ORACLE
Insurance

Oracle Insurance Data Exchange Security Administration

User Guide

Release 11.0.2

December 2019

Oracle Insurance Data Exchange Security Administration User Guide

Release 11.0.2

December 2019

CONTENTS

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 Exchange (OIDX) 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 OIDX 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 Exchange Development. It is reviewed twice per year and adjusted as needed.

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 OIDX platform (Oracle Database, Oracle WebLogic application server, and Oracle SOA Suite).

Restrict Network Access to Critical Services

Keep both the OIDX 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, and so on often leaves a system wide open for misuse. 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 the 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, that is, make sure to only run the required services.
- Make sure that all entry points, such as the system's user interface and its web services are secured.

Chapter – 2

HIPAA COMPLIANCE

This chapter covers HIPAA and HITECH compliance for OIDX.

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:

- Ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- 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 OIDX application development process or architecture (including the Oracle technology stack) handles the rule.

Rule	Implementation	Oracle & OIDX 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 OIDX 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	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). (2) Implementation specifications: (i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity. (ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. (iii) Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information	By default, OIDX only accepts requests from authenticated, identifiable users. OIDX provides role based authorization to associate application roles with users. The WebLogic runtime environment implements account inactivity / session timeout. Users have to re-authenticate in order to continue working. Any web traffic should be encrypted using TLS/SSL, at least from client to load balancer / DMZ (more on this elsewhere in this guide). For data at rest the Oracle database offers the Transparent Data Encryption feature.
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.	OIDX stores PHI data. Requests containing PHI data can be placed in sFTP files or local folders. Oracle recommends that those files be

		encrypted at rest. Regardless, OIDX logs user authentication. For example: • OIDX logs the users that have accessed the system possibly viewing private information
TECHNICAL - Integrity 164.308 (a)(3) (Required)	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.	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. OIDX 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.
TECHNICAL - Transmission Security 164.312 (e) (Mixed)	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. (2) Implementation specifications: (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. (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	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.

HIPAA and OIDX Development and Consulting resources

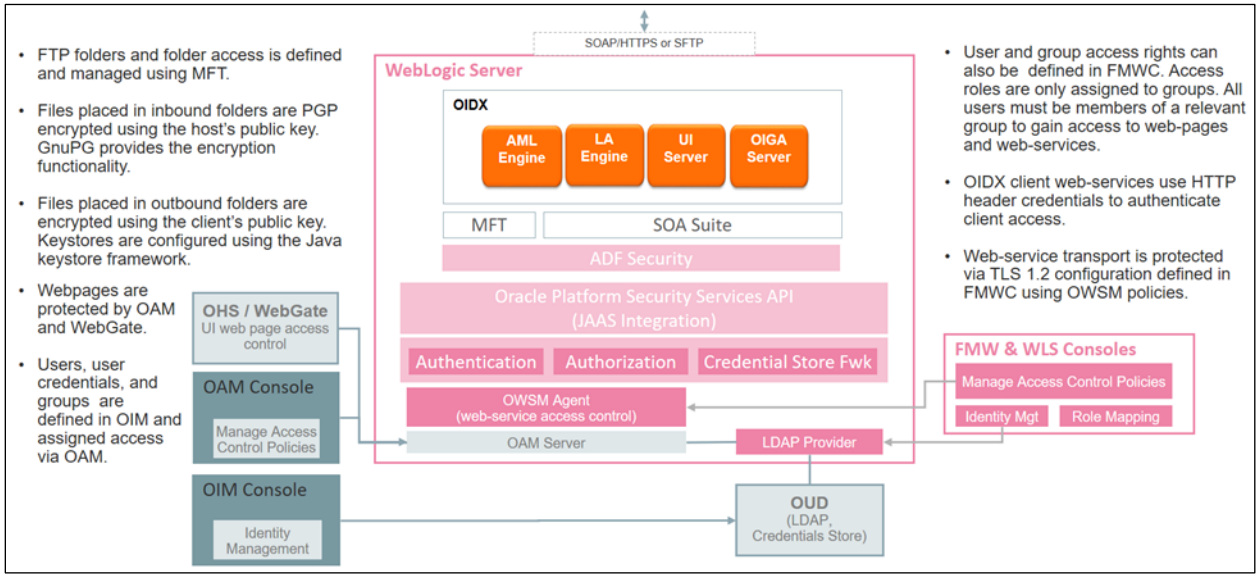
OIDX Development and Consulting resources interact with customers in various ways. Customers make use of OIDX systems through cloud deployments. Oracle staff may be required to access OIDX deployment environments for support or maintenance purposes. Oracle staff utilizes dedicated systems and environments 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 thereafter. Oracle employees with access to ePHI environments are required to take annual HIPAA trainings. Training is provided through Oracle University and completion is tracked.

