



Oracle Identity Governance 12c

Common Criteria Guide

Version 1.4

October 2024

Document prepared by



www.lightshipsec.com

Table of Contents

1	About this Guide	3
1.1	Overview	3
1.2	Audience	3
1.3	About the Common Criteria Evaluation.....	3
1.4	Conventions	5
1.5	Related Documents.....	6
2	Secure Acceptance and Update	7
2.1	Obtaining the TOE.....	7
2.2	Verifying the TOE	7
2.3	Prerequisites	9
2.4	TOE Environment.....	10
2.5	Installing the TOE.....	10
2.6	Starting and Stopping the TOE	41
3	Configuration Guidance	43
3.1	Enterprise Security Management.....	43
3.2	Security Audit	44
3.3	Identification and Authentication	45
3.4	Security Management	46
3.5	Protection of the TSF	48
3.6	Trusted Path/Channel	48

List of Tables

Table 1:	Evaluation Assumptions	5
Table 2:	Related Documents	6
Table 3:	Administrative Roles & Privileges.....	46

1 About this Guide

1.1 Overview

1 This guide provides supplemental instructions to achieve the Common Criteria evaluated configuration of the Oracle Identity Governance 12c and related information.

1.2 Audience

2 This guide is intended for system administrators and the various stakeholders involved in the Common Criteria evaluation. It is assumed that readers will use this guide in conjunction with the related documents listed in Table 2.

1.3 About the Common Criteria Evaluation

3 The Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) is an international standard for security certification of IT products and systems. More information is available at <https://www.commoncriteriaportal.org/>

1.3.1 Protection Profile Conformance

4 The Common Criteria evaluation was performed against the requirements of the Standard Protection Profile for Enterprise Security Management Identity and Credential Management (PP_ESM_ICM), v2.1 available at: https://www.commoncriteriaportal.org/files/ppfiles/PP_ESM_ICM_V2.1.pdf

1.3.2 Evaluated Software and Hardware

5 The TOE is the following software:

- Oracle Identity Governance 12c

6 The TOE is downloaded by users from the Oracle Identity & Access Management Downloads page at: <https://www.oracle.com/security/identity-management/technologies/downloads/>.

1.3.3 Evaluated Functions

7 The following functions have been evaluated under Common Criteria:

- **Enterprise Security Management.** The primary functionality of the TOE is to maintain the identity and credential lifecycle for organizational users. The TSF can define and maintain the organizational attributes of users, enroll and unenroll users, and impose controls that ensure that their authentication credentials (passwords) are sufficiently secure. Additionally, the TSF can associate various user attributes with the notion of an “identity” such that environmental systems and applications are configured for different users based on this identity.
For example, the TSF can associate a number of different office locations with a region and give users who are located in this region a certain set of permissions. As users enter the organization, leave the organization, or change their location, the change will be detected by the TSF so that the user permissions can be updated automatically. Administrators can also manually assign different attributes to organizational users. All updates to identity and credential data that require the TSF to connect to an external server are secured using TLS.

The TSF relies on an authentication server and data store in the Operational Environment to define its administrators and handle their authentication. This allows the TOE to rely on existing organizational user account and authentication information rather than introducing its own.

- **Security Audit.** The TOE generates audit records of its behavior and administrator activities. Audit data includes date, time, event type, subject identity, and other data as required. Audit data is written to a remote database over a secure connection and to the local file system of the server on which the TOE resides.
- **Identification and Authentication.** The TOE checks administrative privileges with each submitted request so that an active administrative session cannot be used to violate the principle of least privileges should that administrator's privileges be changed after the session has been established.
- **Security Management.** The TOE is managed by authorized administrators using a web GUI. Administrative privileges are defined by the TSF using identity data that is defined in the Operational Environment. The TOE can also define workflow steps such that administrative activities can be subjected to an approval process.
The TOE provides a set of out-of-the-box administrative roles with fixed privileges to manage different aspects of the TSF. In addition to direct administration, an organizational user can perform self-service by updating their organizational password or updating some of their personal attributes. These users can also initiate requests to be assigned privileges that can be subjected to a workflow approvals process to ensure that users can quickly be given appropriate privileges to perform their organizational responsibilities.
- **Protection of the TSF.** The TOE ensures that administrator credentials are hashed before being sent to the Operational Environment. If a user forgets their password and uses the recovery feature to access their account, the password will be reset. Similarly, the answers to user security questions (used for password recovery) are stored in a hashed format. The TOE also protects secret and private key data such that there is no mechanism to disclose this information and compromise the security of trusted communications.
- **Trusted Path/Channels.** The TOE allows trusted channels to be established between itself and the remote data stores (LDAP, RDBMS) and endpoint systems that it interfaces with. In addition, the TOE establishes a trusted path between authorized administrators and the TSF using HTTPS for the web GUI. All HTTPS and TLS functionality is provided by a third-party cryptographic module in the operational environment.

8

NOTE: No claims are made regarding any other security functionality.

1.3.4 Evaluation Assumptions

- 9 The following assumptions were made in performing the Common Criteria evaluation. The guidance shown in the table below should be followed to uphold these assumptions in the operational environment.

Table 1: Evaluation Assumptions

Assumption	Guidance
A.CRYPTO (optional) - The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.	Ensure the Operational Environment is capable of providing cryptographic primitives that can be used by the TOE to perform cryptographic operations.
A.ENROLLMENT - There will be a defined enrollment process that confirms user identity before the assignment of credentials.	Ensure that strong and reliable enrolment processes are in place to verify the identity of each user.
A.ESM - The TOE will be able to establish connectivity to other ESM products in order to share security data.	Ensure that network connectivity to additional ESM products in the environment is available.
A.FEDERATE - Third-party entities that exchange attribute data with the TOE are assumed to be trusted.	Ensure that only reliable and properly vetted third-party entities, whose purpose is to exchange attribute data with the TOE, are leveraged in the environment.
A.MANAGE - There will be one or more competent individuals assigned to install, configure, and operate the TOE.	Ensure that all administrators whose role includes the installation, configuration, and general operation of the TOE are competent and properly trained.
A.ROBUST (optional) - The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication.	Ensure that layered security controls are in place to detect impersonation of legitimate users and other authentication spoofing attacks.
A.SYSTIME (optional) - The TOE will receive reliable time data from the Operational Environment.	Ensure that reliable sources of time are redundantly available in the Operational Environment.

1.4 Conventions

- 10 The following conventions are used in this guide:

- CLI Command `<replaceable>` - This style indicates to you that you can type the word or phrase on the command line and press [Enter] to invoke a command. Text within `<>` is replaceable. For example:
Use the `cat <filename>` command to view the contents of a file
- [key] or [key-combo] – key or key combination on the keyboard is shown in this style. For example:

The [Ctrl]-[Alt]-[Backspace] key combination exits your graphical session and returns you to the graphical login screen or the console.

- **GUI => Reference** – denotes a sequence of GUI screen interactions. For example:
Select **File => Save** to save the file.
- **[REFERENCE] Section** – denotes a document and section reference from Table 2. For example:
Follow [ADMIN] *Configuring Users* to add a new user.

1.5 Related Documents

11 This guide supplements the below documents included with the TOE.

Table 2: Related Documents

Reference	Document
[ST]	Oracle Identity Governance 12c Security Target, latest version
[ADMIN]	Oracle Fusion Middleware Administering Oracle Identity Governance, 12c (12.2.1.4.0), E95926-14: https://docs.oracle.com/en/middleware/idm/identity-governance/12.2.1.4/omadm/administering-oracle-identity-governance.pdf
[SELF]	Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance, 12c (12.2.1.4.0), E95920-08: https://docs.oracle.com/en/middleware/idm/identity-governance/12.2.1.4/omusg/performing-self-service-tasks-oracle-identity-governance.pdf
[HELP]	Oracle Fusion Middleware Help Topics for Oracle Identity Governance, 12c (12.2.1.4.0), E95917-05: https://docs.oracle.com/en/middleware/idm/identity-governance/12.2.1.4/omhlp/help-topics-oracle-identity-governance.pdf

12 **NOTE:** The information in this guide supersedes related information in other documentation.

2 Secure Acceptance and Update

2.1 Obtaining the TOE

13 The Oracle Identity Governance 12c software is downloaded from the Oracle Identity & Access Management Downloads page located at:
<https://www.oracle.com/security/identity-management/technologies/downloads/>.

14 To obtain the TOE, download the following:

- Oracle Identity and Access Management 12cPS4 (Version 12.2.1.4.0)
- Oracle Identity and Access Management 12cPS4 Infrastructure (Version 12.2.1.4.0)

15 Patches 36822804, 36770738, 36553894, 1221422, 36805124 (for WebLogic), and 36513778 (for OIG) are downloaded by users from the My Oracle Support page at:
<https://support.oracle.com>.

16 The Oracle OID Connector is downloaded by users from the Oracle Identity Manager 12c Connectors Downloads page at: <https://www.oracle.com/security/identity-management/technologies/oim-connectors-downloads/>.

17 To obtain the OID Connector download the following:

- Oracle Internet Directory (Version 12.2.1.3.0)

18 **Note:** The OID connector 12.2.1.3.0 may also be referred to as the “ODSEE/LOUD/LDAPV3 Connector 12.2.1.3.0” in TOE guidance and GUI pages.

2.2 Verifying the TOE

2.2.1 Checksum

19 Customers can verify the SHA-256 checksum of the downloaded file(s) against the published hash by clicking “View Digest Details” on the Downloads page.

2.2.2 WebLogic and OIG Version and Patch Level

20 To verify the correct version of OIG and WebLogic are installed, administrators may perform the following:

- 1) On the Web GUI, click on the username in the top right corner.
- 2) On the drop-down menu, click **About**.

21 To verify the WebLogic and OIG patches, run the `opatch lsinventory` command from the Oracle Linux CLI.

2.2.3 OID Connector Version and Patch Level

22 To verify the version and patch level of the OID Connector, administrators may perform the following:

- 1) From the Oracle Linux CLI, run the DownloadJars.sh script from the `<OIM_HOME>\bin` directory, select Option 4 and download the jar file “org.identityconnectors.ldap-12.3.0.jar”.

Example:

```
$ sh DownloadJars.sh
```

For running the Utilities the following environment variables need to be set

```
APP_SERVER is weblogic
OIM_ORACLE_HOME is
/u01/app/oracle/product/12.2.1.4.0/oighome_1/idm
JAVA_HOME is /u01/app/oracle/product/jdk
MW_HOME is /u01/app/oracle/product/12.2.1.4.0/oighome_1
WL_HOME is /u01/app/oracle/product/12.2.1.4.0/oighome_1/wlserver
DOMAIN_HOME is
/u01/app/oracle/product/12.2.1.4.0/oighome_1/domains/base_domain
Executing oracle.iam.platformservice.utils.JarDownloadUtility in
IPv4 mode

[Enter Xellerate admin username :]xelsysadm

[Enter the admin password :]

[[Enter serverURL (Ex. t3://oimhostname:oimportno for weblogic or
corbaloc:iiop:localhost:2801 for
websphere)]:]t3://oig.example.com:14000

[[Enter context (i.e.: weblogic.jndi.WLInitialContextFactory for
weblogic or com.ibm.websphere.naming.WsnInitialContextFactory for
websphere)]:]weblogic.jndi.WLInitialContextFactory
```

Enter the jar type

```
1.JavaTasks
2.ScheduleTask
3.ThirdParty
4.ICFBundle
4
```

Enter the full path of the download directory :

```
/home/oracle/Downloads
```

Enter the name of jar file to be downloaded from DB :

```
org.identityconnectors.ldap-12.3.0.jar
```

Do u want to download more jars [y/n] :n

Download jar executed successfully

- 2) Extract the connector jar file with the command `jar -xvf org.identityconnectors.ldap-12.3.0.jar`.

Example:

```
$ jar -xvf org.identityconnectors.ldap-12.3.0.jar
created: META-INF/
inflated: META-INF/MANIFEST.MF
```

- 3) Show the manifest file contents with the command `cat META-INF/MANIFEST.MF`.

