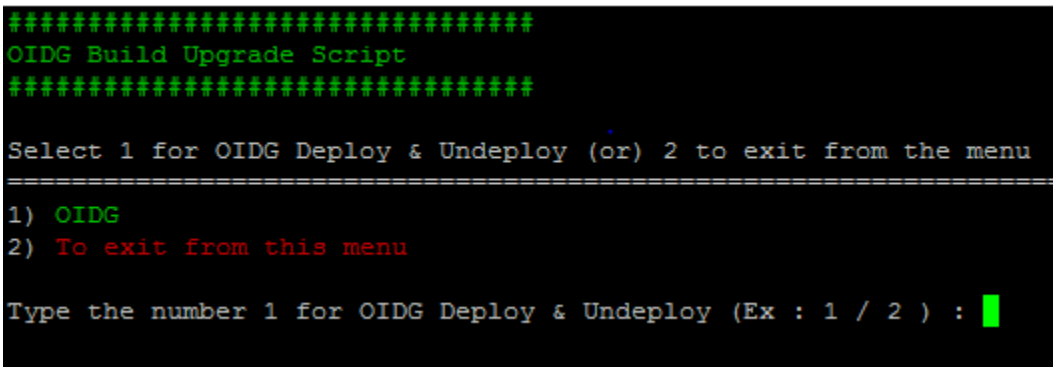

*Figure 19: OIDG release package*

## OIDG Release Deployment / Un-Deployment Process

Go to the path **/OIDG-1.0-automation/chef/** and run: `sh dep_undep_app_config.sh` from root.

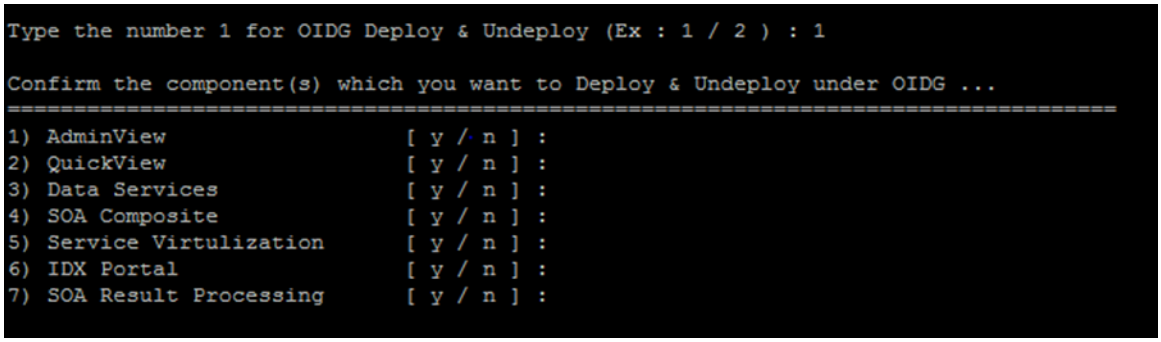
```
[root@HostName chef]# sh dep_undep_app_config.sh
```

3. Select 1 for OIDG Deploy/Un-Deploy (or) 2 for Exit




4. Select the components you want to undeploy and replace from the new release package.

```
1) AdminView                    [ y / n ] : (y/n)
2) QuickView                    [ y / n ] : (y/n)
3) Data Services                [ y / n ] : (y/n)
4) SOA Composite                [ y / n ] : (y/n)
5) Service Virtualization       [ y / n ] : (y/n)
6) IDX Portal                   [ y / n ] : (y/n)
7) SOA Result Processing        [ y / n ] : (y/n)
```




5. Provide the Linux user/group and Middleware Home details.

   - `Linux Username:`
     - Example: oracle (the user you installed Fusion Middleware with)
   - `Linux Groupname:`
     - Example: oinstall or dba (the group you installed Fusion Middleware with)
   - `FMW Middleware Home:`
     - Middleware home path including **Oracle_Home**
       Example: /Path/Oracle/Middleware/Oracle_Home

- All the inputs given are Correct? (y/n) : (y/n)

```
Linux Username (FMW Products installed)                                  : testuser
Linux Groupname (FMW Products installed)                                 : testgroup
FMW Middleware Home  (Ex : /Path/Oracle/Middleware/Oracle_Home ) : /u01/testuser/Oracle/Middleware/Oracle_Home

All the inputs given are Correct? (y/n)     : y
```

- WebLogic User Password

```
----------------------
Weblogic Credentials
----------------------


Weblogic User Password                                  :
```

6. Check the Confirmation

```
Done!

Now run Undeployment of application :
  sh install_undep_app.sh
After completion of Undeployment run deployment of application:
  sh install_dep_app.sh
```

## OIDG Release Un-Deployment Process

1. Go to path **/OIDG-1.0-automation/chef/** and run: `sh install_undep_app.sh` from root

```
[root@HostName chef]# sh install_undep_app.sh
```

2. Check the status of Chef Script: **Finished** or **Failed**

```
Running handlers:
Running handlers complete
Chef Client finished, 31/35 resources updated in 05 minutes 55 seconds
[root@HostName chef]#
```

Please verify the status of Un-Deployment components from WebLogic console and EM.

## OIDG Release Deployment Process

1. Go to the path **/OIDG-1.0-automation/chef/** and run: `sh install_dep_app.sh` from root.

```
[root@HostName chef]# sh install_dep_app.sh
```

2. Check the status of Chef Script: `Finished` or `Failed`.

```
Running handlers:
Running handlers complete
Chef Client finished, 31/35 resources updated in 05 minutes 55 seconds
[root@HostName chef]#
```

Please verify the status of deployed components from the WebLogic and EM consoles.

Chapter – 9

# SETTING UP THE ENTERPRISE SCHEDULER SERVICE JOBS

This chapter includes following topics:

- Configuring Daily Error Log
- Updating OIDX.Properties file

This chapter describes how to configure jobs in the Enterprise Scheduler Services (ESS) for batch request processing. Before proceeding with this section, you must configure your parties and contracts in the AdminView. Please refer to the *Oracle Insurance Data Gateway User Interface Guide* for more info on this.

Once your parties and contracts have been established you can configure schedules for batch jobs following these steps:

1. Login to the Enterprise Manager console
   Example: http://<hostname>:<Admin Server Port Number>/em

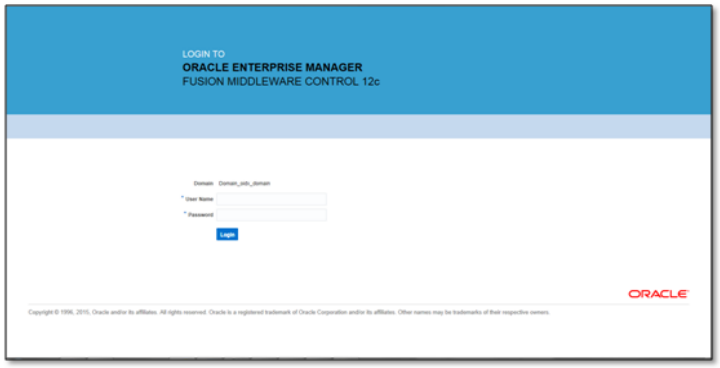



*Figure 20: Enterprise Manager console login page*

2. Click the Target Navigation at the top-left corner.

3. Click Scheduling Services > ESSAPP (ess_server1).

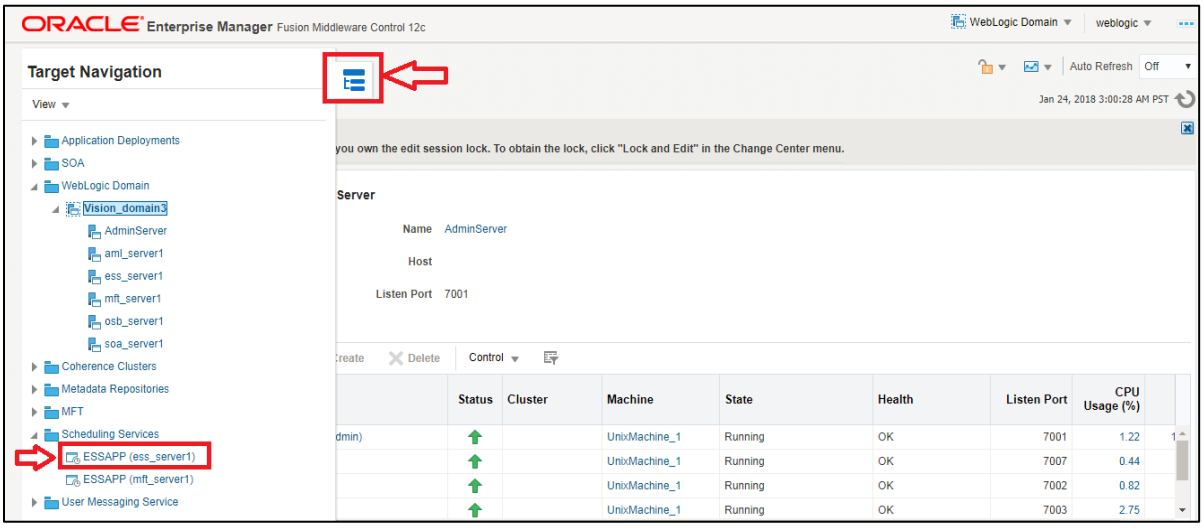



*Figure 21: Scheduling services*

4. Click Scheduling Service → Job Metadata → Job Definitions.

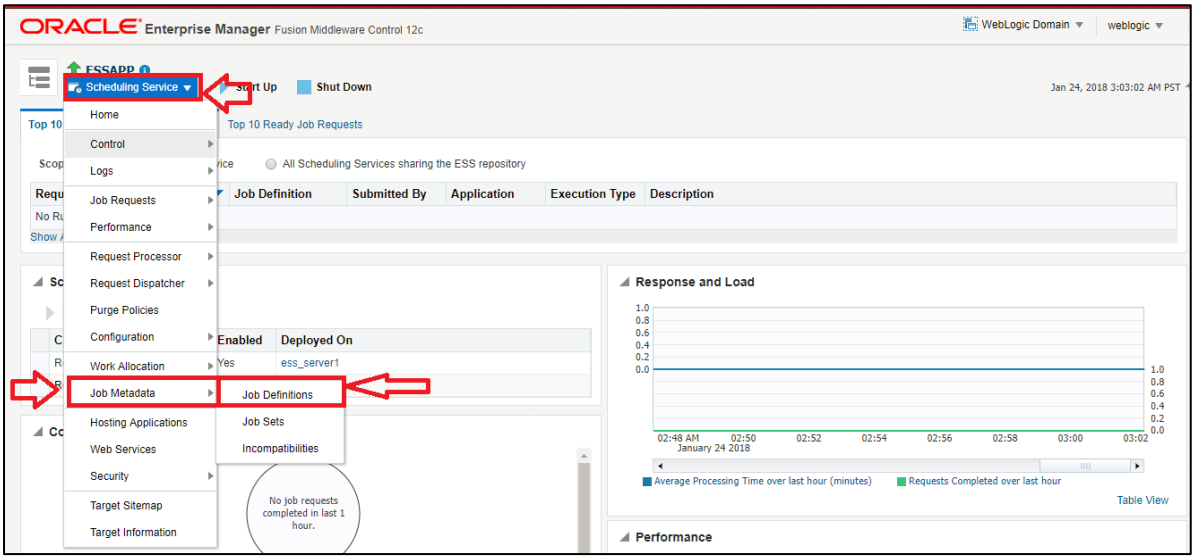



*Figure 22: Job Definitions*

5. Job definition screen appears.


*Figure 23: Job Definitions*

6. Click Create and Enter Name, Display Name, Package, Description and Job Type. As shown in the table below:

| Name | Example | Description |
|---|---|---|
| **Name** | Alamere_IN_Carrier_PolicySync | Job name |
| **Display Name** | Alamere IN Carrier PolicySyncAlamere | Job display name |
| **Package** | /com/oracle/ejb | File Transfer Service package. Always enter this value as '/com/oracle/ejb' |
| **Description** | Alamere IN Carrier PolicySyncAlamere | Job description |
| **Job Type** | OnewayWebserviceJobType | Job type. Always select this field value as "OnewayWebserviceJobType" |

7. Click Select Web Service.

   **Note**: Select Web Service appears only after you select the Job Type as OnewayWebserviceJobType.

8. Enter web service URL at WSDL and Click Go.


*Figure 24: Select web service*

**Example URL**: http://<hostname>:<AML Server Port Number>/OIDX_POC_DSL-EJB-webapp/SchedulerService?WSDL

9. Fill in the details as shown in the table below.

| | |
|---|---|
| **Select Services** | SchedulerServiceMgrEJBBeanService |
| **Port Type** | SchedulerServiceMgrEJBBeanPort |
| **Operation** | fileTransferService |

**Payload:**

```
<PartyShortName></PartyShortName>
<PartyType></PartyType>
<TranactionType></TranactionType>
<BusinessServiceType></BusinessServiceType>
<Direction></Direction>
<Mchnsm></Mchnsm>
<Environment></Environment>
<EndPointId></EndPointId>
```

Gather all the payload values from AdminView to configure jobs.

a. PartyShortName and PartyType

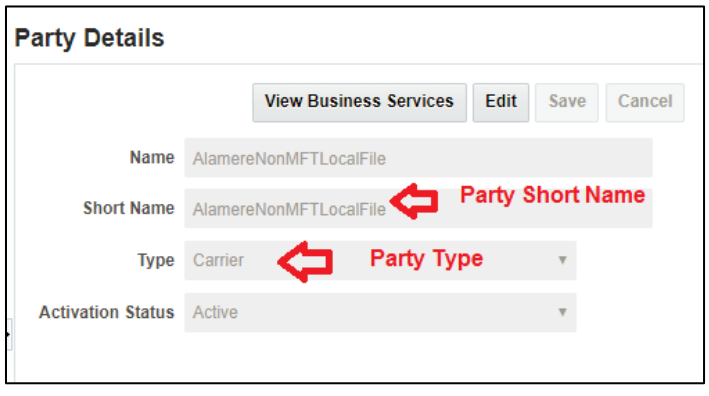



*Figure 25: Party Details section*

b. TransactionType:

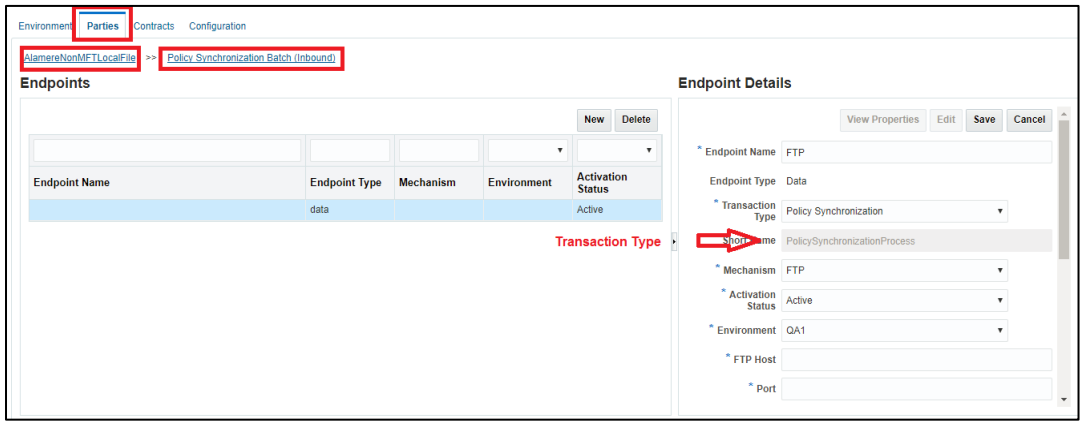



*Figure 26: Endpoint Details section*

c. BusinessServiceType:

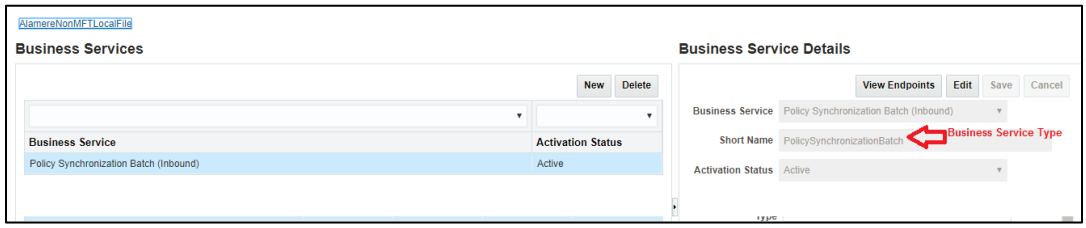



*Figure 27: Business Service Details section*

d. Direction value is always Inbound

e. Mchnsm and Environment:

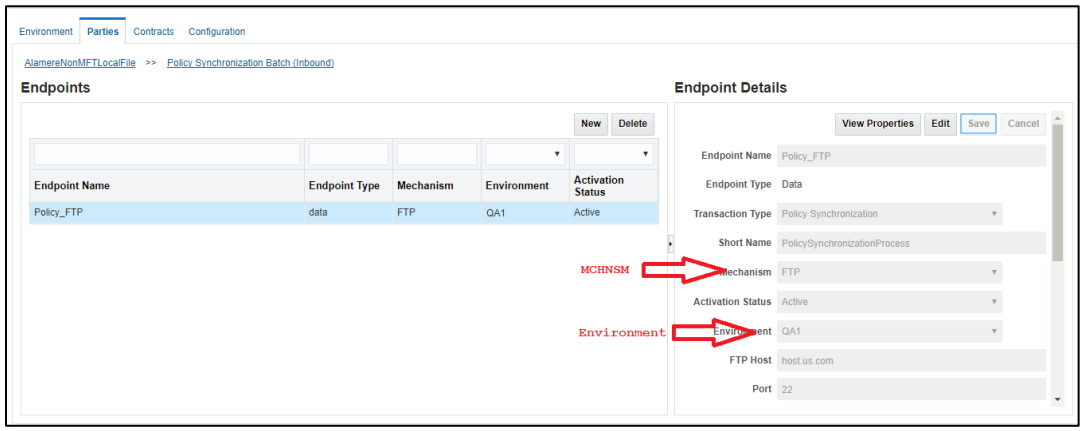



*Figure 28: Endpoint Details section for mechanism and environment*

f. EndPointId:

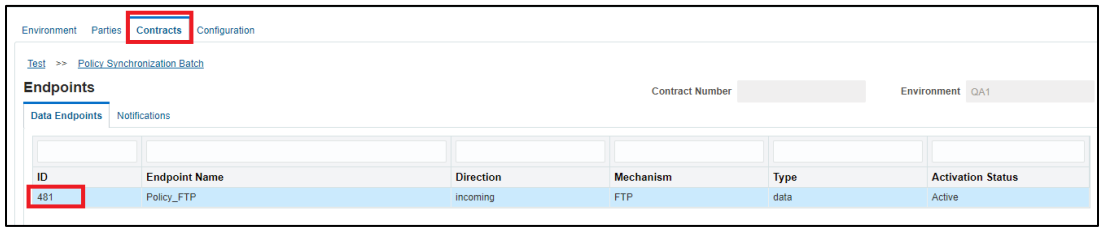



*Figure 29: AdminView application Data Endpoints section*

Example:

```
<ns1:FileTransferService xmlns:ns1="http://oracle.oidx.com/wsdl">
  <PartyShortName>AlamereNonMFTLocalFile</PartyShortName>
  <PartyType>Carrier</PartyType>
  <TranactionType>PolicySynchronizationProcess</TranactionType>

<BusinessServiceType>PolicySynchronizationBatch</BusinessServiceT
ype>
  <Direction>Inbound</Direction>
  <Mchnsm>FTP</Mchnsm>
  <Environment>QA1</Environment>
  <EndPointId>481</EndPointId>
</ns1:FileTransferService>
```

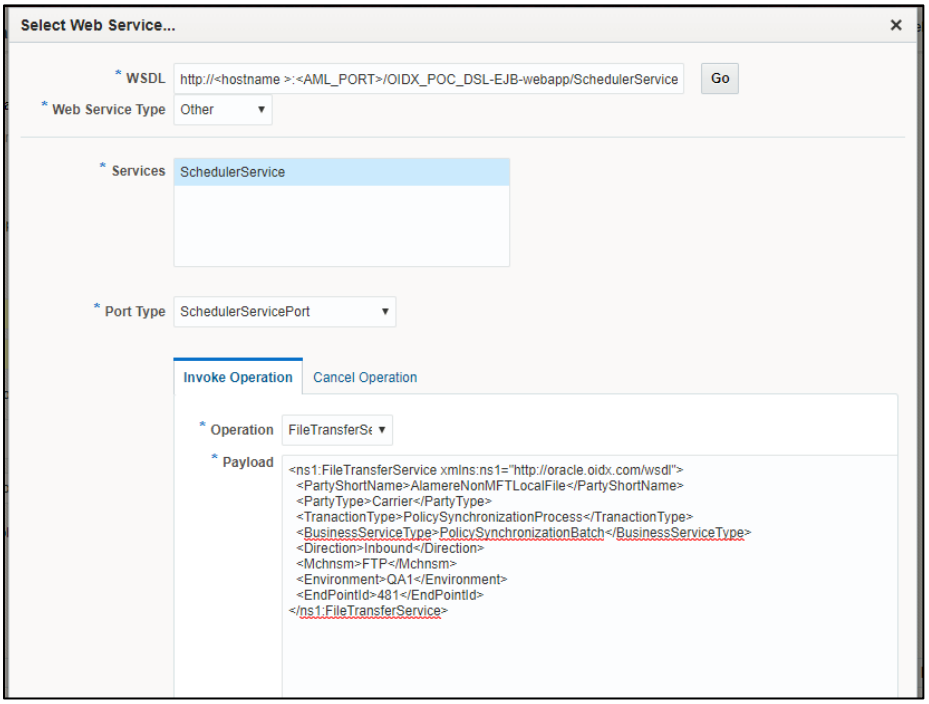



*Figure 30: Select Web Service section*

10. Click Ok to create the Job Definition.

# Configuring Daily Error Log

This section is used to configure Enterprise Scheduler Services by using the ESS application in such a way that you can schedule a particular time to execute the Daily Error Log report generation process.

Follow these steps to configure Daily Error Log report on Enterprise Scheduler Services server.

1. Login to Enterprise Manager Console.
2. Click Scheduling Services > ESSAPP (ess_server1).

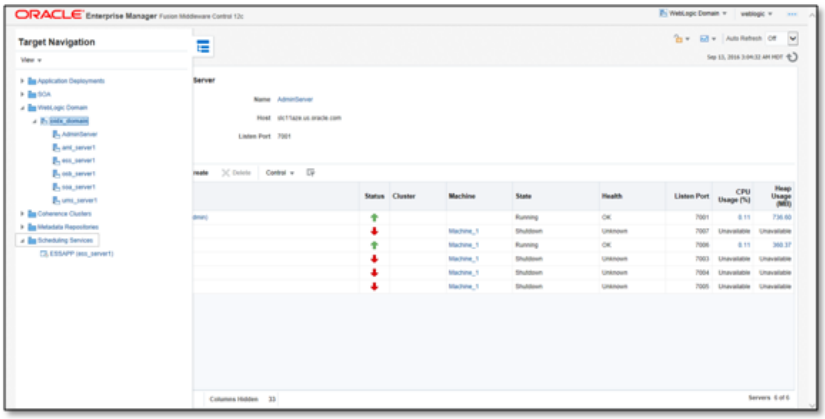


*Figure 31: Enterprise Manager Console after clicking Scheduling Services*

3. Click Scheduling Service → Job Metadata → Job Definitions.

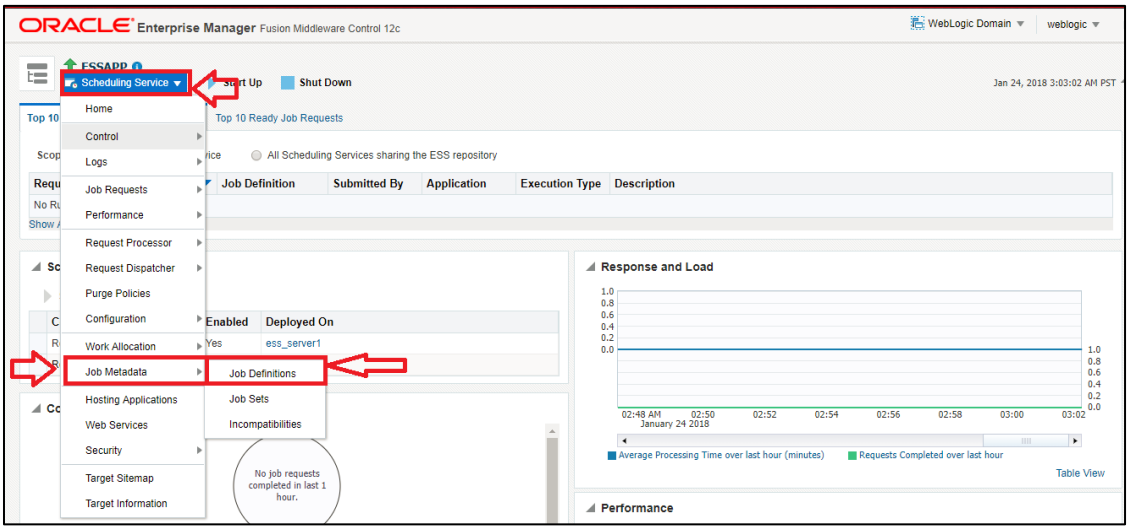



*Figure 32: Enterprise Manager Console after clicking Job Definitions*

4. Click Create and Enter Name, Display Name, Package, Description and Job Type. Example:

| | | |
|---|---|---|
| Name | Daily_Error_Log | Job name |
| Display Name | Daily_Error_Log | Job display name |
| Package | /com/oracle/ejb | Error log service package name. Always enter this value as '/com/oracle/ejb' |
| Description | Daily Error Log | Job description |
| Job Type | OnewayWebserviceJobType | Job type.Always select this value as 'OnewayWebserviceJobType' |