Chapter – 3

SECURITY CONFIGURATION

The critical security features for OIDX are:

- **Authentication** – is provided by the authentication provider in WebLogic. Users are defined in OIM.
- **Authorization** – is achieved through a set of pre-defined OIDX application roles which are mapped to users in the WebLogic security realm. Users 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 OIDX 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

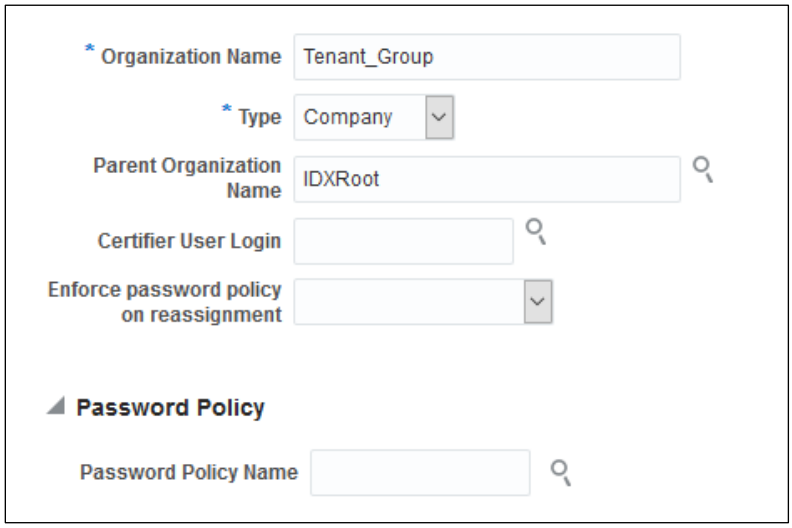
Each client company or organization created in OIDX will be represented by a named group defined in the WLS security realm. Each group can contain further sub-groups as deemed necessary by the customer. These are defined in Oracle Identity Manager (OIM). Users created in the security realm will need to be assigned to an appropriate named group. Access roles should be assigned to groups rather than users.

Creating a User Group

To create a user group, do the following:

1. Login to the OIM console.
2. Click the **Manage** tab located on the top-right corner.
3. Click **Organizations** > **Create**.

4. Enter a value for **Organization Name**.
5. Select the appropriate **Parent Organization Name** and other details based on requirements.

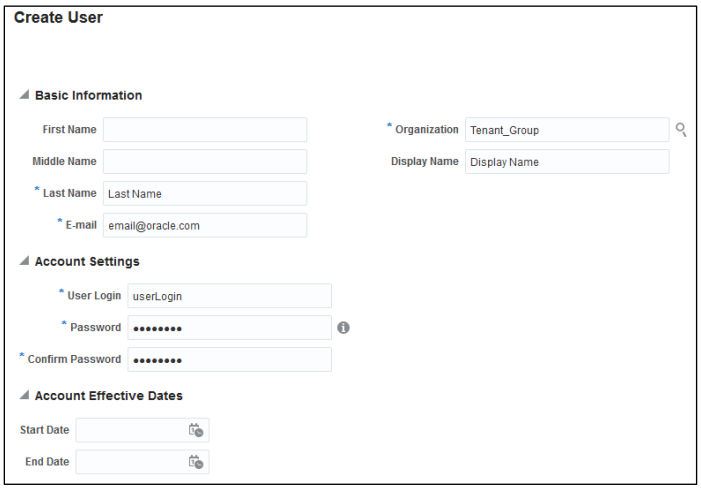


6. Click **Save**.

Creating a User

To create a user, do the following:

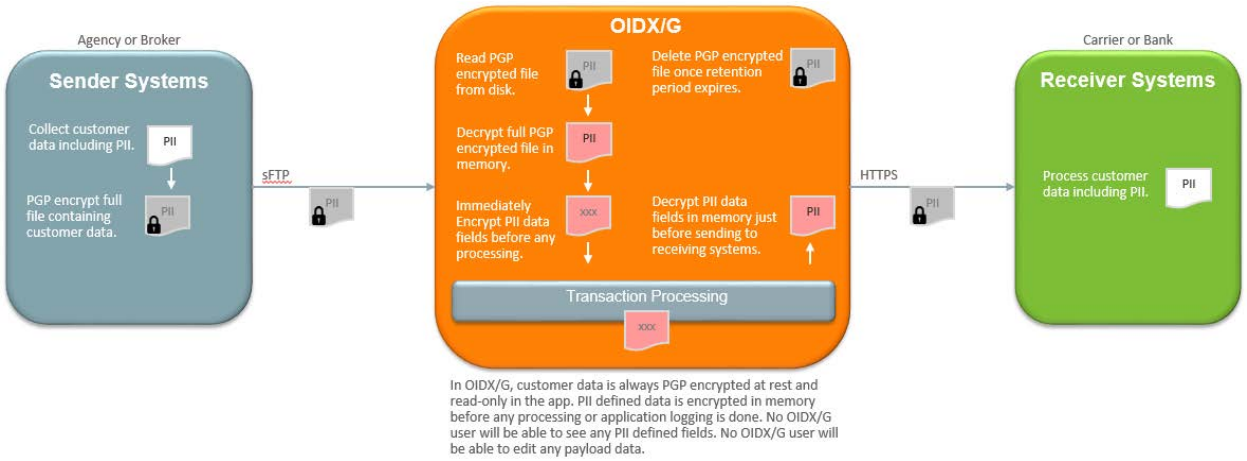
1. In OIM console, click the **Manage** tab located on the top-right corner.
2. Click **Users** > **Create**.
3. Enter values for all mandatory fields as shown below



4. Click **Submit**.

PII, PHI, PCI Data Handling

Customers can send sensitive data through OIDX to target systems. OIDX 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 OIDX.



Data Type	Pre OIDX Submission	Transmission to OIDX	OIDX Inbound Processing	OIDX 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 using a receiver specified key 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 visit https://www.gnupg.org/. From the GPG installation directory, the GPG command line interface is used to generate asymmetric key pairs. This creates a public key and a private key. Both the client and host companies 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.

To do its own encryption and decryption when processing incoming and outgoing files, OIDX will need to be configured to know about the client's public key(s) and the host's public and private key(s).

Client companies who will be sending and receiving files with an OIDX 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, such as GPG.
- The client will need to export their pubic key in public key file to be shared with the OIDX host company. The private key should not be shared.
- The client will need to send the public key file to the OIDX 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 OIDX configuration by the host company. The host company will have to configure their OIDX 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 'GPGUserKeyId'. This is described in the OIDX User Interface Guide.
- The key ID is used by OIDX to look up the actual public encryption key from the public key file that was imported into the GPG installation.
- OIDX 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 OIDX.

A company hosting OIDX and expecting to send and receive files with OIDX 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 pubic key in public key file to be shared with the OIDX client company. The private key should not be shared.
- The host will need to send the public key file to the OIDX 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, OIDX 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, OIDX will lookup 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 OIDX application roles and their behavior in the OIDX components.

	Description	AdminView Rights	OIDX 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. This role is reserved for Oracle Cloud admin employees only.	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	This role is granted to a user or user group that is responsible for maintaining an organization hierarchy in OIM. Users in this role can create other users, user groups, and sub-organizations under their organization. They can also grant the OIDXOrgAdmin role to users and user groups in their organization. This role is assigned to registered OIDX tenant and client company administrators. This role is also granted to OIDX users that represent client applications which need access to OIDX client services.	N/A	Can launch Quick View. Can view reports. Can only view data for organizations user is a member of. Can launch OIM in cloud deployments.	All available functions. Can only view data for organizations that the user is a member of. Can submit on "Retry" tab.
OIDXViewSensitiveData	Used in OIDX cloud offering only. This role allows user to see PII/PHI data in LA QuickView application	N/A	N/A	Read-only access to policy detail screens that show PII data.

	Description	AdminView Rights	OIDX Portal Rights	QuickView Rights
OIDXUser	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.	N/A	Read-only rights. Can launch Quick View. Can view reports. Can only view data for organizations that the 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 users that represent client applications that need access to OIDX client services.	N/A	N/A	N/A
OIDXPortalAdmin	This role is granted to OIDX users that need to configure URLs for tiles on the portal dashboard. This role is typically granted only to an administrative user.	N/A	Can configure URLs for tiles on the portal dashboard.	N/A