

Oracle Insurance Data Gateway Security Administration

User Guide

Version 1.0

Copyright © 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle Insurance Data Gateway Security Administration User Guide

Release 1.0

Part # E93051-01

Library# E93054-01

January 2018

Contributing Authors: Mikalai Krautsevich, Eugene Chen, Michael Schwitzgebel, Mark Taylor

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

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

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

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

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

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

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

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

CONTENTS

Chapter – 1	4
Overview	4
Document Ownership and Control	4
General Security Principles	4
Keep Software Up To Date	4
Restrict Network Access to Critical Services	4
Follow the Principle of Least Privilege	4
Monitor System Activity	5
Keep Up To Date on Latest Security Information	5
Minimize the Attack Surface	5
Chapter – 2	6
HIPAA Compliance	6
Oracle and HIPAA.....	6
HIPAA by Design	6
HIPAA and OIDG Development and Consulting resources.....	8
Chapter – 3	9
Secure Installation	9
Recommended Deployment	9
Secure Installation of Web Application	10
Installing Database Schemas	11
Security Configuration	11
Creating Groups and Users	11
Creating a User Group.....	12
Creating a User	13
Granting Access to Groups with Application Roles	15
Granting Admin Privileges.....	16
Securing Web Services.....	17
PII, PHI, PCI Data Handling.....	18
Encryption Key Management.....	19
Application Roles	22

Chapter – 1

OVERVIEW

Security planning is a critical step to help protect your company's valuable data and ensure that information is not compromised. Established security policies and goals should guide the security plan your organization executes to secure its systems. Oracle Insurance Data Gateway (OIDG) handles sensitive data and requires security measures to be taken to protect it. Security policies should align with those already established at your organization, or new ones should be established if they are not already defined. This document provides guidelines for securing an OIDG installation, including the configuration and installation steps needed to meet security goals. Details on the types of security features and services that are available to detect and prevent a potential security breach are provided. This encompasses secure system deployment, protection of sensitive data, reliability and availability of the application, authentication and authorization mechanisms.

The development and review of security documentation, an evaluation of business requirements, and the configuration and validation of available security measures and services should all be performed.

DOCUMENT OWNERSHIP AND CONTROL

This document is maintained by Oracle Insurance Data Gateway Development. It is reviewed twice per year and adjusted as needed.

Note: Oracle Insurance Data Gateway (OIDG) and Oracle Insurance Data Exchange (OIDX) share the same code base and therefore share many of the same security roles and configuration property names. Because of this you will see references to "OIDX" for OIDG security configuration settings.

GENERAL SECURITY PRINCIPLES

The following principles are fundamental to using any application securely.

Keep Software Up To Date

One of the principles of good security practice is to keep all software versions and patches up to date. Regularly check My Oracle Support for Critical Patch Updates (CPU) for the OIDG platform (Oracle Database, Oracle WebLogic application server, and Oracle SOA Suite).

Restrict Network Access to Critical Services

Keep both the OIDG middle-tier and database behind a firewall. In addition, configure a firewall between the middle-tier and the database. The firewalls provide assurance that access to these systems is restricted to a known network route, which can be monitored and restricted, if necessary.

Follow the Principle of Least Privilege

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. Over ambitious granting of responsibilities, roles, grants, etc. often leaves a system wide open for abuse. User privileges should be reviewed periodically to determine relevance to current job responsibilities.

Monitor System Activity

System security stands on three legs: good security protocols, proper system configuration and system monitoring. Auditing and reviewing audit records address this third requirement. Each component within a system has some degree of monitoring capability. Follow audit advice in this document and regularly monitor audit records.

Keep Up To Date on Latest Security Information

Oracle continually improves its software and documentation. Check the Installation Guide and Release Notes before installing a new release. Regularly check this Security Guide for up-to-date security related information.

Minimize the Attack Surface

The "attack surface" of a system is the sum of the different entry points that an unauthorized user can exploit to gain access to system services or to the data maintained in the system. Common strategies for reducing the attack surface or hardening the system include (but are not limited to):

- Minimize the number of services running, i.e. make sure to only run required services.
- Make sure that all entry points, like the system's user interface and its web services are secured.

Specifically for OIDG, do the following:

- Do not install OIDG software on machines that execute a technology stack that is not required for running the application.
- Follow the Installation Guide to prevent installation of software that is not required to run the application. For example, for Oracle's WebLogic server installation it specifically mentions the services that need to be installed.
- Do not install additional applications in the WebLogic domains running OIDG.
- Make sure to track and trace use of the system, e.g. by logging which users access its services.
- Apply firewalls at the system's boundaries.
- Secure all entries, for example make sure that SSL/TLS is used between clients and load balancer / DMZ.

Chapter – 2

HIPAA COMPLIANCE

This chapter covers HIPAA and HITECH compliance for OIDG.

Oracle and HIPAA

The Healthcare Insurance Portability and Accountability Act of 1996 (HIPAA) requires Covered Entities to implement processes and safeguards designed to protect the privacy and security of electronic protected health information (ePHI or simply PHI). HIPAA has evolved through subsequent legislation:

- The Privacy Rule was added in December 2000. It gives patients rights over their health information and sets rules for how information is used, shared, accessed and protected. Moreover, the rule explicitly lists ePHI identifiers like name and social security number.
- The Security Rule was added in February 2003.
- The HITECH Act that was passed in February 2009 which dictates how the privacy and security of health information must be managed by Covered Entities and Business Associates (or BAs).
- The Omnibus Rule that is effective as of September 2013. Among other things, it extended the definition of a BA to parties that create, receive, maintain and transmit PHI on behalf of a Covered Entity.