Example:

```
$ cat META-INF/MANIFEST.MF
Manifest-Version: 1.0
```



```
Ant-Version: Apache Ant 1.9.2
Created-By: 1.8.0_40-ea-b08 (Oracle Corporation)
Specification-Title: IdentityConnectors-Ldap
Specification-Version: 12.3.0
Specification-Vendor: Oracle Corporation
Implementation-Title: org.identityconnectors.ldap
Implementation-Version:
OIMCP_12.2.1.3.0GENERICLDAP_GENERIC_RELEASE
Implementation-Vendor: Oracle Corporation
ConnectorBundle-FrameworkVersion: 1.1
ConnectorBundle-Name: org.identityconnectors.ldap
ConnectorBundle-Version: 12.3.0
Build-Label: OIMCP_12.2.1.3.0GENERICLDAP_GENERIC_RELEASE
ConnectorPatch-Version: 36910321-OID12.2.1.3.0L
```

```
Name: org/identityconnectors/ldap
```

2.3 Prerequisites

Virtual Machine Minimum Requirements

- **Oracle Database:**
 - i) **OS:** Oracle Linux 8.4
 - ii) **Storage:** 128 GB of Drive Space
 - iii) **Memory:** 16 GB of Memory
 - iv) **Processor:** 4 or more CPU Cores
- **Oracle Unified Directory**
 - i) **OS:** Oracle Linux 8.4
 - ii) **Storage:** 64 GB of Volume Space
 - iii) **Memory:** 8 GB of Memory
 - iv) **Processor:** 4 or more CPU Cores
- **Oracle Identity Governance**
 - i) **OS:** Oracle Linux 8.4
 - ii) **Storage:** 64 GB of Volume Space
 - iii) **Memory:** 8 GB of Memory
 - iv) **Processor:** 4 or more CPU Cores

2.4 TOE Environment

2.4.1 Oracle Database

23 The operational environment requires an instance of Oracle Database 19c (19.3) to be available. The database must be configured to have an SSL/TLS capable listener on port 2484. It may be necessary to ensure a distinct Oracle database instance for your OIG environment.

24 Contact your IT administration team and/or your Oracle Support representative to ensure the Oracle Database is available for use.

2.4.2 Oracle Unified Directory

25 The operational environment requires an instance of Oracle OUD 12cPS4 (12.2.1.4.0) to be available. The OUD instance must be configured to have an SSL/TLS capable listener on port 1636.

26 Contact your IT administration team and/or your Oracle Support representative to ensure the Oracle Unified Directory server is available for use.

2.5 Installing the TOE

Note: The TOE must be deployed by Oracle Support to ensure it is in the evaluated configuration.

2.5.1 Install and Configure OIG

2.5.1.1 Install Java

27 Download Java SE Runtime Environment 8u421 from the following location:
<https://www.oracle.com/java/technologies/downloads/>

28 Install the RPM using the Software Manager

2.5.1.2 Set JAVA_HOME / Path

29 As the root user in the OIG server, set the JAVA_HOME / Path to your OIG VM in the /etc/environment file to include the following:

- /u01/app/oracle/product/jdk/bin
- /u01/app/oracle/product/jdk/jre/bin

30 The PATH variables must be separated by a colon.

31 Add the following environment variables at the end of the file.

- JAVA_HOME="/u01/app/oracle/product/jdk"

32 An example of the environment file after modification is:

```
PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/u01/app/oracle/product/jdk/bin:/u01/app/oracle/product/jdk/jre/bin"
```

```
JAVA_HOME="/u01/app/oracle/product/jdk"
```

33 Create a symlink for "/u01/app/oracle/product/jdk" to "/usr/java/jdk1.8.0_421-amd64" (or similar installation default).

34 Enter the following commands to inform the system about the Java's location. Depending on your JDK version, the paths can be different.

- `sudo update-alternatives --install "/usr/bin/java" "java" "/usr/java/jdk1.8.0_421-amd64/bin/java" 0`
- `sudo update-alternatives --install "/usr/bin/javac" "javac" "/usr/java/jdk1.8.0_421-amd64/bin/javac" 0`
- `sudo update-alternatives --set java /usr/java/jdk1.8.0_421-amd64/bin/java`
- `sudo update-alternatives --set javac /usr/java/jdk1.8.0_421-amd64/bin/javac`

2.5.1.3 Enable FIPS Mode

35 To enable FIPS mode on the system, run the following command:

- `sudo fips-mode-setup --enable`

36 The following output is displayed:

- Setting system policy to FIPS
- FIPS mode will be enabled.
- Please reboot the system for the setting to take effect.
- You must reboot the system for the setting to take effect.

37 Running the previous command configures FIPS mode implicitly by setting the system-wide cryptographic policy to FIPS. Note that using the `update-crypto-policies` command to set FIPS mode is not sufficient, as shown in the following output:

- `sudo update-crypto-policies --set FIPS`

38 The following output is displayed:

- Warning: Using 'update-crypto-policies --set FIPS' is not sufficient for FIPS compliance.
- Use 'fips-mode-setup --enable' command instead.

39 Verify that FIPS is enabled by running any of the following commands:

- `sudo fips-mode-setup --check`
- `sudo update-crypto-policies --show`
- `sudo cat /etc/system-fips`
- `sudo sysctl crypto.fips_enabled`

40 For the command output in the last example, a response of 1 indicates that FIPS is enabled.

2.5.1.4 Download and Install OIG Binaries

41 From the Identify and Access Management Downloads page here:

<https://www.oracle.com/security/identity-management/technologies/downloads/>

42 Download the following binaries and unzip them into a staging area such as /u01/STAGE:

- `fmw_12.2.1.4.0_infrastructure.jar`
- `fmw_12.2.1.4.0_soa.jar`
- `fmw_12.2.1.4.0_idm.jar`

2.5.1.5 Install Fusion Middleware Infrastructure

43 As the 'root' user, perform the following steps:

- `mkdir -p /u01/app`
- `chown -R oracle:orainstall /u01`

44 While logged in as the 'oracle' user on the local Oracle Linux console for the OIG server, run the installer:

- `java -jar /u01/STAGE/fmw_12.2.1.4.0_infrastructure.jar`

45 Work through the wizard.

46 For more information refer to <https://docs.oracle.com/en/middleware/fusion-middleware/12.2.1.4/inoam/index.html>.



47 Click "OK" and then go back to a terminal on the OIG server. As the 'oracle' user run the following command to create a new central inventory file for subsequent installations:

- `cd /u01/app/orainventory`
- `./createCentralInventory.sh`

48 Switch back to the graphical wizard and work through the panes.

1. The first is the Welcome screen. Click "Next" to proceed.
2. The second screen is the "Auto Updates" screen. Configure this according to your organizational policy. Click "Next".

3. Next is the Installation Location. For the remainder of this guide, we assume that the product is installed in `/u01/app/oracle/product/12.2.1.4.0/oighome_1`.

Note that this path will be referred to as `ORACLE_HOME`.

Click “Next”.

4. Next is the Installation Type. Select the “Fusion Middleware Infrastructure” radio button and click “Next”.
5. The wizard will perform Prerequisite Checks. When it is complete, click “Next”.
6. The Installation Summary provides an overview of what the installation will execute. Click “Install” to proceed.
7. The Installation Progress is shown. When completed, click “Next”.
8. At the final Installation Complete screen, click “Finish” to terminate the wizard.

2.5.1.6 Install SOA Binaries

49 While logged in as the ‘oracle’ user on the local Oracle Linux console for the OIG server, run the installer:

- `java -jar /u01/STAGE/fmw_12.2.1.4.0_soa.jar`

50 Work through the wizard by clicking “OK” to start.

51 For more information refer to <https://docs.oracle.com/en/middleware/fusion-middleware/12.2.1.4/insoa/index.html>.

1. The first is the Welcome screen. Click “Next” to proceed.
2. The second screen is the “Auto Updates” screen. Configure this according to your organizational policy. Click “Next”.
Next is the Installation Location. Use the same location as `ORACLE_HOME` from the Infrastructure installation above. Click “Next”.
3. Next is the Installation Type. Select the “SOA Suite” radio button and click “Next”.
4. The wizard will perform Prerequisite Checks. When it is complete, click “Next”.
5. The Installation Summary provides an overview of what the installation will execute. Click “Install” to proceed.
6. The Installation Progress is shown. When completed, click “Next”.
7. At the final Installation Complete screen, click “Finish” to terminate the wizard.

2.5.1.7 Install OIG Binaries

52 While logged in as the ‘oracle’ user on the local Oracle Linux console for the OIG server, run the installer:

- `java -jar /u01/STAGE/fmw_12.2.1.4.0_idm.jar`

53 Work through the wizard by clicking “OK” to start.

54 For more information, refer to <https://docs.oracle.com/en/middleware/idm/identity-governance/12.2.1.4/install.html>.

1. The first is the Welcome screen. Click “Next” to proceed.
2. The second screen is the “Auto Updates” screen. Configure this according to your organizational policy. Click “Next”.
Next is the Installation Location. Use the same location as ORACLE_HOME from the Infrastructure installation above. Click “Next”.
3. Next is the Installation Type. Select the “Collocated Oracle Identity and Access Manager (Managed through WebLogic Server)” radio button and click “Next”.
4. The wizard will perform Prerequisite Checks. When it is complete, click “Next”.
5. The Installation Summary provides an overview of what the installation will execute. Click “Install” to proceed.
6. The Installation Progress is shown. When completed, click “Next”.
7. At the final Installation Complete screen, click “Finish” to terminate the wizard.

2.5.1.8 Run the Repository Creation Utility

55 As the ‘oracle’ user running on the local Oracle Linux GUI console, run the following:

- \$ORACLE_HOME/oracle_common/bin/rcu

56 Work through the wizard.

1. The first is the Welcome screen. Click “Next” to proceed.
2. The second screen is the “Create Repository” screen. Initially, you want to “Create Repository” and select the appropriate radio button representing your specific situation. For the purposes of this Guide, we assume you are also the DBA and therefore select “System Load and Product Load”. Click Next.
3. Next is the Database Connection Details. Complete this screen using the details of your already configured Oracle Database. When completed, it will look something like the below. Ensure that the port is the plaintext port for now (normally port 1521).

Repository Creation Utility - Step 3 of 8

Repository Creation Utility

ORACLE
FUSION MIDDLEWARE

Welcome
Create Repository
Database Connection
Select Components
Schema Passwords
Map Tablespaces
Summary
Completion Summary

Database Type: Oracle Database

Connection String Format: Connection Parameters Connection String

Connect String:

Host Name: oigdb.example.com

Port: 1521

Service Name: IDMDB

Username: sys

Password:

Role: SYSDBA

4. Click Next. The RCU will perform Prerequisite Checks. When it is complete, click "OK".
5. The next screen is where you Select Components. One of the most important things on this screen is to pick a prefix for the schemas to ensure they are unique. The default prefix is "DEV", but ensure you pick one that meets your organizational requirements.

In the Component list, check the box for "IDM Schemas > Oracle Identity Manager". This will automatically select the required child components. However, to avoid any doubt, select the following:

- AS Common Schemas:
 - Common Infrastructure Services
 - Oracle Platform Security Services
 - User Messaging Service
 - Audit Services
 - Audit Services Append
 - Audit Services Viewer
 - Metadata Services
 - Weblogic Services
- SOA Suite
 - SOA Infrastructure
- IDM Schemas
 - Oracle Identity Manager

Click "Next".

At this point, you may get warnings/errors about cursors and/or views. If you do, then perform the following as the 'oracle' user:

- Open a terminal and type: `sqlplus sys as sysdba` and authenticate to the Oracle database.¹
- Execute the following commands, respectfully, as relevant:
 - If cursors are the problem: `alter system set open_cursors=800 scope=spfile;`
 - If views are the problem:
`@/opt/oracle/product/19c/dbhome_1/rdbms/admin/xaview.sql`

After changing the cursors/views for the correct database instance you can click "IGNORE" for the first warning instance and that should be the last time you see it.

6. The next screen allows us to set the Schema Passwords. Set passwords appropriate for your organizational policies. Note however, that this password cannot use all extended characters such as '!'.

We will refer to this as "\$SCHEMA_PASSWORD" and we will make reference to it later.

Click "Next".

7. The next screen allows us to set Custom Variables. There is no need to change anything here unless required by your Oracle Support representative. Click "Next".
8. The Map Tablespaces screen is shown. There are no required changes to be made here. Click "Next" to create the tables.
9. Some last-minute checks are made, click "OK" and then click "Next".
10. At the Summary screen, click "Create" to construct the tables.
11. At the final Completion Summary screen, click "Finish" to terminate the wizard.