5. Click Select Web Service.

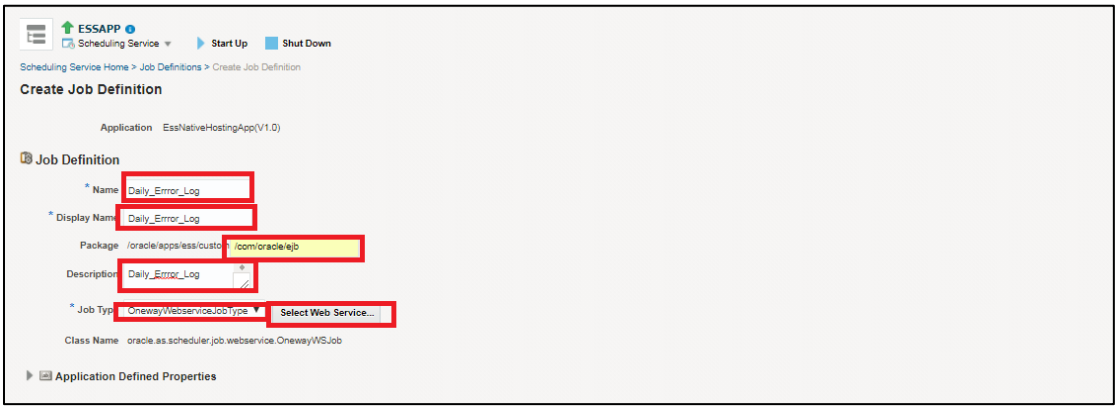



*Figure 33: Creating Job Definition section*

**Note:** Select Web Service appears only after you select the Job Type as OnewayWebserviceJobType.

6. Enter web service URL at WSDL and Click Go.

**Example URL**: http://<hostname>:<AML Server Port Number>/OIDX_POC_DSL-EJB-webapp/SchedulerService?WSDL


*Figure 34 Dialog after clicking Select Web Service*

7. Fill in the details as shown in the table below.

| | |
|---|---|
| Select Services | SchedulerServiceMgrEJBBeanService |
| Port Type | SchedulerServiceMgrEJBBeanPort |
| Operation | errorLogService |

Enter the following Payload:

```
<ns1:ErrorLogService
xmlns:ns1="http://oracle.oidx.com/wsdl">
  <PartyShortName>Daily</PartyShortName>
  <PartyType>Error</PartyType>
  <TranactionType>Log</TranactionType>
  <Direction>report</Direction>
  <SchedulerIntervalInMins>1440</SchedulerIntervalInMins>
</ns1:ErrorLogService>
```

8. Click Ok.


*Figure 35: EM Console*

9. Click Ok.
10. Created Job Definition can be scheduled as per desired requirements.

# Updating OIDX.Properties file

Update the **OIDX.properties** file with active environment value.

1. Open OIDX.properties file from the config folder.
2. Update the **oidx.active.environment='<Environment value>'**

Chapter – 9

# EMAIL CONFIGURATION FOR NOTIFICATIONS

This chapter includes following topics:

- Acquiring mail server SSL certificate
  - Importing the mail server SSL certificate into keystore
  - Synchronizing certificates from central store to local file instanceSynchronizing certificates from central store to local file instance
- Configuring Workflow Notification Properties
- Configuring Email Driver Properties
- Troubleshooting

Please see the *SOA Suite User Guide* for email configuration details. This chapter represents an example set up.

---

Email messages are sent via the Oracle User Messaging Service (UMS) in the WebLogic. The requirements to enable email notifications with User Messaging Service are:

- Acquire and import the mail server SSL certificate into keystore
- Configure Workflow Notification Properties
- Configure Email Driver Properties

If desired, an introduction to UMS is located here:

https://docs.oracle.com/middleware/1212/ums/UMSAG/introduction.htm#UMSAG97582

## Acquiring mail server SSL certificate

Most mail servers will use SSL security and you must import a certificate from the mail server so that UMS can establish a trust relationship with the mail server. One way to acquire a certificate is with a tool like OpenSSL.

From a command window OpenSSL can be invoked to extract certificate information. The sample here is interacting with Oracle Beehive with the results being redirected to the file example.cert:

```
openssl s_client -connect example.oracle.com:465 > example.cert
```

Note that, OpenSSL can take a long time to finish. You can end it after a few seconds with CTRL+C because the needed certificate information is at the beginning.

Next, open the example.cert file with a text editor to copy the portion identified by the “BEGIN CERTIFICATE” and “END CERTIFICATE” records.

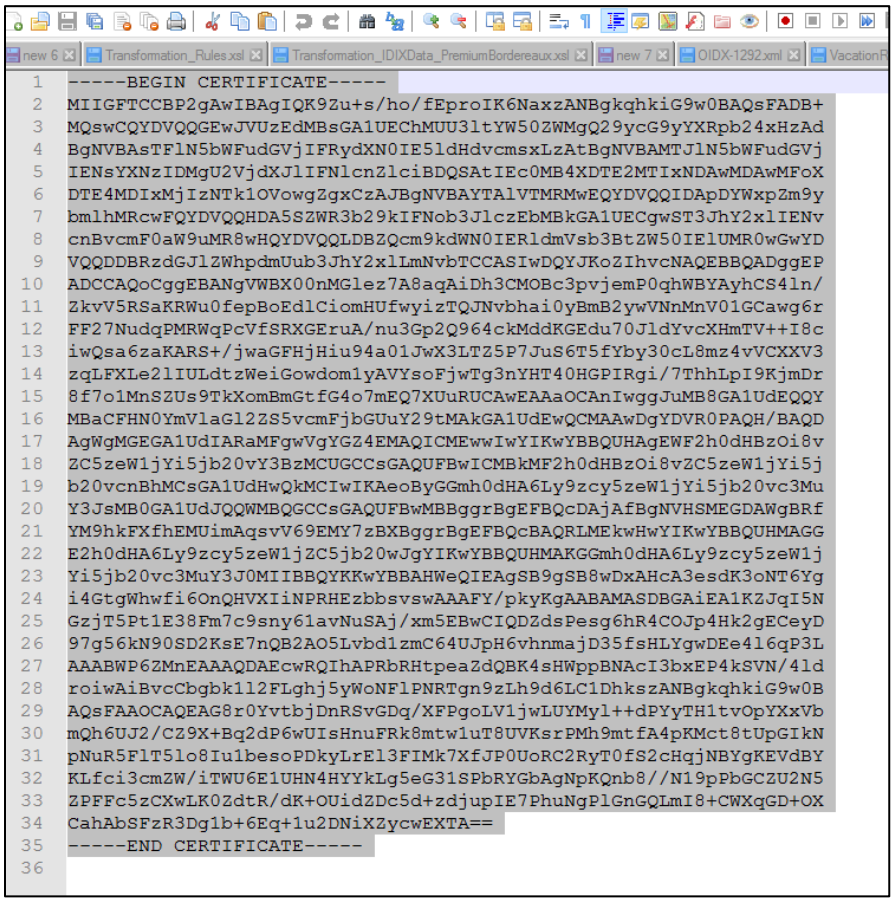



*Figure 36: example.cert file*

## Importing the mail server SSL certificate into keystore

To import the SSL certificate, open the Enterprise Manager Fusion Middle Control and navigate to the Security / Keystore menu item on the WebLogic Domain. Next select the system/trust store and click Manage.

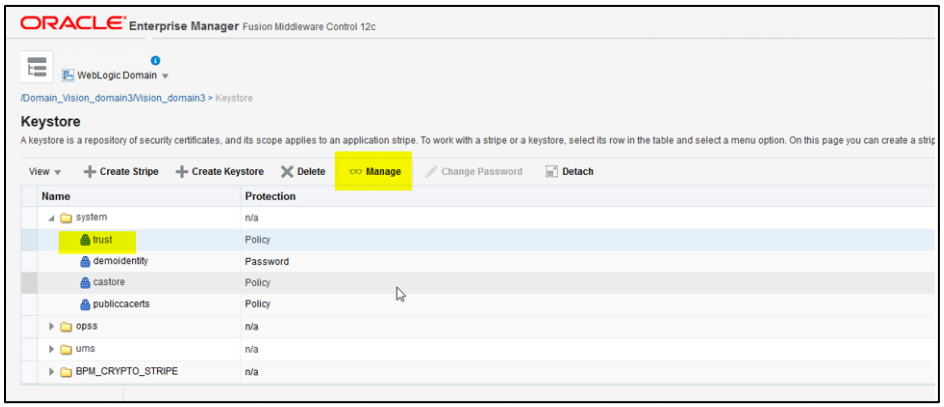



*Figure 37: Enterprise Manager Fusion Middle Control*

On the Manage Certificates pane, click Import and then provide an alias such as “example” and paste the certificate information that was copied earlier.  Click Ok.