By definition of the Omnibus Rule, Oracle is considered a BA when Oracle performs functions on behalf of a Covered Entity that involve access to PHI. That is even the case when no specific customer Business Associate Agreement (or BAA) is in place. To address the requirements coming from this, Oracle implemented:

- Standard BAAs with its suppliers as well as standard BAAs for use by Oracle's customers that enables them to fulfill their requirements.
- Processes that address compliance with the administrative, physical and technical requirements of the Security Rule.
- Annual audits that are conducted by a third party to assess Oracle's level of compliance. This includes cloud services and consulting engagements.

HIPAA by Design

HIPAA and HITECH require covered entities to

1. Ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain or transmit;
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
3. Protect against reasonably anticipated, impermissible uses or disclosures; and
4. Ensure compliance by their workforce.

The Privacy rule is more functional in nature and will be an integral part of the design of the application/service as this is exposed to the user community. The Security Rule is a series of administrative, technical, and physical security safeguards and related policies and procedures designed to require covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting ePHI. Both rules impact the development process but it is the Security rule that has proved more intractable as there are requirements to not only follow the rule but to show that the rule is being followed.

Covered entities are required to comply with every security rule, however, the security rule categorizes certain standards as "addressable," while others are "required."

- Required - These implementation specifications must be implemented.
- Addressable - The "addressable" designation does not mean that an implementation specification is optional. However, it permits covered entities to determine whether the addressable implementation specification is reasonable and appropriate for that covered entity. If it is not, the security rule allows the covered entity to adopt an alternative measure that achieves the purpose of the standard, if the alternative measure is reasonable and appropriate.

There are a number of Administrative Standards and Technical Standards that have a direct impact on the development process. Examples of these are listed in the following table. The last column contains examples that illustrate how the OIDG application development process or architecture (including the Oracle technology stack) handles the rule.

Rule	Implementation	Oracle & OIDG Solution
ADMINISTRATIVE - Security Management Process - 164.308 (a)(1) Risk analysis (Required)	Assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI held by the covered entity or business associate.	Oracle Global Product Security review for every major release of an OIDG application. Static and dynamic code scans are required to be run for every release. Identified high and critical security vulnerabilities must be addressed before release.
TECHNICAL - Security Management Process 164.312(a) - Mixed	<p>Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).</p> <p>(2) Implementation specifications:</p> <p>(i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.</p> <p>(ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.</p> <p>(iii) Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.</p> <p>(iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information</p>	<p>By default, OIDG only accepts requests from authenticated, identifiable users.</p> <p>OIDG provides role based authorization to associate application roles with users.</p> <p>The WebLogic runtime environment implements account inactivity / session timeout. Users have to re-authenticate in order to continue working.</p> <p>Any web traffic should be encrypted using TLS/SSL, at least from client to load balancer / DMZ (more on this elsewhere in this guide).</p> <p>For data at rest the Oracle database offers the Transparent Data Encryption feature.</p>
TECHNICAL - Audit Controls 164.312 (b) (Required)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	OIDG does not store PHI data. Requests containing PHI data can be placed in sFTP files or local folders. Oracle recommends that those files

		<p>be encrypted at rest. Regardless, OIDG logs user authentication.</p> <p>For example:</p> <ul style="list-style-type: none"> • OIDG logs which users have accessed the system possibly viewing private information
<p>TECHNICAL - Integrity 164.308 (a)(3) (Required)</p>	<p>Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.</p>	<p>Users who have access to the ePHI should be minimized. For that, customers should apply the Principle of Least Privilege (see elsewhere in this guide) and the Principle of Minimum level of access. OIDG requires that users are explicitly provisioned to access the application (through the provisioning service). Moreover, users should not be granted access to system functions (and associated data) that they do not need for their work.</p>
<p>TECHNICAL - Transmission Security 164.312 (e) (Mixed)</p>	<p>Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.</p> <p>(2) Implementation specifications:</p> <p>(i) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.</p> <p>(ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.</p>	<p>Customers should use TLS/SSL and sFTP to effectively protect data in transit. Customers should use OpenPGP encryption standards to protect files at rest. Consider the use of Oracle Advanced Security SQLnet encryption between the mid-tiers and the database if required.</p>