2.5.1.9 Configure The WebLogic Domain

57 As the 'oracle' user running on a local GUI console, run the following:

1. `$ORACLE_HOME/oracle_common/common/bin/config.sh`

58 Work through the wizard.

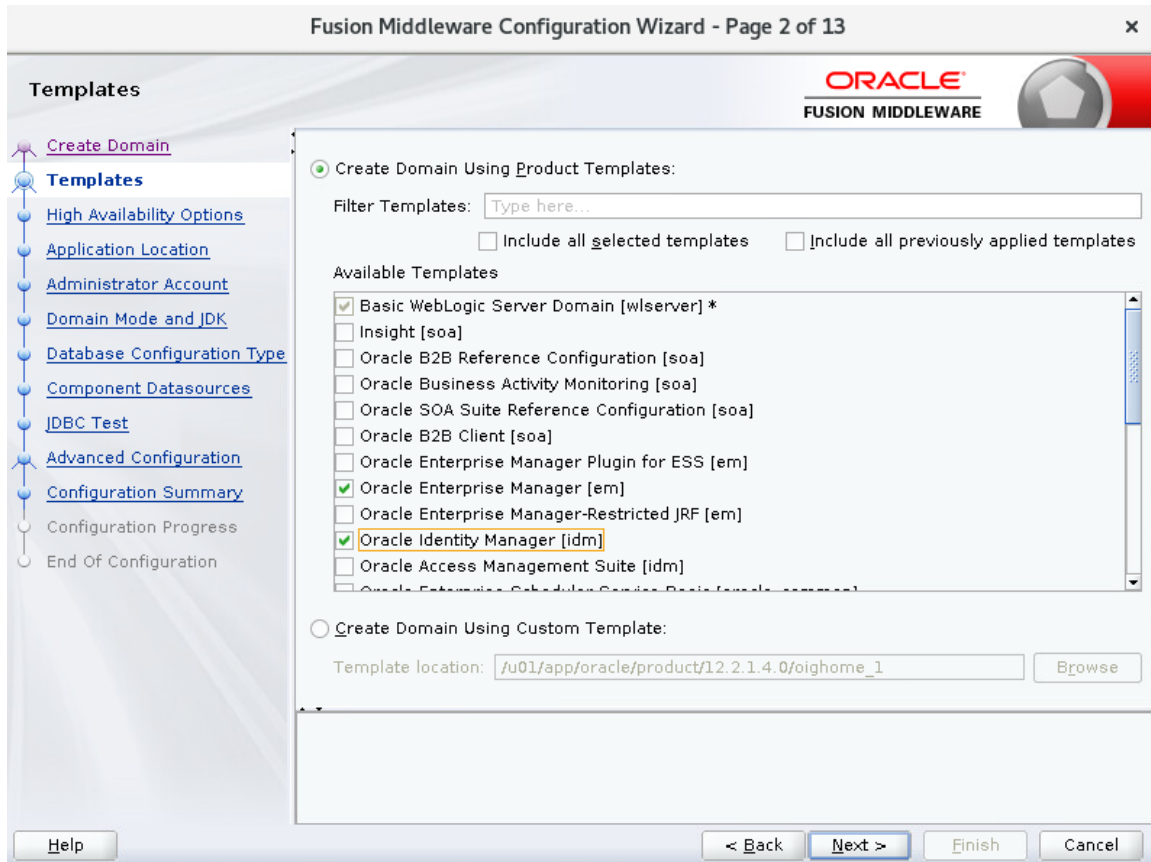
1. The first is the Create Domain screen. Create a new domain and enter a new domain such as `$ORACLE_HOME/domains/base_domain`². This will be known as `$DOMAIN_HOME`.

Click "Next" to proceed.

¹ If necessary prefix the `sqlplus` command with `ORACLE_SID=<DBINSTANCE>` where `DBINSTANCE` is the name of the database for the OIG install.

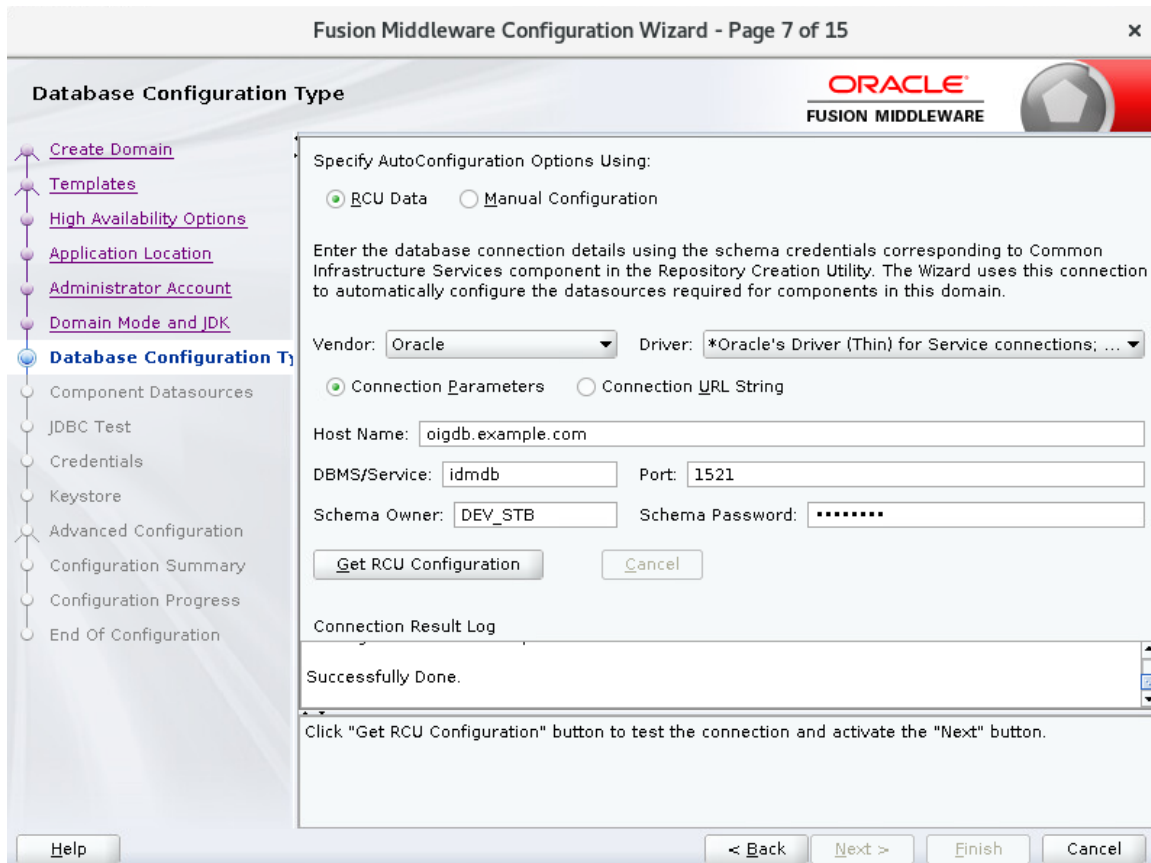
² We use `$ORACLE_HOME` as a placeholder for the previously constructed base installation. Expand this placeholder into the full path in the wizard or use an entirely distinct path for your domain.

- In the Templates screen, choose “Create Domain Using Product Templates” and select ONLY “Oracle Identity Manager [idm]” checkbox. This will cause other child products to be selected at the same time such as “Oracle Enterprise Manager [em]” and others. No other checkboxes need to be selected. Click “Next”.



- In the High Availability Options screen, keep the defaults unless otherwise directed by your Oracle Support representative. Click “Next”.
- In the Application Location screen, set the path for the application location. Click “Next”.
- In the Administrator Account screen, choose an administrative account credential. By default, the username is “weblogic”. Select credentials that meet your organizational policies. Note the restrictions described in the wizard on the username and password. Click “Next”.
- The next screen sets the Domain Mode and JDK. Set these according to your Oracle Support representative and your intended function. The JDK path should be the path where you installed Java earlier. Click “Next”.
- The next screen sets the Database Configuration. This is a busy screen. Select the “RCU Data” radio button and fill out the database connection details accordingly. Note that you must use the plaintext port (default 1521). The “schema password” is \$SCHEMA_PASSWORD for the appropriate schema owner set earlier during the RCU creation step.

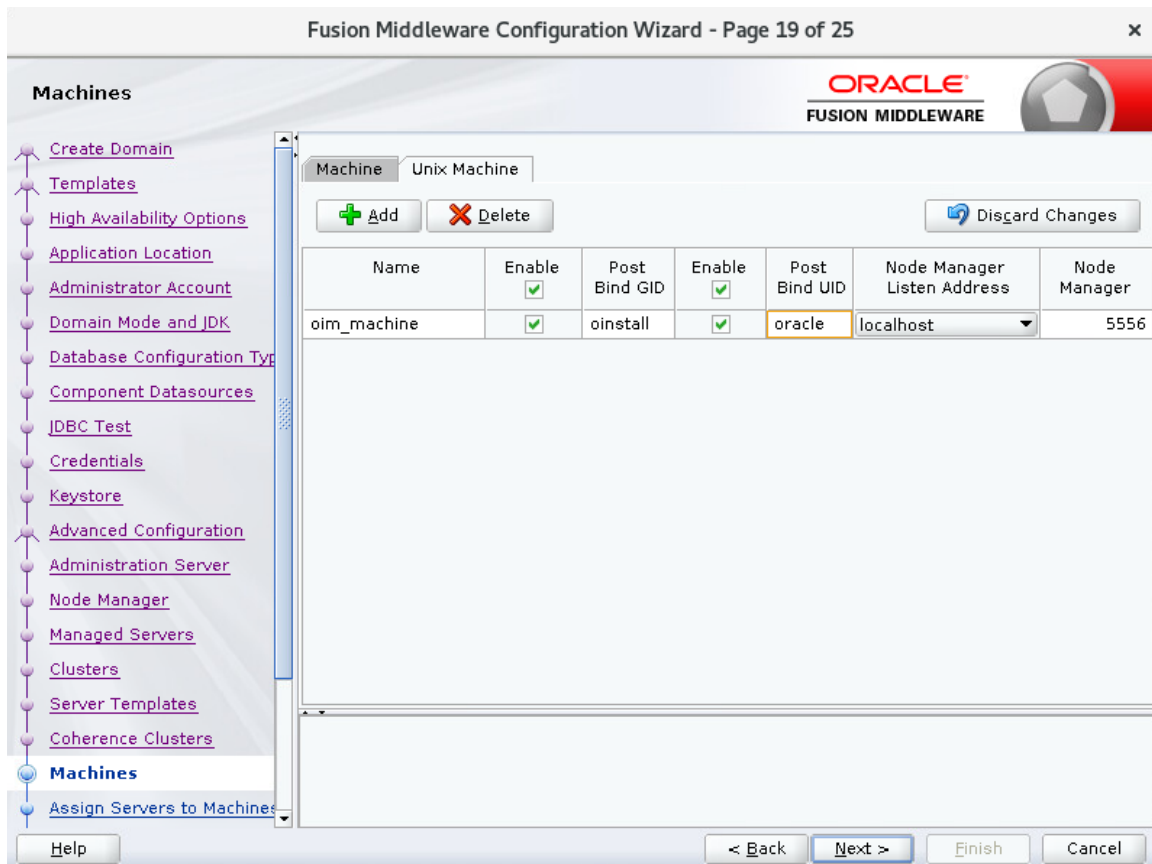
Click on the “Get RUC Configuration” to acquire the necessary database properties and click “Next”.



8. The Component Datasources screen needs no changes made. Click “Next” to continue.
9. The next screen will test the connections to each of the datasources in turn. Wait for the tests to pass and then click “Next”.
10. In the Credentials screen you need to set four credentials, each with a different purpose:
 - Keystore: the username and password for the keystore. The username should be set to “keystore”.
 - OIMSchemaPassword: the username is the schema username for the OIM schema. Assuming you used the DEV prefix and the default schema name from the RCU creation, the schema username is DEV_OIM. The password must be the proper \$SCHEMA_PASSWORD for the DEV_OIM schema owner.
 - sysadmin: this is the username and password for the OIM system. The username should be set to “xelsysadm”.
 - WeblogicAdminKey: this is a password key for the weblogic system administrator.

11. The next screen is the Keystore screen. No changes are needed here. Click "Next" to continue.
12. In the Advanced Configuration screen, select at least the "Topology" checkbox. You may wish to also select the "Administration Server", and "Node Manager" checkboxes. As you check each of these checkboxes, additional panels are added in the left-hand side of the wizard.