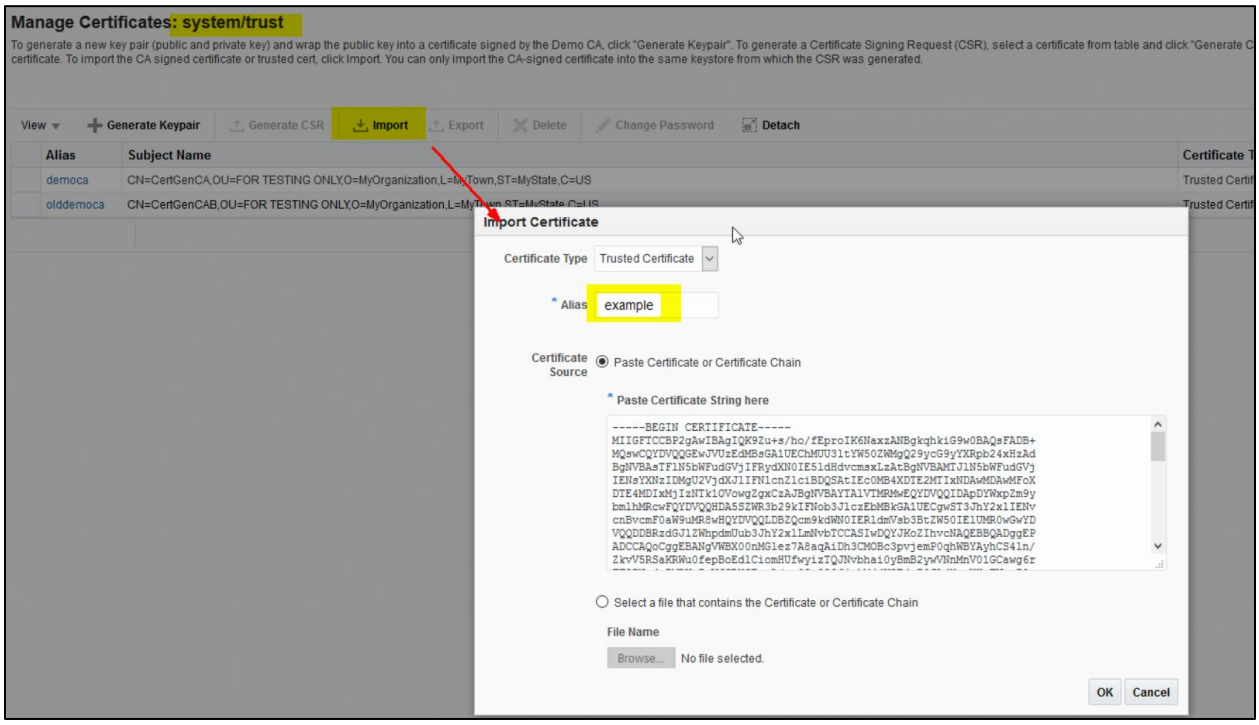



*Figure 38: Managing Certificates screen*

For many mail servers importing the one certificate will complete the task, but for example, Oracle Beehive utilizes a certificate chain, so it is also necessary to acquire and import certificates for Symantec® and Verisign®.

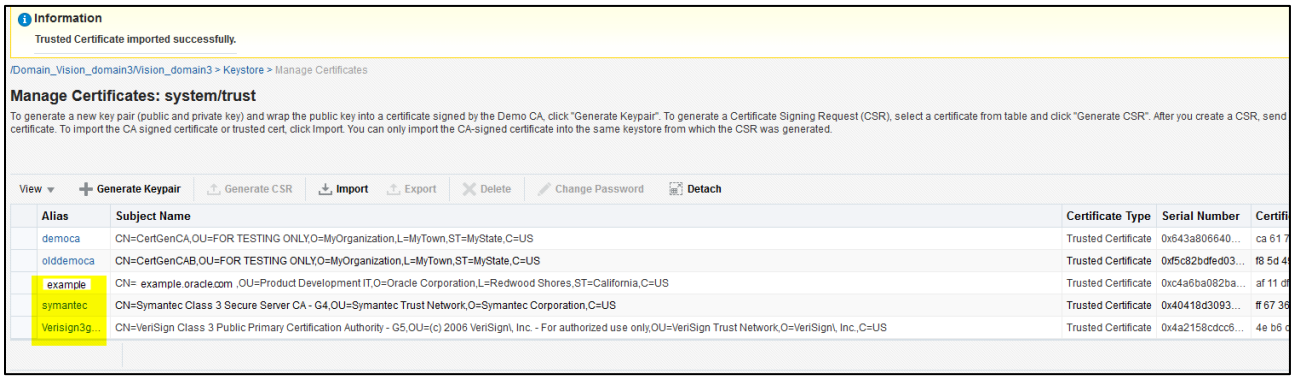



*Figure 39: Import certificates*

## Synchronizing certificates from central store to local file instance

Oracle User Messaging Service depends on certificates that are available from the local file instance of the keystore, so you must synchronize the certificates with the `syncKeyStores` command on the System MBean as previously described in “Synchronizing KSS keystores”. This step requires restarting the WebLogic servers.

# Configuring Workflow Notification Properties

To enable email notifications to be sent from the SOA workflow, open the Enterprise Manager Fusion Middle Control and navigate to the SOA Administration / Workflow Properties menu item on the **soa_server**.

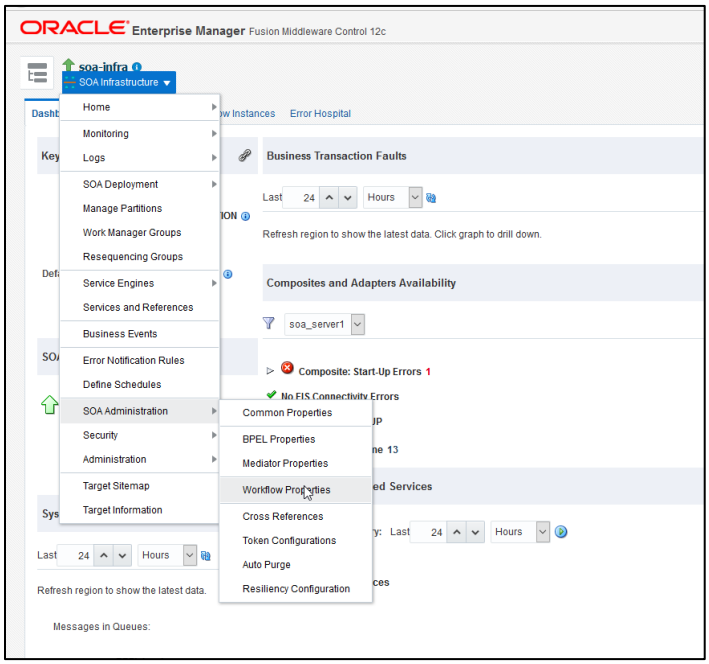



*Figure 40: Workflow Properties*

Change the Notification Mode to Email. Provide From, Actionable, and Reply To email addresses.

All email notifications sent from the SOA workflow will utilize the From email address, so the use of a no-reply email address is recommended (e.g. no-reply@example.com).

Click Apply to apply the changes.

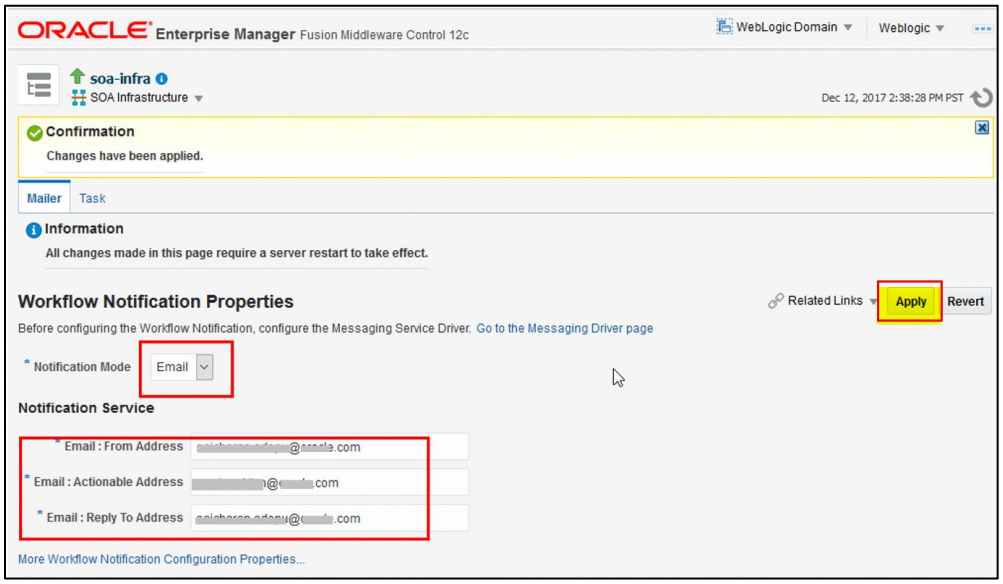



*Figure 41: Workflow Notification Properties*

# Configuring Email Driver Properties

To provide mail server account information:

1. Open the Enterprise Manager Fusion Middle Control and navigate to the User Messaging Service / usermessagingdriver-email (soa_server1) menu item.