HIPAA and OIDG Development and Consulting resources

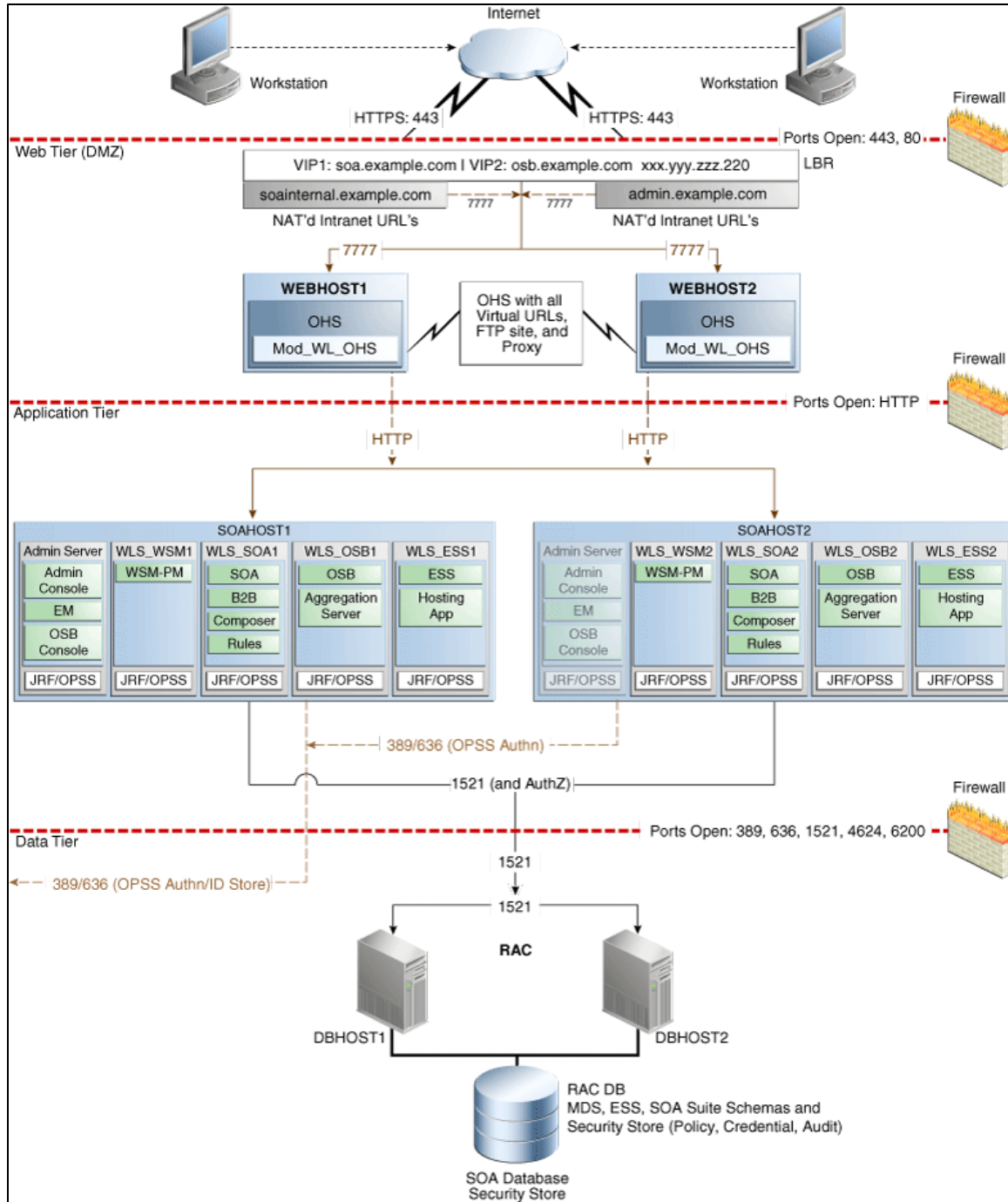
OIDG Development and Consulting resources interact with customers in various ways. Customers make use of OIDG systems through on premise deployments. Oracle staff may be required to access OIDG deployment environments for support or maintenance purposes. Oracle staff utilizes dedicated systems and environments specifically designed to retain PHI. For example, any data stored on Oracle consulting laptops is encrypted; Oracle Support systems are regularly audited for compliance. All Oracle employees are required to take the Information Protection Awareness training upon employment and every two years. Oracle employees with access to ePHI environments are required to take annual HIPAA trainings. Training is provided through Oracle University and completion is tracked.

SECURE INSTALLATION

Recommended Deployment

OIDG requires several .EAR, .JAR, and config files to be deployed and configured in WebLogic. The WebLogic domain should not be installed as root. The installation files should be placed in a secure location on the file server that can be accessed by WebLogic. Access should be restricted to the user or user group that WebLogic is running under.

As mentioned earlier, the OIDG middle-tier and database should each be kept behind a firewall. The following is a reference topology on how the OIDG infrastructure should be deployed.



Secure Installation of Web Application

Secure all entries, for example make sure that SSL/TLS is used between clients and load balancer / DMZ.

Installing Database Schemas

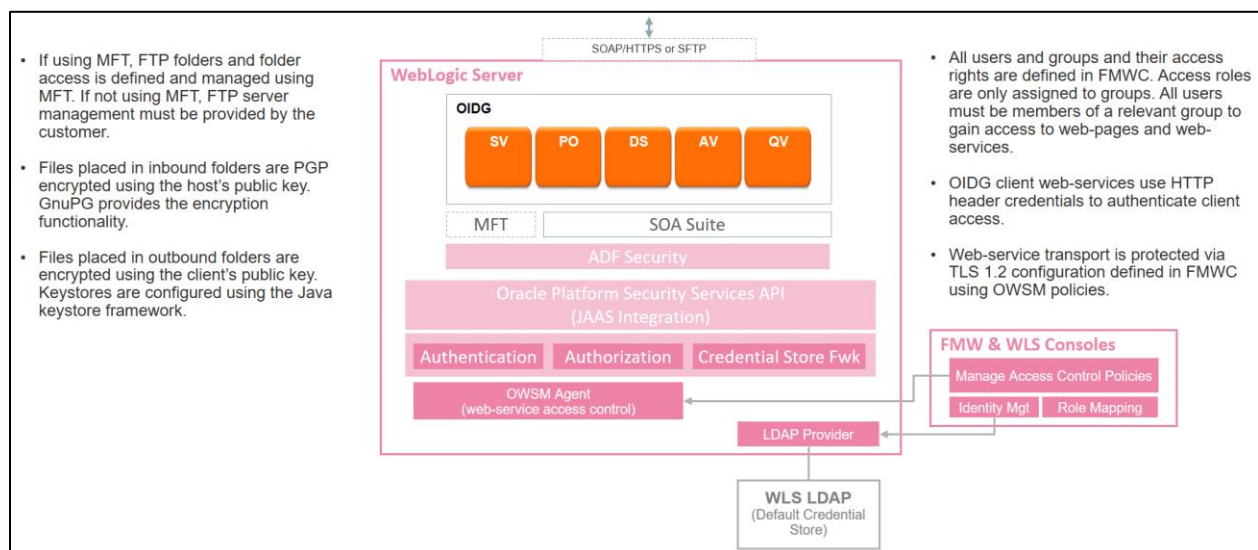
The user created for the database schema should only be given minimal permissions. The OIDG database user needs to be the owner of the schema and does not require any additional permissions. The db owner should not be used for the web location to connect to the database. Another separate database user should be created for the web application to connect to the database.