Click "Next" to continue.
13. If you selected "Administration Server", then in the Administration Server screen, configure the listening properties as per your organizational policy. Ensure that the "Enable SSL" box is checked and that the "SSL Listen Port" is set to 7002. Click "Next".
14. If you selected "Node Manager", then in the Node Manager screen, you need to configure the Node Manager properties. Select "Per Domain Default Location" and select a username for the node manager and an appropriate password. Note that if you did not select "Node Manager" in the Advanced Configuration screen, then the Node Manager is provisioned without a username and password. Click "Next".
15. In the Managed Servers screen, you are shown two servers: oim_server1 and soa_server1. The server listening properties are shown. Adjust as required. However, ensure that "Enable SSL" is checked for all of them and verify the SSL port is appropriate for your environment. Click "Next".
16. If your environment requires Clusters, then configure them in this screen, otherwise leave the cluster definition blank and click "Next".
17. In the Server Templates screen, make any changes needed as per your Oracle Support Representative. Ensure that the "Enable SSL" button is enabled for all of them. Click "Next".
18. In the Coherence Clusters screen, no changes are needed unless directed by your Oracle Support representative. Click "Next".
19. In the Machines screen, click on the "Unix Machine" tab and create at least one machine definition. Give the machine a name such as "oig_machine". Click the "Enable" checkbox to enable it. Set the Post Bind GID and the Post Bind UID as required (or leave blank to run with the default credentials). The Node Manager listen address must be set to "localhost" and the port to the Node Manager listening port. In the evaluated configuration, the Node Manager runs on the same machine as the WebLogic/OIG servers. Click "Next".



20. In the next screen, you Assign Servers to Machines. Select servers in the left-hand side of the split-view and select the machine(s) in the right-hand side of the split view. Click the ">" and "<" icons in the middle of the split to move servers to and from machines. All servers need to be assigned to at least one machine. When satisfied, click "Next".
21. In the Virtual Targets screen, make no changes unless required by your Oracle Support representative. Click "Next".
22. In the Partitions screen, make no changes unless required by your Oracle Support representative. Click "Next".
23. In the Configuration Summary screen, it will summarize all of the selections and options made during the wizard. Go back to make changes if required. Otherwise, click "Create" to construct the OIG instance and all associated servers and settings.
24. The installation will progress on the Configuration Progress screen. Click "Next" to advance.
25. On the End of Configuration screen, click "Finish" to complete the wizard.

2.5.1.10 Post Installation

59 Now that everything is installed, and the domain is configured, we need to update our environment variables to make sure DOMAIN_HOME is pointing to our installations.

60 As the root user in the OIG server, edit the /etc/environment file to include an environment variable for DOMAIN_HOME which points to the configured domain home that was defined above.

61 Next we need to run the offlineConfigManager

- cd \$ORACLE_HOME/idm/server/bin³
- ./offlineConfigManager.sh

62 Watch the output of the command and make sure there are no errors.

2.5.1.11 Enabling FIPS 140-2 Mode From java.security

63 To enable FIPS 140-2 mode from the installed JDK java.security file, follow these steps:

64 Edit the java.security file. Add both the RSA JCE provider and the RSA JSSE provider as the first two Java security providers listed in the java.security properties file:

```
#
security.provider.1=com.rsa.jsafe.provider.JsafeJCE
security.provider.2=com.rsa.jsse.JsseProvider
:
```

65 Put the jcmFIPS.jar jar and sslj.jar JAR files (both are found in \$ORACLE_HOME/wlserver/server/lib/) at the head of the classpath. You can use the PRE_CLASSPATH environment variable to do this. (The RSA JCE provider Crypto-J is located in cryptoj.jar and is in the classpath by default.)

66 Make a copy of \$DOMAIN_HOME/bin/setDomainEnv.sh and \$DOMAIN_HOME/bin/startNodeManager.sh. Within these files, at the top, add something similar to the following:

```
export
PRE_CLASSPATH=/u01/app/oracle/product/12.2.1.4.0/oighome_1/wlserver/server/
lib/jcmFIPS.jar:/u01/app/oracle/product/12.2.1.4.0/oighome_1/wlserver/
server/lib/sslj.jar
```

67 **Note:** Use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.

2.5.1.12 Verifying JCE When FIPS 140-2 Mode is Enabled

68 During normal WebLogic startup, for performance reasons the RSA Crypto-J JCE Self-Integrity test is disabled.

69 If you want to make sure that JCE verification is enabled when configuring WLS for FIPS 140-2 mode, set

³ Ensure you actually CHANGE to this directory and then run the tool otherwise there are problems.

the `-Dweblogic.security.allowCryptoJDefaultJCEVerification=true` JAVA_OPTIONS environment variable when you start WebLogic Server. This is best done within the `$DOMAIN_HOME/bin/setDomainEnv.sh` file by placing a line similar to the following at the top of the file:

```
export
JAVA_OPTIONS="{JAVA_OPTIONS} -Dweblogic.security.allowCryptoJDefaultJCE
Verification=true "
```

70 Note that setting this environment variable adds additional processing and time to the startup.

2.5.1.13 Construct Wallet, JKS Keystore and Certificate files

71 Logged in as the 'oracle' user on the OIG server, perform a series of steps to create a PKI wallet to store a server public/private keypair. (The sequence of steps may differ depending on the exact environment.)

72 For wallet operations, each wallet needs to have a password. We will refer to this as the "SIMPLE_PASSWORD".

73 The following will create an empty wallet:

- `mkdir -p /home/oracle/oig_wallet`
- `$ORACLE_HOME/bin/orapki wallet create -wallet ~/oig_wallet -pwd <SIMPLE_PASSWORD> -auto_login`

74 Then, you need to create a new public/private key pair. The public key will be associated with a Distinguished Name (DN). The DN in our example below uses a Common Name of "oig.example.com" which is the hypothetical name given to the OIG server in our environment. Ensure you use your own hostname. While the example below constructs a 4096-bit RSA key, the key built for your own environment may be a different size (between 2048 bits and 4096 bits) or use elliptic curve cryptography (ECC) instead using appropriate NIST named curves.

- `$ORACLE_HOME/bin/orapki wallet add -wallet ~/oig_wallet -dn cn=oig.example.com -asym_alg RSA -keysize 4096 -pwd <SIMPLE_PASSWORD>`

75 Next, export the Certificate Signing Request (CSR) to be signed by your environment CA:

- `$ORACLE_HOME/bin/orapki wallet export -wallet ~/oig_wallet -dn cn=oig.example.com -request ~/oig.example.com.csr.pem -pwd <SIMPLE_PASSWORD>`

76 Have the CSR signed by the CA which will result in a certificate file (which we will call `oig.example.com.cert.pem`). This certificate file needs to be re-imported into the wallet along with any certificate validation chain provided by the CA.

- `$ORACLE_HOME/bin/orapki wallet add -wallet ~/oig_wallet -trusted_cert -cert ~/ca-chain.pem -pwd <SIMPLE_PASSWORD>`
- `$ORACLE_HOME/bin/orapki wallet add -wallet ~/oig_wallet -user_cert -cert ~/oig.example.com.cert.pem -pwd <SIMPLE_PASSWORD>`

77 Finally, you can display the set of certificates in your wallet to ensure that they are consistent with the configuration:

- `$ORACLE_HOME/bin/orapki wallet display -wallet ~/oig_wallet -pwd <SIMPLE_PASSWORD>`

- 78 Convert the wallet to a pair of Java keystores – one for the public/private key pair and another containing the certificates for the trusted chain:
- `$OUDHOME/oracle_common/bin/orapki wallet pkcs12_to_jks -wallet ~/oud_wallet/ewallet.p12 -pwd <SIMPLE_PASSWORD> -jksKeyStoreLoc ~/oud_wallet/oud.jks -jksKeyStorepwd <SIMPLE_PASSWORD> -jksTrustStoreLoc ~/oud_wallet/trustStore.jks -jksTrustStorepwd <SIMPLE_PASSWORD>`
- 79 Convert the trust key store to FIPS compliant format.
- `keytool -importkeystore -srckeystore ewallet.p12 -srcstoretype PKCS12 -srcprovidername JsafeJCE -destkeystore DemoTrust.rsa -deststoretype PKCS12 -destprovidername JsafeJCE -providerclass com.rsa.jsafe.provider.JsafeJCE -providerpath $CLASSPATH`
- 80 Convert the identity key store to PKCS12 format.
- `keytool -importkeystore -srckeystore Demoidentity.jks -srcstoretype jks -destkeystore DemoTrust.p12 -deststoretype pkcs12`
- 81 Convert the identity key store to FIPS compliant format.
- `keytool -importkeystore -srckeystore Demoidentity.p12 -srcstoretype PKCS12 -srcprovidername JsafeJCE -destkeystore Demoidentity.rsa -deststoretype PKCS12 -destprovidername JsafeJCE -providerclass com.rsa.jsafe.provider.JsafeJCE -providerpath $CLASSPATH`
- 82 Verify FIPS compliant key store details
- `keytool -list -keystore DemoTrust.rsa -storetype PKCS12 -providerclass com.rsa.jsafe.provider.JsafeJCE -providerpath $CLASSPATH -providername JsafeJCE`
 - `keytool -list -keystore Demoidentity.rsa -storetype PKCS12 -providerclass com.rsa.jsafe.provider.JsafeJCE -providerpath $CLASSPATH -providername JsafeJCE`
- 83 Extract the private key from the PKCS#12 ewallet file and convert to PEM format:
- `openssl pkcs12 -in ~/oig_wallet/ewallet.p12 -out ~/oam_key.pem -nocerts -nodes -passin pass:<SIMPLE_PASSWORD>`
- 84 After this conversion, the /home/oracle/oam_key.pem file will contain text above the “BEGIN PRIVATE KEY” which needs to be removed before it can be used. Edit the file accordingly.
- 85 Convert the PEM private key to DER format:
- `openssl pkcs8 -topk8 -nocrypt -in ~/oam_key.pem -inform PEM -out ~/oam_key.der -outform DER`
- 86 Finally, convert the PEM formatted server certificate to DER format:
- `openssl x509 -in oig.example.com.cert.pem -out oig.example.com.cert.der -outform DER`

- 87 For more information on the orapki tool, please see <https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/using-the-orapki-utility-to-manage-pki-elements.html>.
- 88 To finish the remainder of the certification setup, update the Java nodemanager.properties \$DOMAIN_HOME/nodemanager directory with the following entries.

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityAlias=Demoidentity
CustomIdentityKeyStoreFileName=/opt/oracle/Domains/
Identity/security/Demoidentity.rsa
CustomIdentityKeyStorePassPhrase=<Password>
CustomIdentityKeyStoreType=PKCS12
CustomIdentityPrivateKeyPassPhrase=<Password>
CustomTrustKeyStoreFileName=/opt/oracle/IAM12c/wlserver/
server/lib/DemoTrust.rsa
CustomTrustKeyStorePassPhrase=<Password>
CustomTrustKeyStoreType=PKCS12
```

- 89 Add the following lines just below EXTRA_JAVA_PROPERTIES in \$IDENTITY_DOMAIN_HOME/bin/setDomainEnv.sh script:

```
EXTRA_JAVA_PROPERTIES="-Djavax.net.ssl.trustStore=$
{WL_HOME}/server/lib/DemoTrust.rsa ${EXTRA_JAVA_PROPERTIES}
-Dsoa.archives.dir=${SOA_ORACLE_HOME}/soa
-Dsoa.oracle.home=${SOA_ORACLE_HOME} -Dsoa.instance.home=$
{DOMAIN_HOME} -Dtangosol.coherence.log=jdk
-Djavax.xml.soap.MessageFactory=oracle.j2ee.ws.saaj.soap.Me
ssageFactoryImpl
-Dweblogic.transaction.blocking.commit=true
-Dweblogic.transaction.blocking.rollback=true
-Doracle.xml.schema.Ignore_Duplicate_Components=true
-Doracle.xdkjava.compatibility.version=11.1.1
-Doracle.soa.compatibility.version=11.1.1 -Ddisable-implicit-bean-discovery=true"
export EXTRA_JAVA_PROPERTIES
```


90 Add these lines just below PRE_CLASSPATH:

```
export PRE_CLASSPATH="{WL_HOME}/server/lib/jcmFIPS.jar:${WL_HOME}/server/lib/sslj.jar:${PRE_CLASSPATH}"

export JAVA_OPTIONS="-Djavax.net.ssl.trustStore=${WL_HOME}/server/lib/DemoTrust.rsa
-Djavax.net.ssl.trustStoreType=PKCS12
-Djavax.net.ssl.trustStorePassword=<Password> $
{JAVA_OPTIONS} "

export JAVA_OPTIONS="
-Dweblogic.security.TrustKeyStore=CustomTrust
-Dweblogic.security.CustomTrustKeyStoreFileName=${WL_HOME}/server/lib/DemoTrust.rsa
-Dweblogic.security.CustomTrustKeyStorePassPhrase=<Password>
-Dweblogic.security.CustomTrustKeyStoreType=PKCS12
-Dweblogic.security.SSL.ignoreHostnameVerification=true $
{JAVA_OPTIONS} "
```

91 Add the following lines at the end of the file:

```
setWlstEnv_internal.sh script.
export JVM_ARGS="
-Dweblogic.security.SSL.ignoreHostnameVerification=true
-Dweblogic.security.TrustKeyStore=CustomTrust
-Dweblogic.security.CustomTrustKeyStoreFileName=${WL_HOME}/lib/DemoTrust.rsa
-Dweblogic.security.CustomTrustKeyStorePassPhrase=<Password>
-Dweblogic.security.CustomTrustKeyStoreType=PKCS12 ${JVM_ARGS} "
```

2.5.1.14 Add Root CA to JDK CA Certs File

92 Execute the following commands as the oracle user:

- cd /u01/app/oracle/product/jdk/jre/lib/security
- cp cacerts cacerts.orig

93 When importing the certificate, you need to provide an alias for the certificate – a friendly name that you can recognize. In this example, we will refer to it as the Org_Root_CA:

- `keytool -import -trustcacerts -alias Org_Root_CA -file ~/ca-chain.pem -keystore cacerts -storepass <CACERTS_PASSWORD>`

2.5.1.15 Modify Java Platform Security Config Files

94 Create backup copies of the `jps-config.xml` and `jps-config-jse.xml` files located in `$DOMAIN_HOME/config/fmwconfig`.

95 Execute the following as the oracle user:

- `cd /u01/app/oracle/admin/domains/oam_domain/config/fmwconfig`
- Edit the `jps-config.xml`

Under the `props.db.1` property set, modify the `jdbc.url` property and add the following properties to the file. The JDBC URL requires the hostname, configured TLS port (usually 2484) and the database service/instance name (i.e. `idmdb` or whatever was configured as a prerequisite to installing OIG).

- `<property name="jdbc.url" value="jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCPS)(HOST=oradb.example.com)(PORT=2484))(CONNECT_DATA=(SERVICE_NAME=idmdb))(SECURITY=(SSL_SERVER_CERT_DN='CN=oradb.example.com')))/>`
- `<property name="javax.net.ssl.keyStore" value="/home/oracle/oig_wallet/oig.jks"/>`
- `<property name="javax.net.ssl.keyStoreType" value="JKS"/>`
- `<property name="javax.net.ssl.trustStore" value="/home/oracle/oig_wallet/trustStore.jks"/>`
- `<property name="javax.net.ssl.trustStoreType" value="JKS"/>`
- `<property name="oracle.net.ssl_version" value="1.2"/>`
- `<property name="javax.net.ssl.trustStorePassword" value="TRUSTSTORE_PASSWORD"/>`
- `<property name="javax.net.ssl.keyStorePassword" value="KEYSTORE_PASSWORD"/>`
- `<property name="oracle.net.ssl_server_dn_match" value="false"/>`

The `TRUSTSTORE_PASSWORD` and `KEYSTORE_PASSWORD` are replaced with the plaintext passwords associated with the previously defined truststore and keystores in `/home/oracle/oig_wallet/trustStore.jks` and `/home/oracle/oig_wallet/oig.jks`, respectively.

- Edit `jps-config-jse.xml`

Under the `props.db.1` property set, modify the `jdbc.url` property and add the following properties to the file as shown below. (The same notes above apply similarly here.)

```
<property name="jdbc.url"
value="jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=
```

```

L=TCPS)(HOST=oradb.example.com)(PORT=2484))(CONNECT_D
ATA=(SERVICE_NAME=idmdb))(SECURITY=(SSL_SERVER_CER
T_DN='CN=oradb.example.com'))"/>
<property name="javax.net.ssl.keyStore"
value="/home/oracle/oig_wallet/oig.jks"/>
<property name="javax.net.ssl.keyStoreType" value="JKS"/>
<property name="javax.net.ssl.trustStore"
value="/home/oracle/oig_wallet/trustStore.jks"/>
<property name="javax.net.ssl.trustStoreType" value="JKS"/>
<property name="oracle.net.ssl_version" value="1.2"/>
<property name="javax.net.ssl.trustStorePassword"
value="TRUSTSTORE_PASSWORD"/>
<property name="javax.net.ssl.keyStorePassword"
value="KEYSTORE_PASSWORD"/>
<property name="oracle.net.ssl_server_dn_match" value="false"/>

```

96 Restart all of the services using the start/stop sequence described in section 2.6.

2.5.1.16 Configure TLS for the WebLogic/OIG Servers

97 Log into the WebLogic administration console by navigating to:
<https://oig.example.com:7002/console>. The username is the weblogic username
and the password. The weblogic username and password was defined in section
2.5.1.9 in step 5.

98 Once inside of the WebLogic administration screen, use the navigation panel on the
left hand side to expand “Environment” and select “Servers”. The list of servers is
shown. Click on the “AdminServer”.

99 The first thing to do is click “Lock and Edit” in the top-left side of the screen to make
configuration changes.

100 Given the large array of tabs at the top of the right-hand side of the admin screen,
ensure you are in the “Configuration” top-level tab and the “Keystores” second-level
tab.



101 In the “Keystores” section, the keystore is, by default, set to the “Demo Identity and
Demo Trust’. We need to change this to the previously constructed keystore. Click
“Change”. In the screen that appears, select “Custom Identity and Custom Trust”.
Click “Save” to commit the change.

102 After the save commits, you are brought back to the “Configuration > Keystores” tab
set. In the “Identity” section of the lower part of the pane, add the path to the
“Custom Identity Keystore” that was constructed in section 2.5.1.13 (the oig.jks file).
The “Custom Identity Keystore Type” is set to :JKS”. Ensure that the “Custom
Identity Keystore Passphrase” (and the confirmation box) are the passwords to those
keystores.

- 103 Do a similar configuration for the next group under the “Trust” section. The trust store is the trustStore.jks file constructed in 2.5.1.13. Click “Save”.
- 104 Go to the “Configuration > SSL” tab set. In the “Identity” section, set the “Private Key Alias” to “orakey” (unless you changed the key alias from this default when building the private key). Ensure the “Private Key Passphrase” (and the confirmation box) are set the private key password previously set.⁴ Click “Save”.
- 105 Go back to the “Summary of Servers” by using the URL breadcrumb at the top of the middle of the screen.
- 106 Back in the list of servers, select each other server in sequence (the oim server and the soa server). Perform the same series of configuration changes as directed above.
- 107 Once you have specified all of the changes, click the “Activate Changes” button in the top-left corner.

2.5.1.17 Configure TLS within the JDBC Data Sources

- 108 Now that the WebLogic servers have been configured for TLS, we will now configure the JDBC datasources to use TLS connectivity to the Oracle Database.
- 109 Log into the WebLogic administration console by navigating to:
<https://oig.example.com:7002/console>. The username is the weblogic username and the password. The weblogic username and password was defined in section 2.5.1.9 in step 5.
- 110 Once inside of the WebLogic administration screen, use the navigation panel on the left hand side to expand “Services” and select “Data Sources”. The list of data sources is shown. Each of the data sources needs to be configured in turn. This process is time-consuming and manual.
- 111 The first thing to do is click “Lock and Edit” in the top-left side of the screen to make configuration changes.
- 112 For each data source, click on the data source name. In the panel that appears, ensure you are in the “Configuration” top-level tab and the “Connection Pool” second-level tab. You need to make changes to the URL to point to the TLS-enabled Database connection. The URL looks like this:
- jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=oradb.example.com)(PORT=2484))(CONNECT_DATA=(SERVICE_NAME=idmdb)))
- 113 The JDBC URL uses a protocol of “TCPS” and the port of 2484 (or whatever the database was configured for a TLS listener).
- 114 A number of parameters need to be pasted into the “Properties” box in addition to what might already be in the Properties box:
- javax.net.ssl.keyStore=/home/oracle/oig_wallet/oig.jks
 - javax.net.ssl.keyStoreType=JKS
 - javax.net.ssl.trustStore=/home/oracle/oig_wallet/trustStore.jks
 - javax.net.ssl.trustStoreType=JKS

⁴ Note that the Java keystore passphrase and the private key passphrase can be independent passphrases and may, in fact, be different from one another.

- oracle.net.ssl_version=1.2

115 (The oig.jks is used for any mutually authenticating connections. If no such connections are mutually authenticating, then this JKS can be omitted. The trustStore.jks is used to validate the certificate from the Oracle Database. Therefore it must contain a trust anchor that can verify the chain of trust returned in the Database TLS handshake.)

116 Click “Save” to save the changes.

117 Scroll down the screen to find the “Encrypted Properties” box. Click “Add Securely” to add the following properties, one-by-one:

- Name: javax.net.ssl.trustStorePassword, Value: <TRUSTSTORE_PASSWORD>
- Name: javax.net.ssl.keyStorePassword, Value: <KEYSTORE_PASSWORD>

118 Click “OK” after adding an encrypted property before adding the next one.

119 When done adding the two properties, click “Save”.

120 Using the URL breadcrumb at the top of the middle part of the administration console, go back to the “Summary of JDBC Data Sources” and pick the next JDBC data source and make the exact same changes. Repeat until all JDBC sources are updated to use the TLS/SSL enabled Oracle Database connection. Be aware that there may be multiple screens of data sources to modify.

121 Once you have specified all of the changes, click the “Activate Changes” button in the top-left corner.

122 Restart all of the services using the start/stop sequence described in section 2.6.

2.5.1.18 WebLogic TLS Configuration

123 All managed WebLogic servers can be configured simultaneously for TLS parameters.

124 As the ‘oracle’ user, modify the \$DOMAIN_HOME/bin/setDomainEnv.sh file and apply the following near the top:

- export
 JAVA_OPTIONS="{JAVA_OPTIONS} -Djdk.tls.ephemeralDHKeySize=2048 -Dweblogic.security.SSL.minimumProtocolVersion=TLSv1.2 -Dweblogic.configuration.schemaValidationEnabled=false"

This restricts DH key sizes, enforces a minimum TLS protocol and to correct a problem in parsing unknown attributes in the server specification XML.

125 To configure server ciphers, as the ‘oracle’ user modify \$DOMAIN_HOME/config/config.xml.

126 Within each defined server, you need to find the <ssl></ssl> XML block and add <ciphersuite></ciphersuite> lines with each of the named ciphersuites you want to explicitly enable.

127 For example, for the SOA server:

```
<server>
  <name>soa_server1</name>
  <ssl>
    <name>soa_server1</name>
    <enabled>true</enabled>
```

```
<listen-port>7503</listen-port>
<ciphersuite>
  TLS_RSA_WITH_AES_128_CBC_SHA</ciphersuite>
<ciphersuite>
  TLS_RSA_WITH_AES_256_CBC_SHA</ciphersuite>
<ciphersuite>
  TLS_RSA_WITH_AES_128_CBC_SHA256</ciphersuite
  >
<ciphersuite>
  TLS_RSA_WITH_AES_256_CBC_SHA256</ciphersuite
  >
<ciphersuite>
  TLS_RSA_WITH_AES_128_GCM_SHA256</ciphersuite
  >
<ciphersuite>
  TLS_RSA_WITH_AES_256_GCM_SHA384</ciphersuite
  >
<ciphersuite>
  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256</ciphers
  uite>
<ciphersuite>
  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256</ciphers
  uite>
<ciphersuite>
  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256</ciphers
  uite>
<ciphersuite>
  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384</ciphers
  uite>
<ciphersuite>
  TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256</cip
  hersuite>
<ciphersuite>
  TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</cip
  hersuite>
<ciphersuite>
  TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384</cip
  hersuite>
<ciphersuite>
  TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384</cip
  hersuite>
<ciphersuite>
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256</ciphe
  rsuite>
<ciphersuite>
  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</ciphe
  rsuite>
<ciphersuite>
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384</ciphe
  rsuite>
<ciphersuite>
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384</ciphe
  rsuite>
```