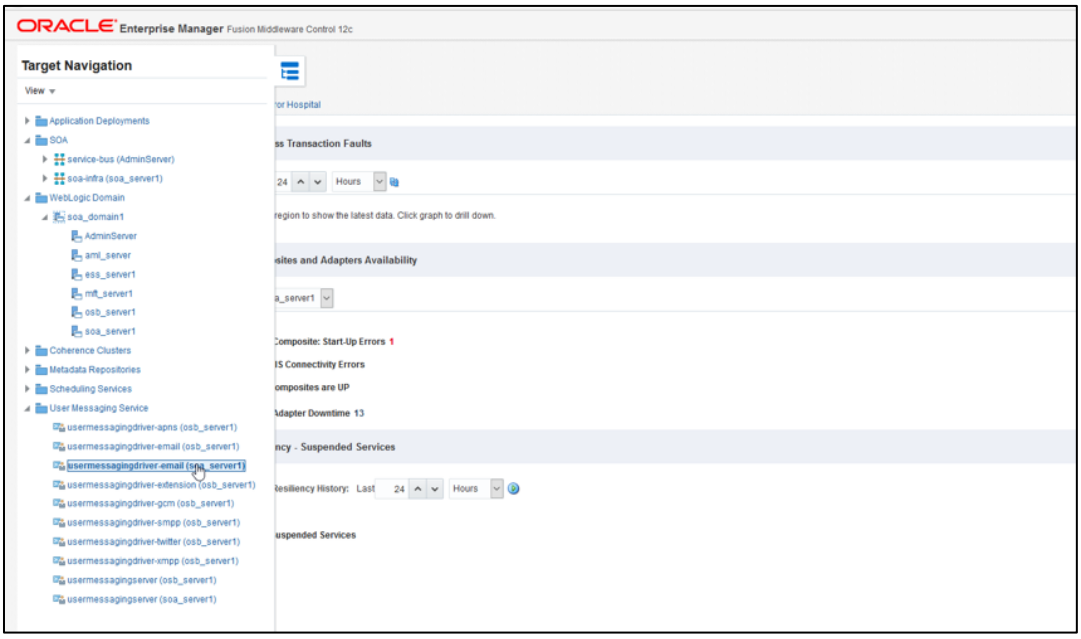



*Figure 42: User Messaging Service / usermessagingdriver-email (soa_server1) menu item*

2. Choose the Email Driver Properties menu item.

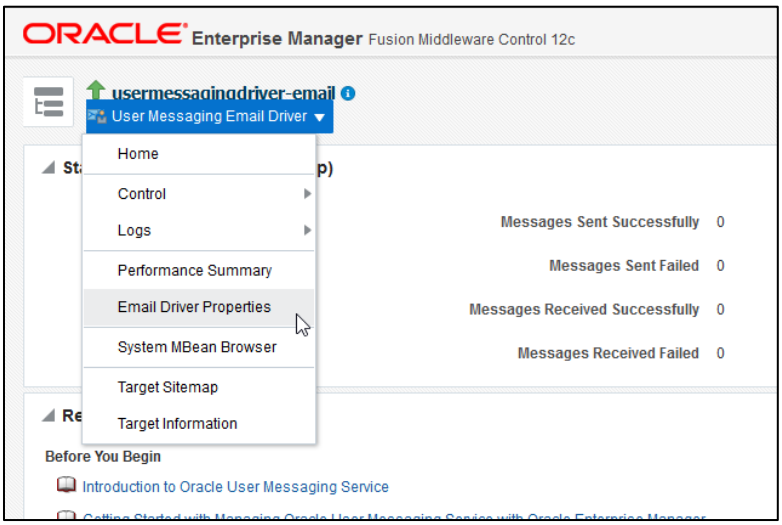



*Figure 43: Email Driver Properties menu item*

3. Create an email configuration.

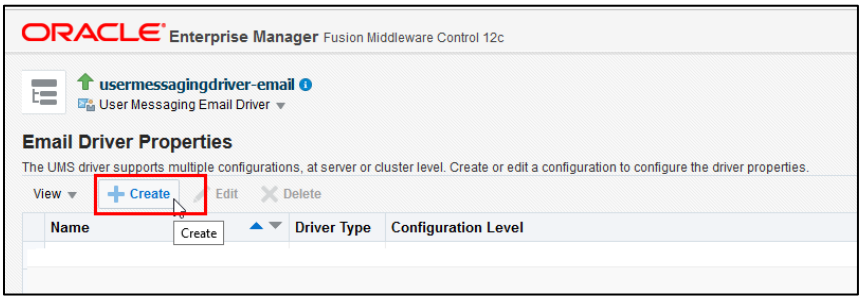



*Figure 44: Creating Email configuration*

4. Now provide a configuration name, sender address and set the delivery type to SEND.

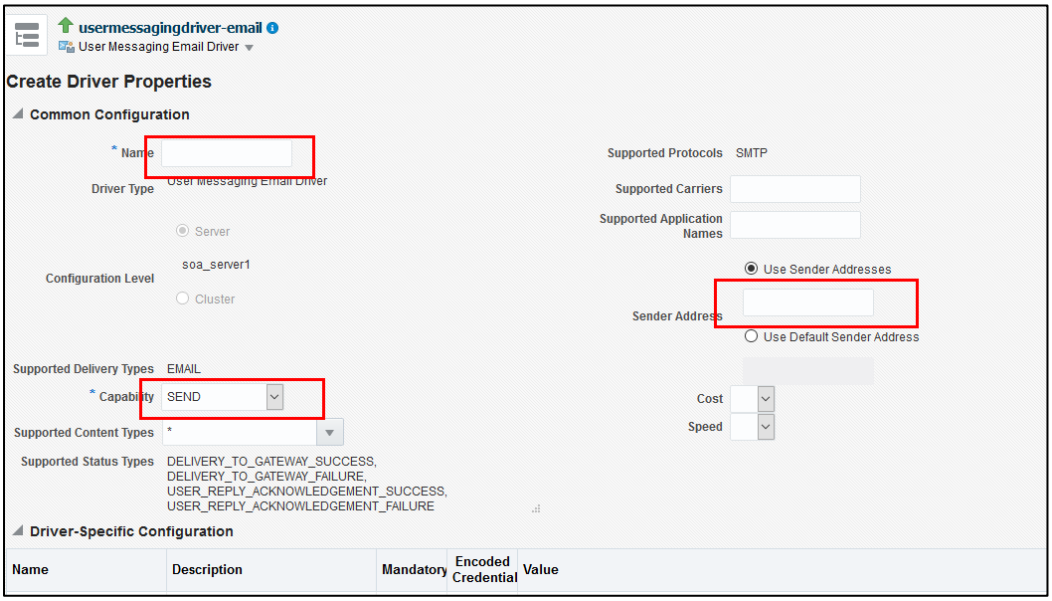



*Figure 45: Create Driver Properties screen*

5. Since the deliver type is SEND, you only need to provide the outgoing email information. Scroll down and set the outgoing email Server, Port, Security, Default from address, Username and Password.

The email address given here must match the From address provided earlier in the Workflow Notification Properties.

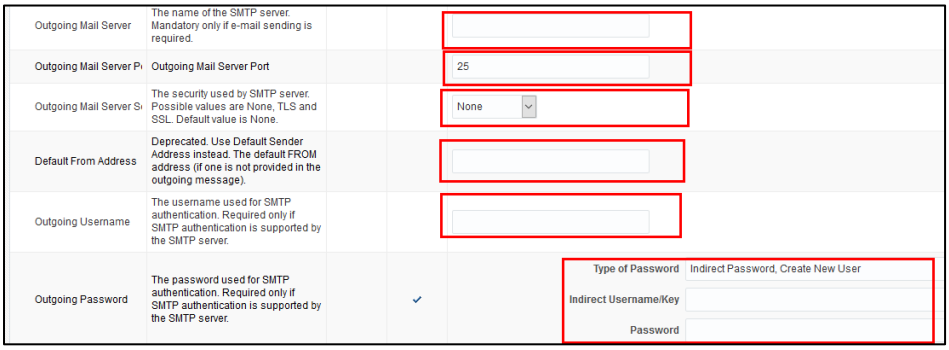



*Figure 46: Create Driver Properties screen*

6. Scroll back to the top and click Test to confirm the configuration. If the test does not show “The driver configuration is valid”, there is an issue with the server or credentials provided, or a missing SSL security certificate.