Please consult the OIDG Installation Guide and Oracle database documentation for more details.

SECURITY CONFIGURATION

The critical security features for OIDG are:

- **Authentication** – is provided by the authentication provider in WebLogic. OIDG can authenticate against any WebLogic supported LDAP credential store. The embedded WebLogic LDAP credential store is used by default.
- **Authorization** – is achieved through a set of pre-defined OIDG application roles which are mapped to users and groups in the WebLogic security realm. Users and groups can be assigned to application roles using the Fusion Middleware Control application that comes with the SOA Suite infrastructure. It provides authorization and security policy services that are used by OIDG to authorize access to UI pages and web services.
- **Audit** – authentication events are recorded in the WebLogic authentication log. This log is not enabled by default and does not contain application specific security information.



Creating Groups and Users

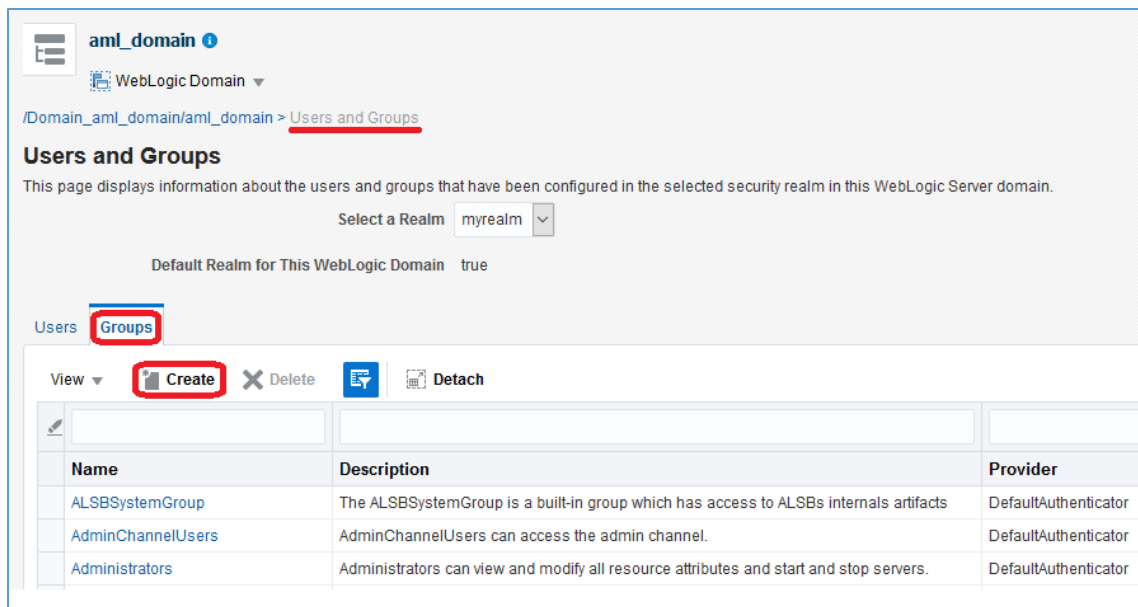
Each client company or organization created in OIDG will be represented by a named group [defined in the WLS security realm](#). Each group can contain further sub-groups as deemed necessary by the customer. These could be defined via in Fusion Middleware Control (FMWC) or in the WebLogic console by an OIDG administrator. Users created in the security realm will need to be assigned to an appropriate named group. Access roles should be assigned to groups rather than users.

Note: The configuration steps below are based on using the embedded WebLogic LDAP server. The steps could vary if another supported LDAP provider was chosen. Below is the configuration for Embedded LDAP.

Creating a User Group

Below is an example of creating an 'OIDXAdmin_Group' user group that will be assigned the OIDG OIDXAdmin application role. A group can be assigned more than role.

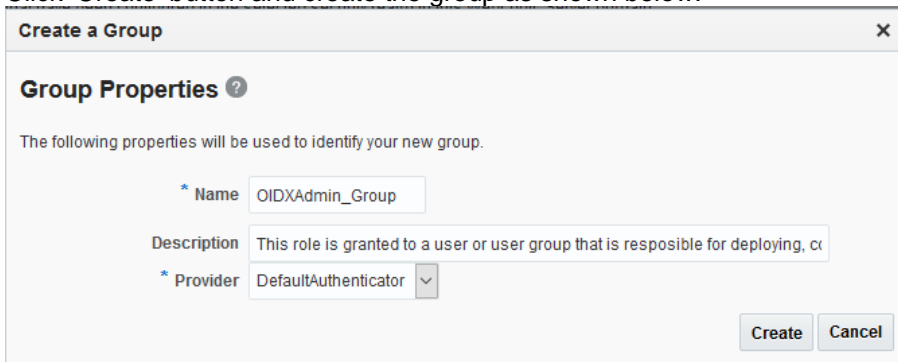
- Login to the FMWC console, select the domain if not already selected.
- Choose Security → 'Users and Groups' and go to Groups tab.



The screenshot shows the 'Users and Groups' configuration page for the 'aml_domain'. The 'Groups' tab is active, and the 'Create' button is highlighted. Below the navigation bar is a table listing existing groups:

Name	Description	Provider
ALSBSystemGroup	The ALSBSystemGroup is a built-in group which has access to ALSBs internals artifacts	DefaultAuthenticator
AdminChannelUsers	AdminChannelUsers can access the admin channel.	DefaultAuthenticator
Administrators	Administrators can view and modify all resource attributes and start and stop servers.	DefaultAuthenticator

- Click 'Create' button and create the group as shown below.