```
</ssl>
```

```

    <machine>oim_machine</machine>
    <listen-port>7003</listen-port>
    . . .

```

128 Configure the appropriate ciphersuites.

129 There are other ways to adjust the ciphersuites (such as using the \$JAVA_HOME/jre/lib/security/java.security file to adjust all client and server ciphersuites). Choose the method that is appropriate to your organizational policy and environment. Use OpenSSL s_client with the -cipher parameter to verify that the servers respond to the configured ciphers.

130 Restart all of the services using the start/stop sequence described in section 2.6.

2.5.1.19 Client policy changes to create custom policy for FIPS:

131 Go to the OWSM policy page : Weblogic Domain -> Web Services -> WSM Policies

- Look for http_saml20_token_bearer_over_ssl_client_policy and replicate it, name it as 'http_saml20_token_bearer_over_ssl_client_policy_FIPS'
- Export the policy to a zip file - policyexport_clint.zip, extract it.
- Edit the policy file.
- In the policy, look for: xml : <orasp:require-tls orasp:algorithm suite=suite="Basic128" orasp:include-timestamp="false" orasp:mutual-auth="false"/>
- Replace the string : "orasp:algorithm-suite="Basic128" with "orasp:algorithm-suite="Basic256Exn256Rsa15"
- Save the file and rezip it back into the previously downloaded .zip file being sure to overwrite the existing file with the same name.
- In the WSM Policies screen, delete the existing custom policy as you are about to reimport it and WSM won't import a policy that already exists with the same name.
- You should find the updated policy - 'http_saml20_token_bearer_over_ssl_client_policy_FIPS' listed back.

132 Do the same steps as above, but this time make a new copy of the "oracle/multi_token_over_ssl_rest_service_policy" and rename with a "_FIPS" suffix.

133 Now, go to the OWSM policy page : Weblogic Domain -> Web Services -> WSM Policy Sets

- Select policy set "policySetFacade" - Detach the existing "oracle/http_saml20_token_bearer_over_ssl_client_policy" policy and attach "oracle/http_saml20_token_bearer_over_ssl_client_policy_FIPS".
- Select policy set "policySetAPPONBRD" - Detach the existing "oracle/multi_token_over_ssl_rest_service_policy" policy and attach "oracle/multi_token_over_ssl_rest_service_policy_FIPS".

In the evaluated configuration, administrators must customize the client and service policies algorithm-suite by changing the "Basic128" value to "Basic256Exn256Rsa15" as follows:

Service Policy:

- Using the Enterprise Manager (EM) console, navigate to *WebLogic Domain* > *Web Services* > *WSM Services*.

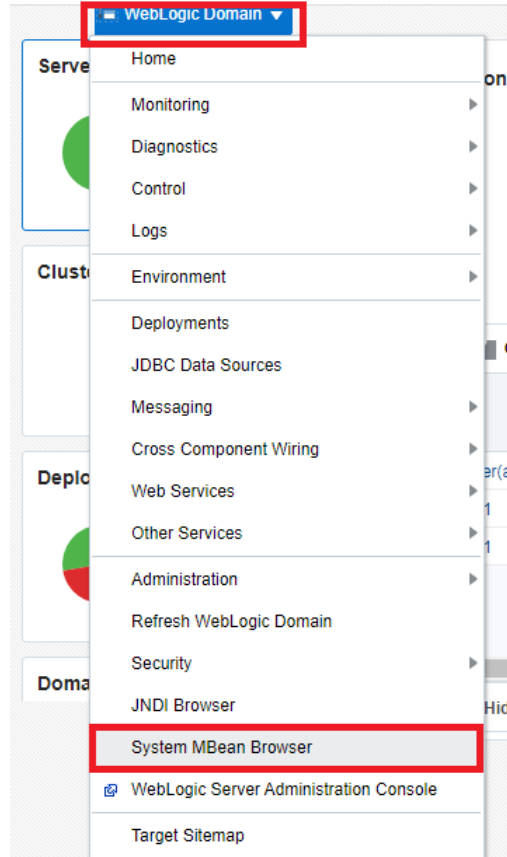
- Search for:
'wss11_saml_or_username_token_with_message_protection_service_policy'
' and replicate it to:
'wss11_saml_or_username_token_with_message_protection_service_policy_FIPS'
- Export this policy and extract it.
- Using a text editor modify the algorithm-suite within the orasp:wss11-saml-with-certificates section by replacing "Basic128" with "Basic256Exn256Rsa15".
- Save the policy and zip it and the associated folders.
- Delete the FIPS policy that was created from the clone in the EM console.
- Import the FIPS policy zip file.

Client Policy:

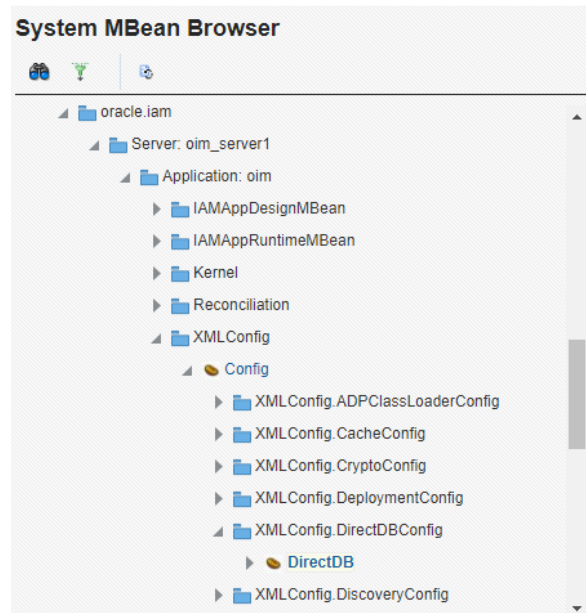
- Repeat the above steps for the wss11_saml_token_with_message_protection_client_policy updating to wss11_saml_token_with_message_protection_client_policy_FIPS
- This policy has only one instance of "Basic128" which is modified to "Basic256Exn256Rsa15".
- In the EM console attach the modified policies to the Callback services.
- Attach the client policy to the DefaultOperationApproval/CallbackService_2
 - This is found in SOA/soa-infra/Deployed Composites/DefaultOperationApproval/CallbackService_2/
 - Then the administrator should detach the default policy and attach the FIPS policy on the Policy Configuration screen.
- Attach the service policy to the service application.
 - This is found in Application Deployment/oim/Administration/Web Services Configuration then select
'/WLS/base_domain/oim|#workflowservice|WS-Service({http://wls.ws.workflowservice.platform.iam.oracle/}CallbackService#CallbackServicePort)'
 - Then the administrator should detach the default 'wss11_saml_or_username_token_with_message_protection_service_policy' policy and attach the FIPS policy.
- Restart the TOE using the start/stop sequence described in section 2.6.

2.5.1.20 Enterprise Manager JDBC TLS Connection String Modification

- 134 Log into the <https://oig.example.com:7002/em> Enterprise Manager. Use the weblogic system administrator user.
- 135 Go to the Weblogic Domain menu, and find the "System MBean Browser".



136 In the browser, find Application Defined MBeans and then expand oracle.iam. Expand the 'oim_server1' server > XML Config > XMLConfig > DirectDBConfig.



Application Defined MBeans: XMLConfig.DirectDBConfig:DirectDB Apply Revert

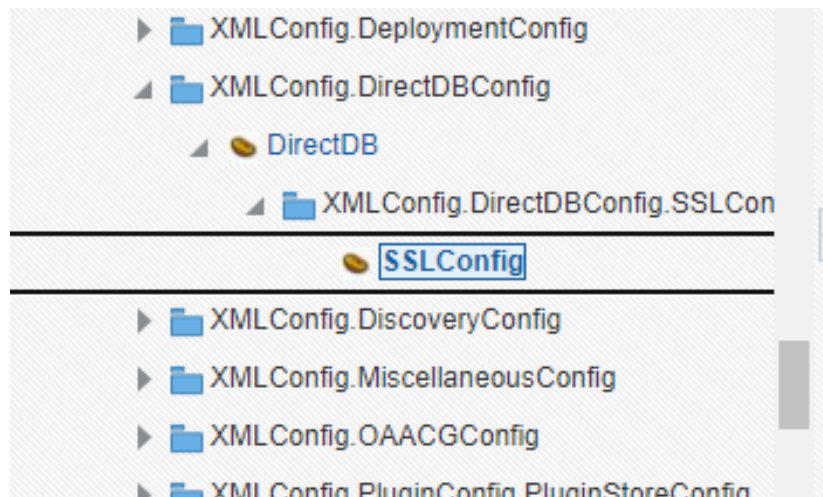
Information
 The changes made on this mbean are not managed by the configuration session. The changes will be applied immediately. You cannot undo the changes from the Change Center.

Show MBean Information

Attributes Operations Notifications

	Name	Description	Access	Value
16	SslEnabled	Direct DB Config SSL enabling	W	<input type="checkbox"/>
17	SystemMBean	If true, it indicates that this MBean is a System MBean.	R	false
18	Url	Direct DB Config URL	RW	jdbc:oracle:thin:@(DESCRIPTION=
19	Username	Direct DB Config username	RW	DEV_OIM
20	ValidateConnectionOnBorrow	Direct DB Config validate connection on borrow	W	<input type="checkbox"/>
21	Visible	If true, it indicates that this MBean is visible to current user.	R	true

- 137 In the "DirectDB" set the "Url" attribute to something like this:
- jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP S)(HOST=oradb.example.com)(PORT=2484))(CONNECT_DATA=(SERVICE_NAME=IDMDB)))
- 138 Set the SslEnabled property to "true"
- 139 In addition, you need to set the SSLConfig properties to point to the correct trust store JKS:



Application Defined MBeans: XMLConfig.DirectDBConfig.SSLConfig:SSLConfig Apply Revert

Information
 The changes made on this mbean are not managed by the configuration session. The changes will be applied immediately. You cannot undo the changes from the Change Center.

▶ Show MBean Information

Attributes Notifications

	Name	Description	Access	Value
1	ConfigMBean	If true, it indicates that this MBean is a Config MBean.	R	true
2	DBTrustStore	SSL Config DB trust store	RW	/home/oracle/oig-wallet/trustSto
3	DBTrustStorePasswordKey	SSL Config DB trust store password key	RW	[REDACTED]
4	DBTrustStoreType	SSL Config DB trust store type	RW	JKS