   If the server and credentials are valid but the test still fails, see Troubleshooting below.

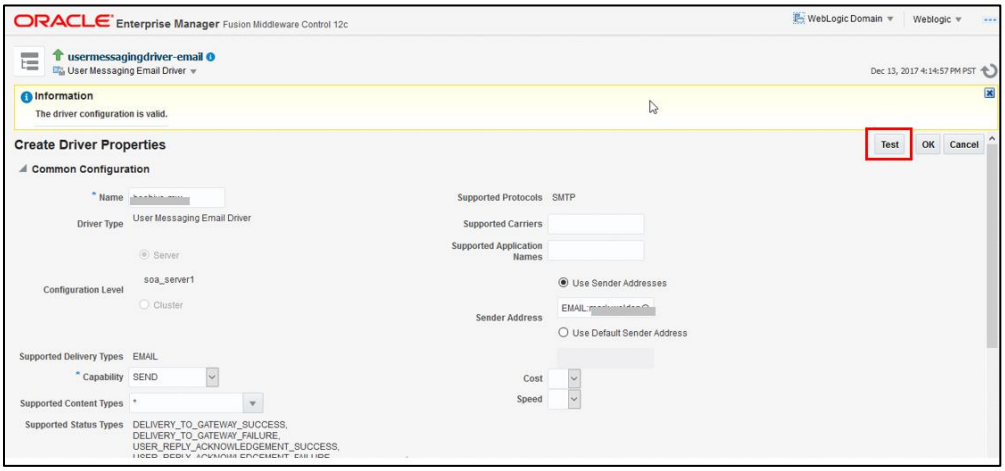



*Figure 47: Create Driver Properties screen*

# Troubleshooting

If the test gives a Fail to connect error or a review of the SOA server log shows a failed SSL handshake, it could be an issue with the security certificate.


*Figure 48: Error dialog*

## Verifying Trust Keystore

Open the WebLogic Server Administration Console to verify that the trust keystore used by the SOA server is the same system/trust were the security certificates were imported.

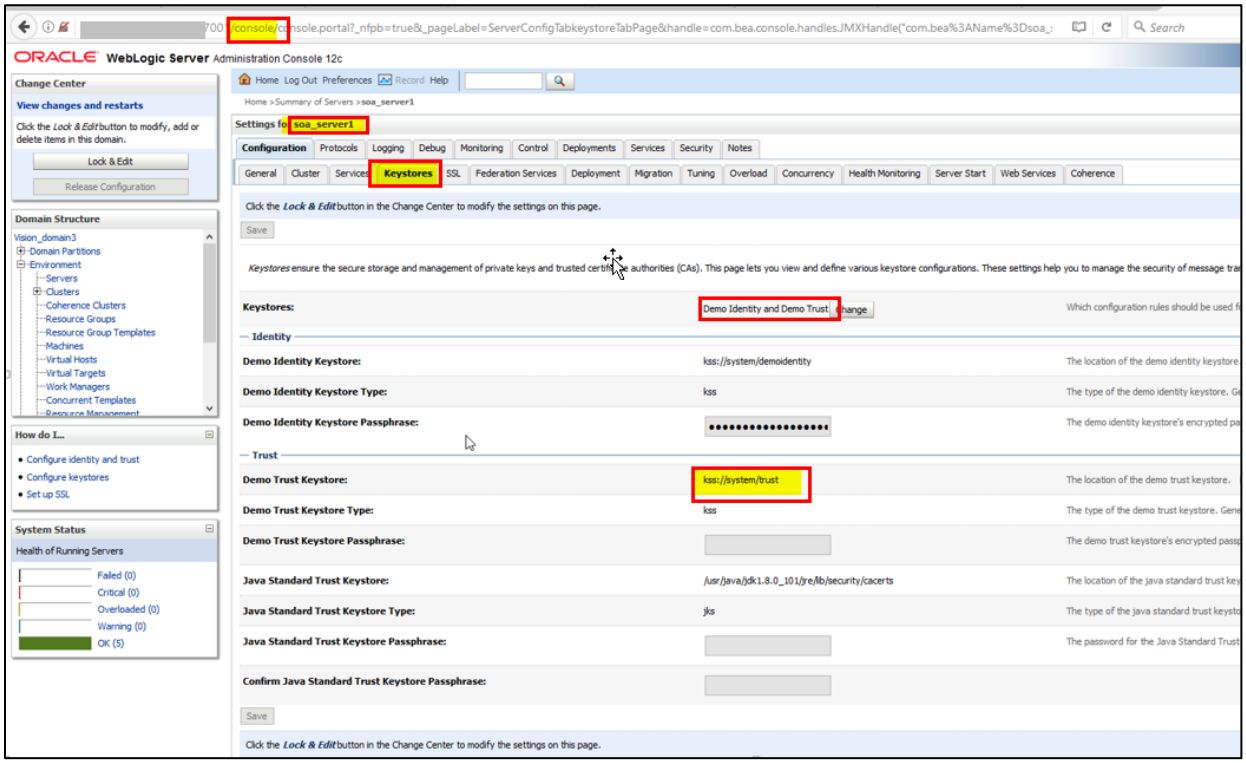



*Figure 49: WebLogic Server Administration Console*

## Reviewing the WebLogic start script

Review the WebLogic start script to verify that no extraneous keystore is being provided at startup. If there is, remove it and restart the WebLogic servers.

Edit the **setDomainEnv.sh** and remove the "**javax.net.ssl.trustStore**" property on the server start command `(… /bin/java -server …)` if there is one and restart the WebLogic servers.

# OIDG GNUPG ENCRYPTION AND DECRYPTION

OIDG supports GPG encrypted batch request processing .To support this you need to configure the GnuPG keys in your Linux machine. Following section describes the gpg-key creation.

## Verifying GnuPG-Agent

1. Login to Putty.
2. Run the GnuPG agent from application Linux user using below command.

   `gpg-agent`

   ```
   -bash-4.1$ gpg-agent
   gpg-agent: gpg-agent running and available
   -bash-4.1$
   ```

   **Output**: `gpg-agent: gpg-agent running and available`

3. If the output is `'No gpg-agent running in this session'`, follow the steps to run the gpg agent.
   - Enter the following command to run the gpg-agent

     `eval 'gpg-agent --daemon'`

     ```
     -bash-4.1$ eval 'gpg-agent --daemon'
     GPG_AGENT_INFO=/tmp/gpg-ExCSEX/S.gpg-agent:57227:1; export GPG_AGENT_INFO;
     ```

   - It shows the location of the GPG Agent file
     Now copy that file by following command

     `cp -fs /tmp/gpg-CENE8e/S.gpg-agent  ~/.gnupg/`

     ```
     -bash-4.1$ eval 'gpg-agent --daemon'
     GPG_AGENT_INFO=/tmp/gpg-ExCSEX/S.gpg-agent:57227:1; export GPG_AGENT_INFO;
     -bash-4.1$ cp -fs /tmp/gpg-ExCSEX/S.gpg-agent ~/.gnupg/
     ```

   - Verify the status of GPG- agent

     `gpg-agent`

     ```
     -bash-4.1$ gpg-agent
     gpg-agent: gpg-agent running and available
     -bash-4.1$
     ```

## Generating GnuPG Key

1. Login to putty with root user.

2. Give the permission to the gpg-agent by using the following command.

```
chmod o+rw $(tty)
```

3. Switch to the WebLogic installed user.
4. Enter the following command to create GPG Key.

```
gpg --gen-key
```

```
-bash-4.1$ gpg --gen-key
gpg (GnuPG) 2.0.14; Copyright (C) 2009 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection?
```

5. Enter 1 as your section option (RSA and RSA).

```
Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
```

6. Enter the Key size as 2048 and enter 0 for never expire.

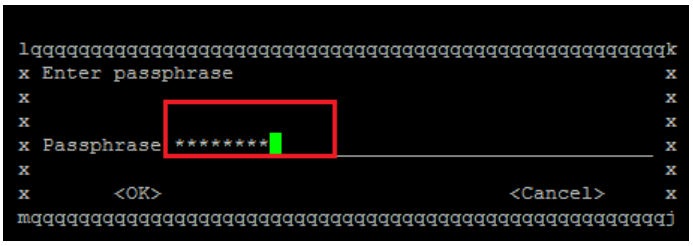
```
What keysize do you want? (2048) 2048
Requested keysize is 2048 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 0
Key does not expire at all
Is this correct? (y/N)
```

7. Enter y, Real name, Email Address and Comment.

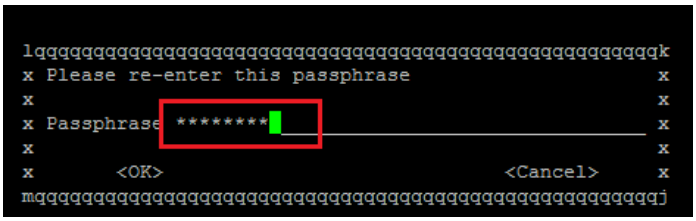
```
Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

Real name: oidg1
Email address: oidg1@oracle.com
Comment: Key generated
```