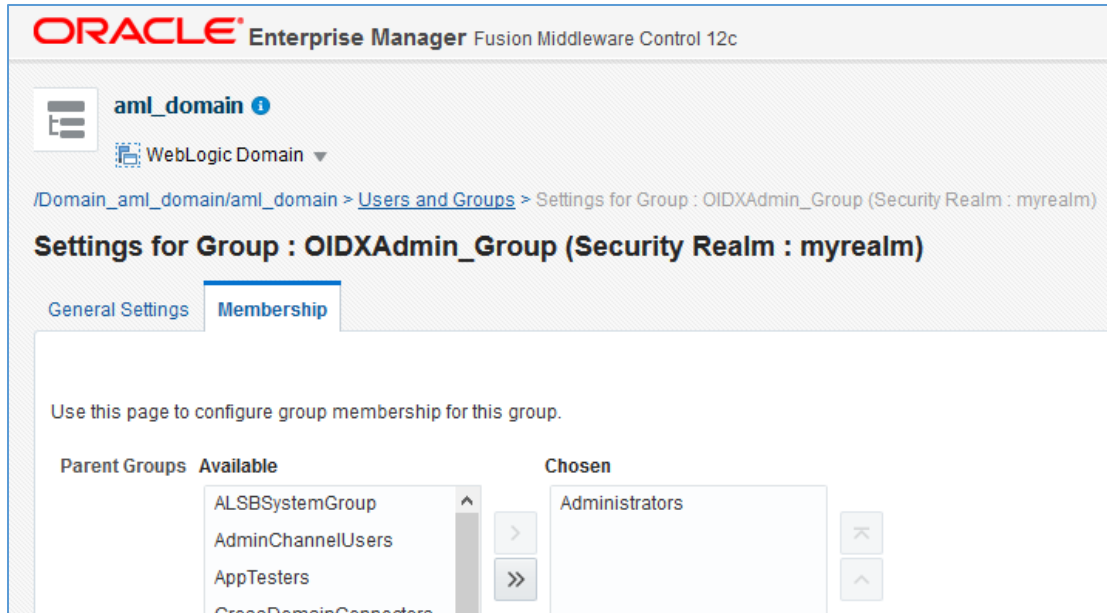


The 'Create a Group' dialog box shows the following properties:

- Name:** OIDXAdmin_Group
- Description:** This role is granted to a user or user group that is responsible for deploying, c
- Provider:** DefaultAuthenticator

Buttons: Create, Cancel

- Click on each created group and in 'Membership' tab select the required Parent group and move to Chosen as shown below.



- Click 'Save'.

Creating a User

Below is an example of creating an 'OIDXAdminUser1' user that will be placed in the 'OIDXAdmin_Group' that we created in the previous section. Adding this user to the OIDXAdmin_Group will result in this user inheriting all the privileges that have been granted to the group.

- If not already in 'Users and Groups', Login to the FMWC console, select the domain if not already selected.
- Choose Security → 'Users and Groups'
- Now to go the Users tab and click 'Create'.

aml_domain **WebLogic Domain**

/Domain_aml_domain/aml_domain > Users and Groups

Users and Groups

This page displays information about the users and groups that have been configured in the selected security domain.

Select a Realm

Default Realm for This WebLogic Domain true

Users Groups

View

Name	Description	Provider
LCMUser	This is the default service account ...	DefaultAuthenticator
OracleSystemUser	Oracle application software syste...	DefaultAuthenticator
alsb-system-user	The ALSB system user is a built-in...	DefaultAuthenticator
weblogic	This user is the default administra...	DefaultAuthenticator

- Create the user as shown below.

Create a User ✕

User Properties ?

The following properties will be used to identify your new user.