140 In the browser, find Application Defined MBeans and then expand oracle.iam. Expand the 'oim_server1' server > XML Config > XMLConfig > DiscoveryConfig and select "Discovery".

141 Set both the OimFrontEndURL and OimExternalFrontEndURL to the https server name and port (e.g. https://oig-server.example.com:14001)

2.5.2 Configure OIG to Communicate with OUD

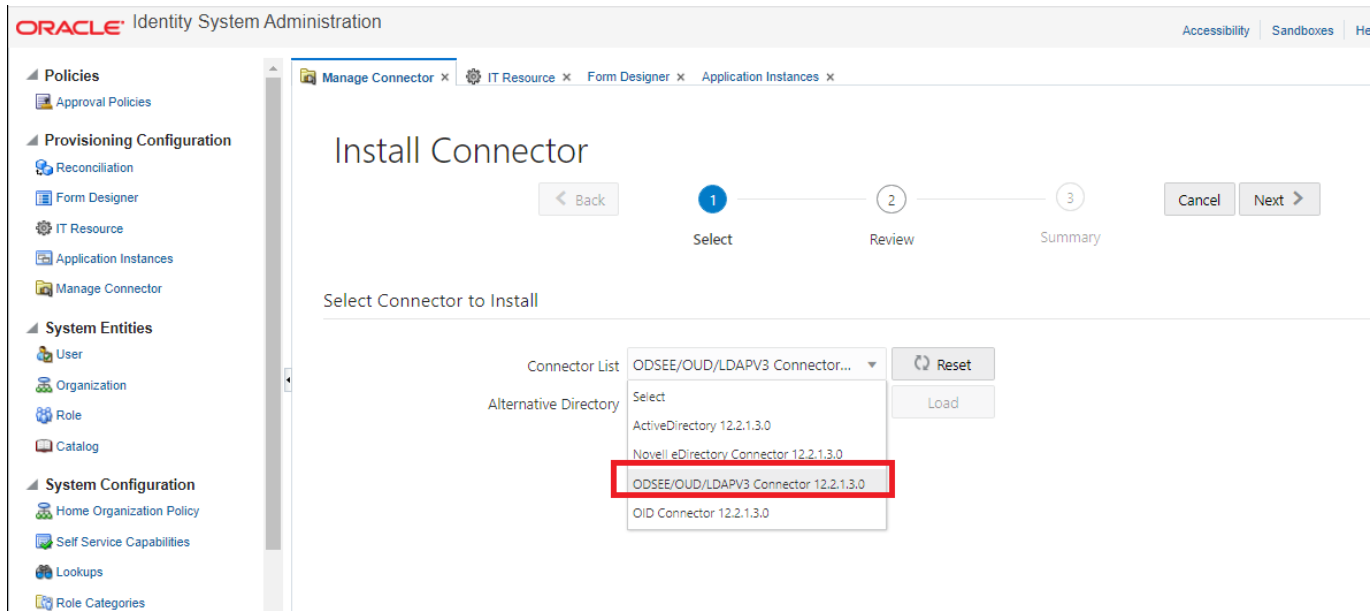
2.5.2.1 Install Connector

142 Download the connector from OTN and unzip into a staging directory on the OIG Oracle Linux server (eg. in /u01/STAGE). Ensure that the files are owned by the 'oracle' user:

- `chown -R oracle:oinstall` the entire unzipped dir.

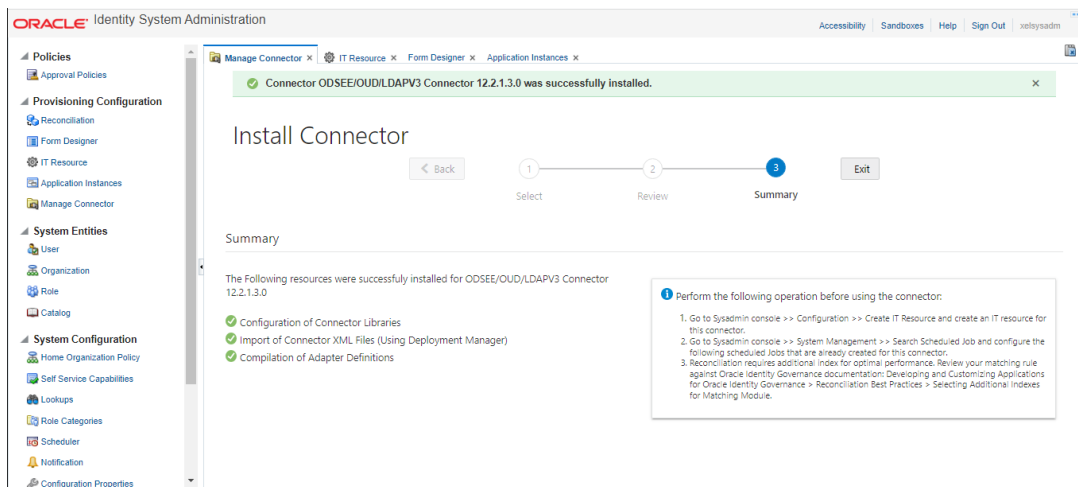
143 As the 'oracle' user, copy the unzipped archive to the \$ORACLE_HOME/idm/server/ConnectorDefaultDirectory/

144 Using a web browser, log into the sysadmin tool (https://oig.example.com:14001/sysadmin) and under the Manage Connector pane, install a new connector.



145 You specifically need to install the “ODSEE/OU/LDAPV3 Connector 12.2.1.3.0”.

146 Click “Next” to advance and then complete the installation. When completed, you will be presented with this screen:



i Perform the following operation before using the connector:

1. Go to Sysadmin console >> Configuration >> Create IT Resource and create an IT resource for this connector.
2. Go to Sysadmin console >> System Management >> Search Scheduled Job and configure the following scheduled Jobs that are already created for this connector.
3. Reconciliation requires additional index for optimal performance. Review your matching rule against Oracle Identity Governance documentation: Developing and Customizing Applications for Oracle Identity Governance > Reconciliation Best Practices > Selecting Additional Indexes for Matching Module.

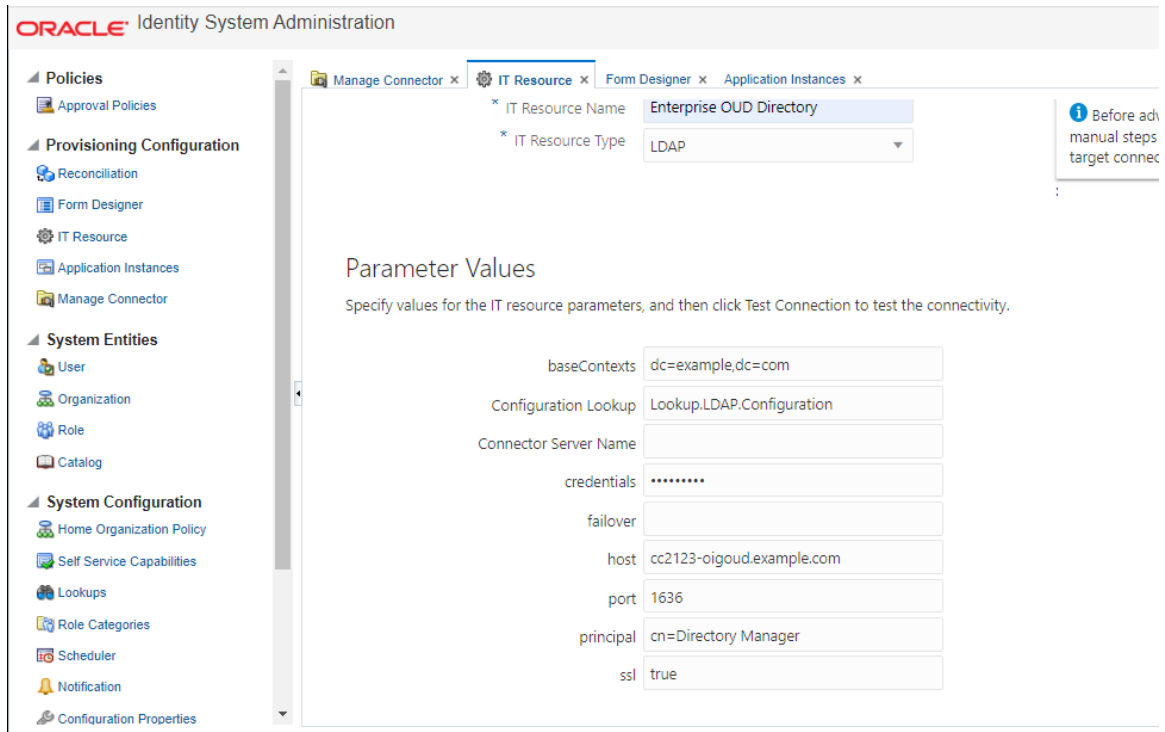
147 Proceed to create a new IT Resource as directed, picking LDAP as the resource type.

The screenshot displays the Oracle Identity System Administration interface. The main content area is titled "Create IT Resource". There are two required fields:

- * IT Resource Name: Enterprise OUD Directory
- * IT Resource Type: A dropdown menu is open, showing a list of options: ActiveDirectory, Active Directory, LDAP (which is highlighted), Mail Server, Directory Server, and Email Provider Definition - UMS.

 The left sidebar contains a navigation menu with categories: Policies, Provisioning Configuration, System Entities, and System Configuration. The top navigation bar includes tabs for Manage Connector, IT Resource, Form Designer, and Application Instances.

148 Provide relevant LDAP related configuration parameter values.



- **baseContext.** The context in the LDAP server to use.
- **Configuration Lookup.** The lookup function that can browse the LDAP server. These lookup functions are already built, and you just need to pick the correct one. In this case, “Lookup.LDAP.Configuration” is the correct lookup function to use.
- **Connector Server.** There is no need for a connector server in this case, so we leave that blank.
- **Credentials.** Credentials used for the principle.
- **Host.** The LDAP server.
- **Port.** For OUD, The SSL enabled port runs on 1636. We want to use SSL.
- **Principal.** The manager user of the LDAP.
- **SSL.** Set to “true” if using SSL.

149 Click “Finish” to complete the configuration.

2.5.2.2 Create the Provisioning Target (OUD)

150 Proceed to the Identity web management system (<https://oig.example.com:14001/identity>) and log in as an admin. Go to “Manage” and pick “Applications”. Create a new application and provide the Basic Information.

ORACLE Identity Self Service

Self Service Manage

Home Applications x

Basic Information

Provide details for the application you wish to onboard

Disconnected

Do you want to create the application from connector package or use a template?

Connector Package Template

Select Bundle

ODSEE/OU/LDAPV3 Connector 12.2.1.3.0

Alternate Connector Directory

Alternate Connector Directory

Application Name *

oudserver

Display Name *

oud-server

Description

Description

Connector Display Name

ODSEE/OU/LDAPV3 Connector

Parent Application Name

Select

Basic Configuration

* baseContexts dc=example,dc=com

* principal cn=Directory Manager

* credentials

* host oud.example.com

* port 1636

Connector Server Name Select a value

* failover

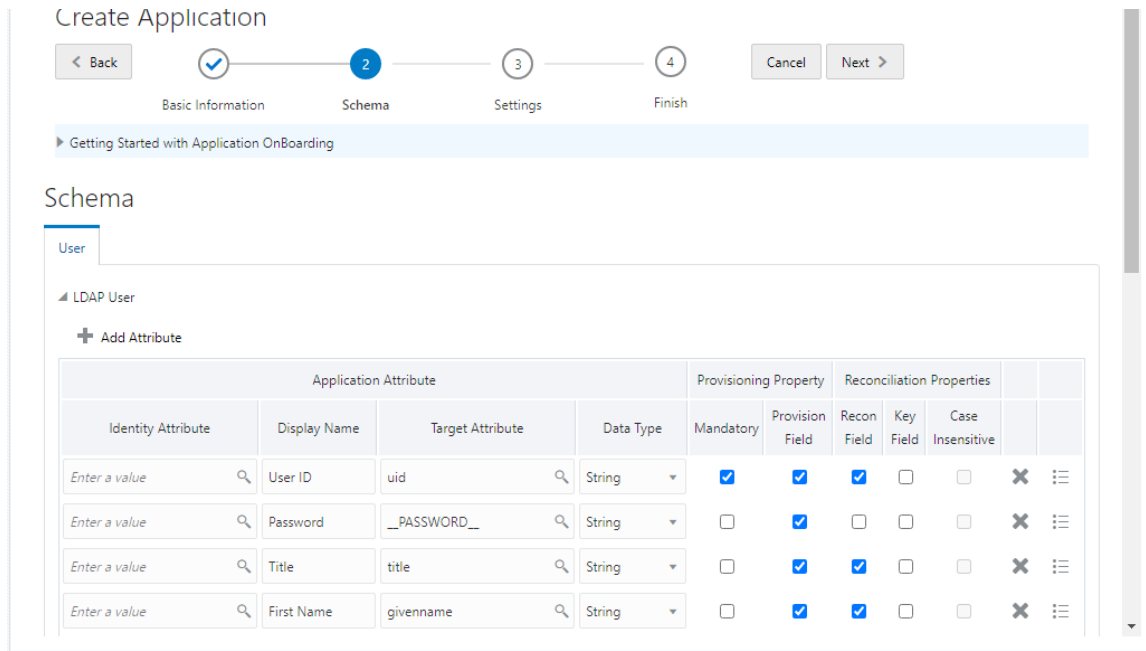
* ssl true

Test Connection

151 Click "Test Connection" and verify that it works.

If it does not work, it is likely due to problems with the OUD name (eg. No route, no resolvable name, certificate is missing required information, etc.)

152 Click "Next" to move to the schema. Keep the defaults.



153 Click “Next” to move to “Settings” and keep the defaults. Finally, click “Finish”.

2.5.2.3 Ensuring that OUD can Interoperate with OIG

154 Ensure OUD provisioning occurs successfully by verifying that “External Change Log” is enabled. First, confirm that the appropriate Oracle contexts are created by following the instructions <https://docs.oracle.com/en/middleware/idm/directory-integration-platform/12.2.1.4/administer/configuring-oracle-unified-directory.html#GUID-7D05F2EA-17BC-44FA-94BD-009E3186E0FB>

155 Execute the following commands on the OUD system as the ‘oracle’ user:

- `cd /u01/app/oracle/product/12.2.1.4.0/oudhome_1/asinst_1/OUT/bin`
- `./setup-oracle-context -h oud.example.com -p 4444 -D "cn=Directory Manager" -j <(echo -n 'Password') --no-prompt --trustAll`

Note: The use of the FQDN is very important due to the requirement to match the CN/SAN in the certificate.

156 Next, enable the ECL by following the instructions located here: <https://docs.oracle.com/en/middleware/idm/directory-integration-platform/12.2.1.4/administer/configuring-oracle-unified-directory.html#GUID-E2CCBBBE-2979-4A5D-9F86-A3754334B5B4>

157 As the ‘oracle’ user, run the following in the `/u01/app/oracle/product/12.2.1.4.0/oudhome_1/asinst_1/OUT/bin` directory:

- `./dsreplication enable-changelog -h oud.example.com -p 4444 -D "cn=Directory Manager" -j <(echo -n 'Password') -r 8989 -b "dc=example,dc=com" --trustAll --no-prompt`

The replication port (-r) is required to configure the ECL, even on a standalone server, because the ECL relies on the replication mechanism. You need only specify

the replication port if the change log (or replication) was not previously configured on the server. The default value of the replication port is 8989.

158 To verify that the ECL is configured on a directory server instance, run the following search command and look for the cn=changelog naming context.

- `./ldapsearch -h localhost -p 1389 -D "cn=directory manager" -w Password! -s base -b "" "objectclass=*" namingContexts`

159 The expected output looks similar to this:

```
dn:
namingContexts: cn=changelog
namingcontexts: cn=OracleContext
namingcontexts: cn=OracleSchemaVersion
namingcontexts: dc=example,dc=com
```

2.6 Starting and Stopping the TOE

160 The TOE must be carefully started and stopped in a specific sequence.

161 You must start the Node Manager, then start WebLogic, then start the WebLogic managed servers.

162 To shutdown the TOE, do the operations in reverse: shutdown the WebLogic managed servers, then shutdown WebLogic, then shutdown Node Manager.

2.6.1 Start Node Manager

163 The top-level component which must be started is the Node Manager. Log into the OIG Oracle Linux box and switch to the 'oracle' user. Run the following to start Node Manager:

- `cd $DOMAIN_HOME`
- `nohup ./startNodeManager > ~/nm.log 2>&1 &`
- `tail -f $HOME/nm.log`

164 Watch the output of the Node Manager log until it says "Plain socket listener started on port".

2.6.2 Start WebLogic

165 As the 'oracle' user, run the following:


- `cd $DOMAIN_HOME`
- `nohup ./startWebLogic.sh > ~/wls.log 2>&1 &`
- `tail -f $HOME/wls.log`

166 The WebLogic server takes a few minutes to start. You are looking for the string "The server started in RUNNING mode".

2.6.3 Start WebLogic Managed Servers


167 Use a web browser to navigate to the <https://oig.example.com:7002/console> URL. Log in using the weblogic system administration account (weblogic). Using the left-

hand navigation tree, expand “Environment” and select “Servers” to show the Summary of Servers. The “AdminServer” should already be running. In the tab group, select “Control” and click each of the other non-running servers and click “Start”.

168 Click the refresh icon  to allow the web browser to periodically poll the status. Starting these servers can take a few minutes.

2.6.4 Stopping WebLogic Managed Servers

169 Use a web browser to navigate to the <https://oig.example.com:7002/console> URL. Log in using the weblogic system administration account (weblogic). Using the left-hand navigation tree, expand “Environment” and select “Servers” to show the Summary of Servers. In the tab group, select “Control” and click each of the running servers (except for the AdminServer) and click “Shutdown”. Choose an appropriate shutdown type.

170 Click the refresh icon  to allow the web browser to periodically poll the status. Shutting down these servers is relatively quick.

2.6.5 Stopping WebLogic

171 As the ‘oracle’ user, run the following:

- `cd $DOMAIN_HOME`
- `./stopWebLogic.sh`

172 The WebLogic server shuts down relatively quickly.

2.6.6 Stopping Node Manager

173 Run the following as the ‘oracle’ user to stop Node Manager:

- `cd $DOMAIN_HOME`
- `./stopNodeManager`

3 Configuration Guidance

3.1 Enterprise Security Management

3.1.1 ESM_EAU.2 - Reliance on Enterprise Authentication

174 As part of installation of OIG and configuration of its operational environment, OIG will be configured to use OUD as an authentication server with the desired Identity Store as the repository for administrative accounts. This is performed by completing the steps described in Section 2.5.2.

175 Users attempting to perform self-service password reset activities are defined in OIG by their email addresses and are authenticated using their security questions. The process by which a user can reset a forgotten password is described in section 3.3 of [SELF]. If a user wishes to modify any of their authentication data that resides in the Identity Store, they will access OIG by following the steps outlined in section 4 of [SELF]. They will then modify password and security questions and answers

176 Note: There are no IT entities that authenticate directly to OIG.

3.1.2 ESM_EID.2 - Reliance on Enterprise Identification

177 Refer to ESM_EAU.2 above.

3.1.3 ESM_ICD.1 - Identity and Credential Definition

178 The primary purpose of OIG is to provide a method to administer the identity and credential data of organizational users. In addition to allowing for direct configuration of this data, collections of privileges known as entitlements can be defined that are automatically granted based on combinations of relevant identity data. The following guidance describes how to configure identity and credential data for environmental users:

- User attributes: section 6 of [ADMIN]
- Roles and Role membership: section 3.18 and 3.19 of [HELP]

179 Administrators also have the ability to define new attribute fields for Identity Store accounts that are linked to OIG, known as user defined fields (UDFs). The process for creating UDFs is described in section 6 of [ADMIN]. Administrators can also modify user identity data by approving or rejecting requests that are initiated by users themselves. The process for users initiating requests for modification is described in section 6.1 of [SELF], and the process for administrators approving or rejecting these requests is described in section 8 of [SELF].

180 Identity and credential data that is managed by OIG can also be modified by trusted sources. For example, a separate HR system may be used to enrol users into the system when they join the organization and in OIG will recognize the change. This process is called reconciliation. Guidance on how reconciliation is performed can be found in section 10 of [ADMIN].

3.1.3.1 Challenge Questions Configuration

181 Administrators must enable and configure the Challenge Options as described in section 3.16 of [HELP]. Specifically, the following configuration is recommended:

- Allowed Challenges = User Defined
- Total Questions To Be Collected = 3

- Minimum Correct Answers When Challenged = 3
- Allow Duplicate Responses = No
- Minimum Answer Length = 5
- Lock User After Attempts = 5.

Note: When the password policy has been configured with user-defined challenge questions, the user must define their own challenge questions during registration as described in section 2.1 of [SELF].

3.1.4 ESM_ICT.1 - Identity and Credential Transmission

182 When a change is made to user identity and/or credential data using OIG, the change is immediately pushed to the Identity Store. There are no separate actions an administrator needs to perform and this behavior is not configurable.

3.2 Security Audit

3.2.1 FAU_GEN.1 – Audit Data Generation

183 In the evaluated configuration, logging is enabled for OIG in order to provide accounting for the operations that are performed by administrators of the product. The steps to enable logging are described in sections 20 and 27.3 of [ADMIN]. Log entries will contain a large number of individual fields. The security-relevant aspects of the log are as follows:

- Timestamp (this is not the name of the field, the timestamp is identified as the first element in the log entry): indicates when the action was performed
- Type and Operation: indicates the action being performed as part of the event by its type (e.g. user) and the operation performed (e.g. change_password)
- Status: indicates the outcome of the event
- UserId: indicates the authenticated user performing the action represented by the event

184 Logging related to TLS activity is enabled in the underlying WebLogic server. Instructions for doing this can be found at http://docs.oracle.com/cd/E13222_01/wls/docs90/ConsoleHelp/taskhelp/logging/RedirectJVMOutput.html. The TLS log data shows the establishment and termination of TLS connections as well as extensive diagnostic data for the connection such as the timestamps, cipher suite used, and hello messages. This logging data is stored on the OIG server OS platform.

3.2.2 FAU_STG_EXT.1 – External Audit Trail Storage

185 By default, audit data produced by OIG is stored in the environmental Oracle database. This is not configurable. Communications to the database are not secured by default, so if the database is not located on the same system as the OIG Server, it is necessary to follow the steps outlined in the installation and configuration steps above. Note that since an active database connection is required for OIG to function, it is not possible for a situation to occur where audit server communications are disrupted while OIG continues to be operational.

3.3 Identification and Authentication

3.3.1 FIA_USB.1 – User-Subject Binding

186

As stated in ESM_EAU.2 above, the Identity Store where administrator accounts are defined is configured during the association of OIG to the OUD authentication mechanism. The Oracle database used by OIG stores a replicated copy of the administrator identity data for the purpose of mapping the authenticated administrator to their assigned privileges. OIG's administrative authority is role-based. Each role has the ability to perform certain tasks and an administrator account can be assigned to more than one role. Section 3.12 of **[HELP]** describes administrative roles in more detail.

3.4 Security Management

3.4.1 FMT_MOF.1 – Management of Functions Behaviour

187 OIG relies on the environmental Identity Store as its external data source for administrative identity data. However, it also maintains a local copy of these records in the Oracle database for synchronization purposes. The database also stores the assigned administrative roles for each account. By default, these are mapped 1:1 to the administrator accounts. The default mapping can be overridden so that an administrator’s privileges are mapped to a different account defined within OIG. This is known as “ad hoc” linking. Section 10.5.7 of **[ADMIN]** describes ad hoc linking and the steps that must be followed in order to perform this.

3.4.2 FMT_MTD.1 – Management of TSF Data

188 Non-administrative users can access OIG to perform modifications to their account information, which includes their identifying attributes and authentication data such as passwords and security questions/answers. A user can also initiate a change to their account, role, and/or entitlements data, which is then reviewed for approval by an administrator. The process by which a user performs these actions is described in detail in section 6.1 of **[SELF]**. Administrative approvals of user data change requests is described in section 8 of **[SELF]**. Additionally, administrators can manage the identity and credential data of other users directly, as described in section 3.1 of **[HELP]**.

3.4.3 FMT_SMF.1 – Specification of Management Functions

189 The management functions provided by OIG to securely administer the product in the evaluated configuration are referenced throughout this guide under their associated security functional requirements (SFR).

3.4.4 FMT_SMR.1 – Security Management Roles

190 OIG defines a number of out-of-the-box administrative roles that grant varying degrees of permission to manage the security functions of the product. These roles and their associated privileges are defined in Table 3 below. Administrators can be assigned to multiple roles. The process for associating administrators with roles is described in section 3.12 of **[HELP]**.

191 The product also allows for the definition of custom administrative roles that have administratively-defined privileges. In the evaluated configuration, the default roles should be used.

192 **Note:** to review members associated with a specific Admin role, navigate to *Organization > Admin Role* in the GUI.

Table 3: Administrative Roles & Privileges

Administrator Role	Privileges
Application Instance Administrator	Has the ability to create, modify, and delete application instances, which consist of accounts used to access resources in the Operational Environment.
Application Instance Authorizer	Has the ability to associate organizational users with environmental accounts via application instances.

Administrator Role	Privileges
Application Instance Viewer	Has the ability to approve self-service requests initiated by users to have their environmental account associations updated.
Entitlement Administrator	Has the ability to create, modify, and delete entitlements.
Entitlement Authorizer	Has the ability to associate organizational users with environmental entitlements.
Entitlement Viewer	Has the ability to approve self-service requests initiated by users to have their environmental entitlements updated.
Help Desk	Can manage user passwords, enable or disable users, and unlock the user if they have been locked out due to an excessive number of failed authentication attempts.
Organization Administrator	Can manage organizations and specify additional ones if the environment's organizational structure dictates it. Can also associate password policies with organizations to enforce on those organizational users.
Role Administrator	Can manage enterprise roles as well as identity conditions that determine their membership.
Role Authorizer	Can modify the enterprise role identity attribute by granting roles to and revoking rules from users.
Role Viewer	Has the ability to approve self-service requests initiated by users to have their role information updated.
Self-Service (implicit)	Can manage a subset of their own identity attributes, change their password, and request changes to their identity attributes, user role, accounts, or entitlements.
System Administrator	Has full privileges to manage all aspects of the TSF.
System Configurator	Has the ability to define and modify extended identity attributes, password policies, and general TSF system performance attributes such as lockout settings. Also can define policies governing the approval requests that can be granted by various roles.
User Administrator	Has the ability to create, delete, and manage users, including their identity attributes, user role, accounts, or entitlements, as well as whether the user is enabled at an organizational level.
User Viewer	Has the ability to approve self-service requests to change their identity attributes, user role, accounts, or entitlements. Can also assign users to admin roles to give them the ability to manage the TSF.

3.5 Protection of the TSF

3.5.1 FPT_APW_EXT.1 – Protection of Stored Credentials

193 There are no administrative functions associated with the protection of stored credentials. Administrative credentials are always stored securely and this is not configurable.

3.5.2 FPT_SKP_EXT.1 – Protection of Secret Key Parameters

194 There are no administrative functions associated with the protection of cryptographic materials. These materials are always stored securely and this is not configurable.

3.6 Trusted Path/Channel

3.6.1 FTP_ITC.1 – Inter-TSF Trusted Channel

195 Configuration of trusted communications is performed by following the relevant steps outlined in the installation and configuration steps above.

3.6.2 FTP_TRP.1 – Trusted Path

196 Configuration of trusted communications is performed by following the relevant steps outlined in the installation and configuration steps above.