8. Enter 0.

9. Enter the GPG Password.

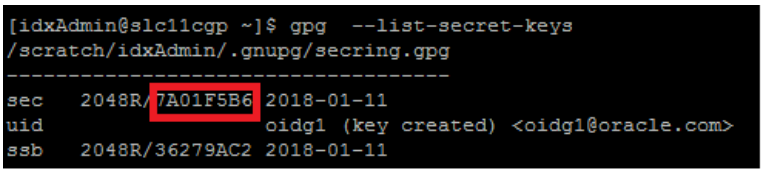



10. Reenter GPG Password.



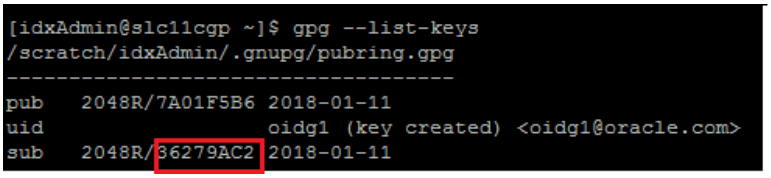

11. Now, you can check the key and secret keys using the following command:

```
gpg --list-secret-keys
```




12. Enter the below command to check List keys.

```
gpg --list-keys
```




# Exporting and Importing secret sub keys

## Exporting a secret key

```
gpg --export-secret-keys -a '<secret key id>' > Full path/gpgchefsecret.asc
```

**Note:** `<secret key id>` should be highlighted value of step 11 screenshot.

## Exporting a public key

```
gpg --armor --export  '<Email id>'> Full path /gpgchefpublic.asc
```

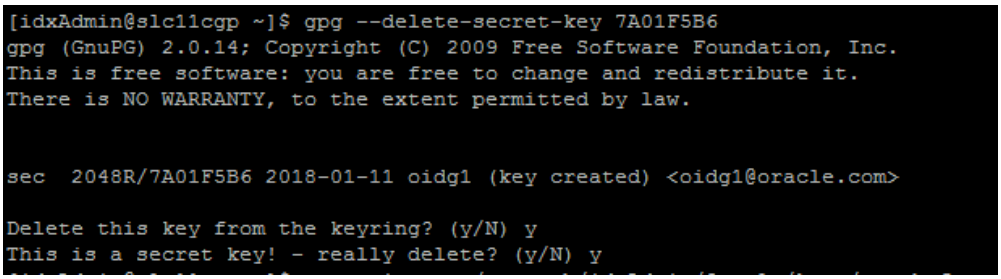
**Note:** `<Email id>` should be same as the one entered in the step 7.

## Backing up the secret and public key and deleting secrete key

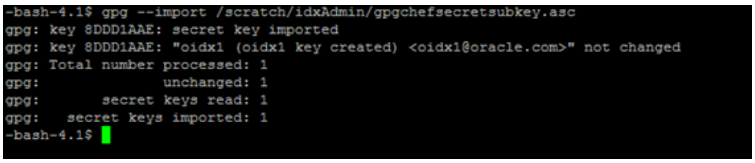
```
gpg --export-secret-subkeys '<sub id>' > Full path
/gpgchefsecretsubkey.asc
```

**Note:** `<sub id >` should be highlighted value of step 12 screenshot.

```
gpg --delete-secret-key '<secret key id>'
```



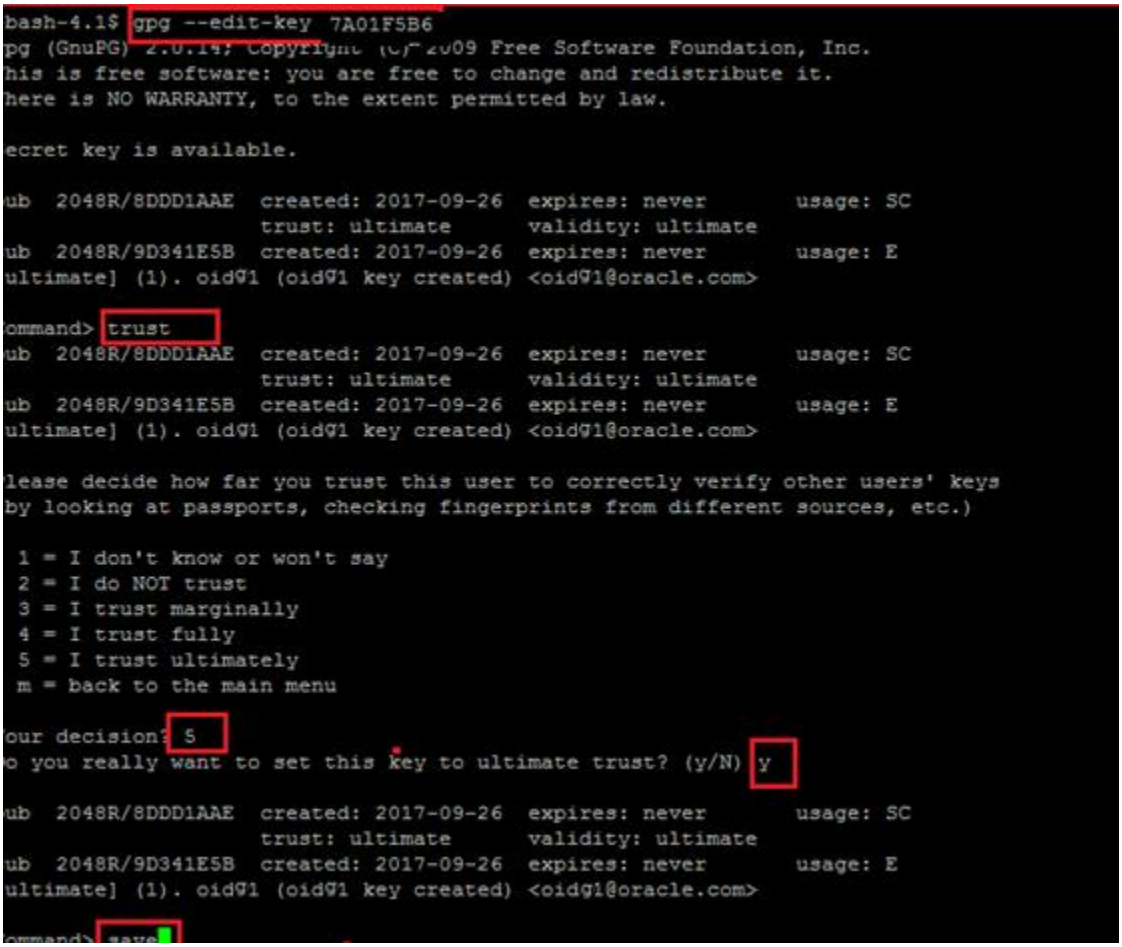

```
gpg --import Full path /gpgchefsecretsubkey.asc
```




# Trusting the keys

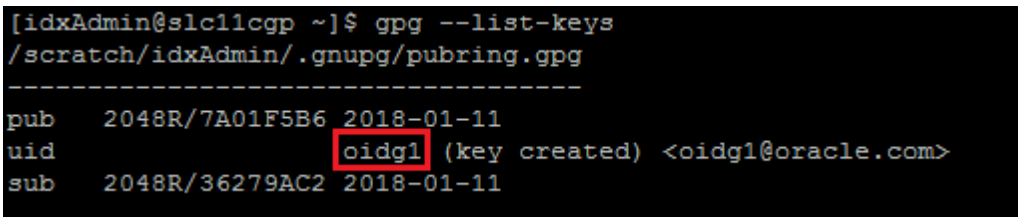
Trust the secret key by using the below command:

```
gpg --edit-key <secret key id>
Command> trust
Your decision? 5
Do you really want to set this key to ultimate trust? (y/n) y
Command> save
```




## Steps to find oidx.gpg.backup.key.id:

Enter `gpg -list-keys` command as shown below.




In the above screen, oidg1 is the backup key id.

## Testing the gpg:

Encrypt File:

```
gpg -e -r " <GPG KeyID> " <InputFilePath>/<InputFileName>
```

Example: gpg –e –r “oidg1” /scratch/oraBase/FileMove/POLMIG_1.xml

Decrypt File:

```
gpg --output <OutputFilePath>/<OutputFileName>--batch -passphrase
<Password> --decrypt<InputFilePath>/<InputFileName>
```

Example: gpg --output /scratch/oraBase/FileMove/POLMIG_TEST.xml --batch --passphrase Welcome123 --decrypt "/scratch/oraBase/FileMove/POLMIG_1.xml.gpg”