* Name

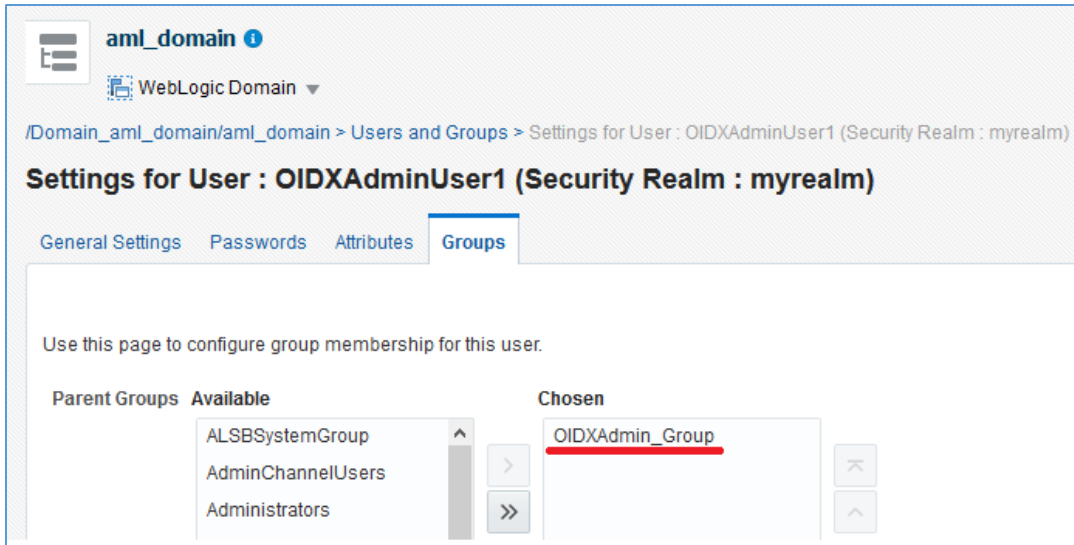
Description

* Provider

* Password

* Confirm Password

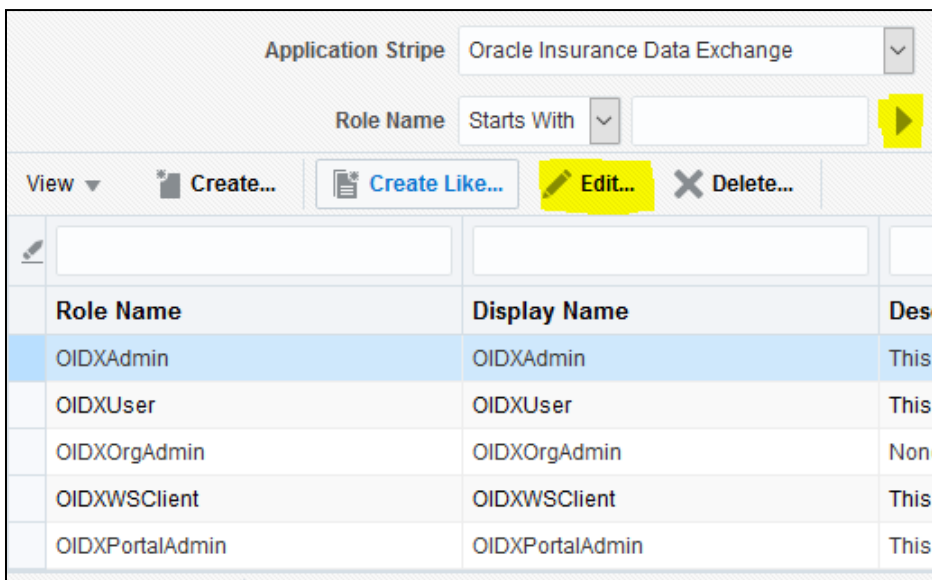
- Click on created User and in 'Groups' tab choose the group that we created earlier from Parent Groups and move to Chosen as shown below.



- Similarly create required groups and users. Assign the users to appropriate group based on required privilege.

Granting Access to Groups with Application Roles

- In FMWC console, select <Domain> → Security → Application Roles.
- Select 'Oracle Insurance Data Exchange' from the Application Stripe drop-down.
- Click the arrow at the end of the Role name field to search for application roles.



- Select any existing role and click on Edit.
- Click 'Add'.
- Select 'Group' for Type.

- Click the arrow at the end of the Display Name field to search for roles.


Add Principal

Specify criteria to search and select the application roles that you want to grant permissions to.

▲ Search

Type

Principal Name

Display Name 

Searched Principals

View

Principal	Display Name	Description
AdminChannelUsers		AdminChannelUsers can access the admin channel.
Administrators		Administrators can view and modify all resource attributes and start and stop servers.
ALSBSystemGroup		The ALSBSystemGroup is a built-in group which has access to ALSBs internals artifacts
AppTesters		AppTesters group.
CrossDomainConnectors		CrossDomainConnectors can make inter-domain calls from foreign domains.
Deployers		Deployers can view all resource attributes and deploy applications.
IntegrationAdministrators		IntegrationAdministrators have complete access to all AquaLogic Service Bus resources (but have read-only access to users, groups, roles and access control policies)
IntegrationDeployers		IntegrationDeployers have complete access to all AquaLogic Service Bus resources (but have read-only access to users, groups, roles and access control policies)
IntegrationMonitors		IntegrationMonitors have read-only access to all AquaLogic Service Bus resources
IntegrationOperators		IntegrationOperators have access to the following operations: 1) read all AquaLogic Service Bus resources. 2) view, create, update and delete alert rules, and 3) session management including create, commit, discard and undo of sessions
Monitors		Monitors can view and modify all resource attributes and perform operations not restricted by roles.
OIDXAdmin_Group		This role is granted to a user or user group that is responsible for deploying, configuring, and debugging deployment issues. This role should only assigned to administrative users.
OIDXPortalAdmin_Group		This role is granted to OIDX users that need to configure URLs for files on the portal dashboard. This role would typically only be granted to an administrative user.
OIDXUser_Group		This role is granted to OIDX users that only need to be able to view transactional data. Users in this role only have read access and can only access Quick View and the Tenant Portal.
OIDXWSCClient_Group		This role is granted to OIDX users that represent client applications which need access to OIDX client services.
Operators		Operators can view and modify all resource attributes and perform server lifecycle operations.
OracleSystemGroup		Oracle application software system group.

- Select the appropriate existing group and click Ok.
- Click Ok again.
- Repeat the above steps for other roles.

Granting Admin Privileges

- To grant Admin privileges to the OIDXAdmin_Group group, log in to the WebLogic console as the administrator user.
- In Security Realms, choose 'Roles and Policies'.
- Expand Global Roles → Roles → For required role click on 'View Role Conditions'

Roles		
Edit Role		
Name ↔	Resource Type	Role Policy
[-] Coherence Clusters		
[-] Deployments		
[-] Domain		
[-] Global Roles		
[-] Roles		
Admin	Global Role	View Role Conditions
AdminChannelUser	Global Role	View Role Conditions
ALSBSystem	Global Role	View Role Conditions
Anonymous	Global Role	View Role Conditions
AppTester	Global Role	View Role Conditions
CrossDomainConnector	Global Role	View Role Conditions
Deployer	Global Role	View Role Conditions
IntegrationAdmin	Global Role	View Role Conditions
IntegrationDeployer	Global Role	View Role Conditions
IntegrationMonitor	Global Role	View Role Conditions
IntegrationOperator	Global Role	View Role Conditions
Monitor	Global Role	View Role Conditions
Operator	Global Role	View Role Conditions
OracleSystemRole	Global Role	View Role Conditions

- Select 'Group' in drop-down and click 'Next'.
- For the 'Group Argument Name' field, provide the group that we created earlier and click 'Add'.

Edit Global Role

Back Next Finish Cancel

Edit Arguments

On this page you will fill in the arguments that pertain to the predicate you have chosen.

Add one or more groups to this condition. If you add multiple groups, the condition evaluates as true if the user is a member of ANY of the groups.

Group Argument Name: Add

OIDXAdmin_Group Remove

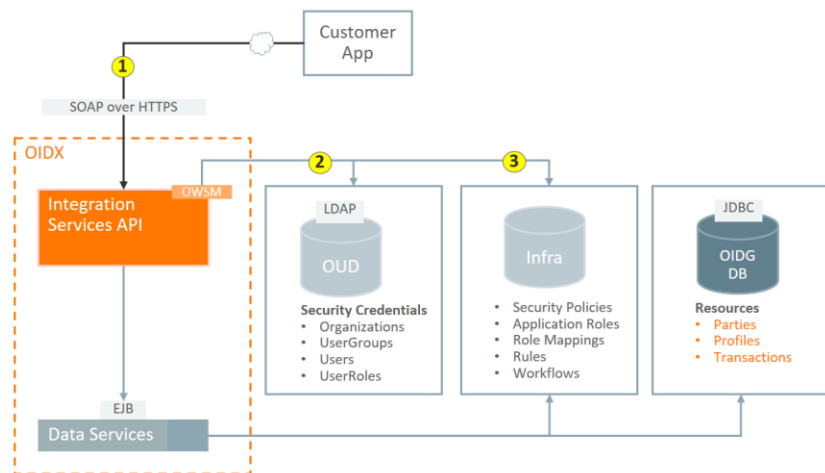
Back Next Finish Cancel

- Click 'Finish' and then 'Save'.
- The user who needed to access the WebLogic console should have the '**Admin**' and '**IntegrationAdmin**' roles. Repeat for any additional.

Securing Web Services

Oracle Service Bus is used by OIDG to expose web-services to clients and it uses OWSM to manage access to these services via access control policies. An access control policy specifies conditions under which users, groups, or roles can access a proxy service. For all proxy services, you can create a transport-level policy, which applies a security check when a client attempts to establish a connection with the proxy service.

1. Customer makes an OIDG SOAP/HTTPS request
2. OWSM Authentication
 - SOAP/HTTPS Header UsernameToken containing user/pwd credentials is used by OWSM to authenticate against credentials in WebLogic
3. OWSM Authorization
 - OWSM uses credential-mappings defined in FMWC to authorize a user or group to access client web-services



OIDG adheres to the [WS-Security standards](#), as developed by the OASIS Open committee, for the authentication of SOAP messages. As per this approach, consuming applications need to send the Username token as part of the SOAP security header along with the SOAP request. An OWSM user token policy is employed which only allows requests from users who are listed in the transport-level policy to proceed.

The SOAP header must include a <wsse:UsernameToken> element which holds the authentication information. Inside this element the username and password are specified with the <wsse:Username>, and <wsse:Password> elements, respectively.

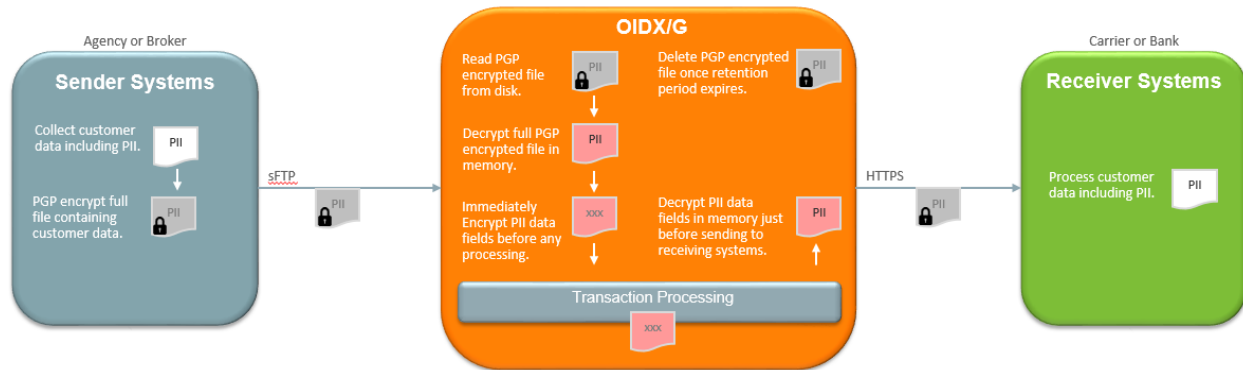
TLS 1.2 is required as the method of encryption for all SOAP messages.

Access control policies are persisted in authorization providers and are managed within a design session, not outside the session. Because the changes are made within a session, you can commit or discard the changes as with other resources.

See the Service Virtualization Deployment and Configuration section of the Installation Guide for more details.

PII, PHI, PCI Data Handling

Customers can send sensitive data through OIDG to target systems. OIDG supports a standard ACORD AML model and is aware of data that is sensitive in that model. Files holding this data are always PGP encrypted at rest. They are decrypted once pulled into memory. Sensitive data is encrypted before any processing occurs in OIDG.



In OIDX/G, customer data is always PGP encrypted at rest and read-only in the app. PII defined data is encrypted in memory before any processing or application logging is done. No OIDX/G user will be able to see any PII defined fields. No OIDX/G user will be able to edit any payload data.

Data Type	Pre OIDG Submission	Transmission to OIDG	OIDG Inbound Processing	OIDG Outbound Processing
PII	PII fields are not encrypted before full payload PGP encryption.	Transmitted over HTTPS (TLS 1.2) or over sFTP	Payload decrypted but PII data immediately encrypted before transit. If stored on disk, files are encrypted using Oracle private key and later deleted. TDE enabled on DB so all data at rest is encrypted.	PII data is decrypted just before PGP encrypting the entire payload and is then sent to the receiver.
PHI	PHI fields are not encrypted before full payload PGP encryption.	Transmitted over HTTPS (TLS 1.2) or over sFTP	Payload decrypted but PHI data immediately encrypted before transit. If stored on disk, files are encrypted using Oracle private key and later deleted. TDE enabled on DB so all data at rest is encrypted.	PHI data is decrypted just before PGP encrypting the entire payload using a receiver specified key and is then sent to the receiver.
PCI	PCI fields are encrypted using non-Oracle specified keys before full payload PGP encryption	Transmitted over HTTPS (TLS 1.2) or over sFTP	Payload decrypted except PCI data since key is unknown to OIDX/G. If stored on disk, files are encrypted using Oracle private key and later deleted. Data is stored encrypted.	PCI data fields remain encrypted since key is unknown to OIDX/G. Entire payload is PGP encrypted using receiver specified key and sent to the receiver.

Customers wanting to send PCI data through OIDX must do so without any OIDX knowledge of the data. It must be encrypted before coming into OIDX and decrypted after leaving OIDX with PGP keys unknown to OIDX. OIDX does not support storage of PGP keys or any other details about encrypted PCI data using its infrastructure.

Encryption Key Management

OIDX was developed and tested using GnuPG (GPG) to encrypt and decrypt files. For more info on GnuPG please go [here](#). From the GPG installation directory, the GPG command line interface is used to generate asymmetric key pairs. This will create a public key and a private key. Both the client and host companies will need an asymmetric key pair to safely share files with each other.

The key pair is used as follows:

- The Public key is used only for file encryption. As the name suggest, this key can be shared.
- The Private key is used for file encryption and decryption. This key should never be shared.

In order to do its own encryption and decryption when processing incoming and outgoing files, OIDG will need to be configured to know about the client's public key(s) and the host's public and private key(s). Please see the OIDG installation guide for details on how to configure the system to use asymmetric file encryption.

Client companies who will be sending and receiving files with an OIDG hosted system should encrypt their files before sending them and should expect to receive encrypted files from the host company. These are the guidelines a client company should follow:

- The client company should generate their own asymmetric key pair using a tool like GPG.
- The client will need to export their public key in public key file to be shared with the OIDG host company. The private key should not be shared.
- The client will need to send the public key file to the OIDG host company. This can be done through email or upload to an FTP server made available by the host company.
- The host company will need to import the client's public key file into their GPG installation.
- The key id for this public key will need to be entered into the OIDG configuration by the host company. The host company will have to configure their OIDG deployment to know about the client company. Part of this configuration is identifying the encryption and decryption key IDs to use when sending and receiving data from the client. The folder locations used to send and receive files for a specific client for a specific transaction type are generically called "endpoints". The public key IDs will need to be entered on endpoint definitions that represent these folders. The key ID is captured on an endpoint property called 'GPGUserKeyld'. This is described in the OIDG Portal User Guide.
- The key ID is used by OIDG to look up the actual public encryption key from the public key file that was imported into the GPG installation.
- OIDG will use the clients public encryption key to encrypt notification and error report files that will be sent back to the client.
- The client company will need to use their private key to decrypt encrypted files it receives from OIDG.

A company hosting OIDG and expecting to send and receive files with OIDG should encrypt their files before sending them and should expect to receive encrypted files from the client company. These are the guidelines a host company should follow:

- The host company should generate their own asymmetric key pair using a tool like GPG.
- The host will need to export their public key in public key file to be shared with the OIDG client company. The private key should not be shared.
- The host will need to send the public key file to the OIDG client company. This can be done through email or upload to an FTP server made available by the client company.
- The client company will need to import the host company's public key file into their GPG installation.
- When the client company prepares a file to be sent to the host, it will need to encrypt the file with the host company's public encryption key.
- Once the host company receives an encrypted file from the client, it will use its private encryption key to decrypt the file.
- During system deployment, OIDG needs to be configured to know about the host company. During this setup, a file transfer endpoint definition is created that captures a password called the

GPG passphrase. This passphrase is needed to retrieve the private key from the key file stored in the GPG installation.

- When processing file requests, OIDG will look up the passphrase from its host company endpoint configuration and use it to retrieve the host company's private encryption key from the GPG install. It will then use that private key to decrypt the request file which will then be sent on for further processing.

Application Roles

The following lists the available OIDG application roles and their behavior in the OIDG components.

	Description	AdminView Rights	OIDX/G Portal Rights	QuickView Rights
OIDXAdmin	This role is granted to a user or user group that is responsible for deploying, configuring, and debugging deployment issues. This role should only assigned to administrative users.	All available functions	All available functions. Can launch all admin consoles. Can view data for all organizations. Can launch Quick View, Admin View, SB, FMWC, and WLS consoles.	All available functions. Can view data for all organizations.
OIDXOrgAdmin (Cloud Only)	Used in the OIDX cloud offering only.	N/A	N/A	N/A
OIDXUser	This role is granted to OIDX/G users that only need to be able to view transactional data. Users in this role only have read access and can only access Quick View and the Tenant Portal.	N/A	Read-only rights. Can launch Quick View. Can view reports. Can only view data for organizations user is a member of.	Read-only rights. Can only view data for organizations user is a member of. No access to "Retry" functionality.
OIDXWSClient	This role is granted to OIDX/G users that represent client applications which need access to OIDX/G client services.	N/A	N/A	N/A
OIDXPortalAdmin	This role is granted to OIDX/G users that need to configure URLs for tiles on the portal dashboard. This role would typically only be granted to an administrative user.	N/A	Can configure URLs for tiles on the portal dashboard.	N/A