Oracle® Retail Supplier Evaluation Cloud Service

Security Guide

Release 24.1.301.0
F98276-01
July 2024

Oracle Retail Supplier Evaluation Cloud Service Security Guide, Release 24.1.301.0

F98276-01

Primary Author: Bernadette Goodman

Contributing Authors: Aidan Ratcliffe

Contents

Send Us Your Comments

Oracle Retail Supplier Evaluation Cloud Service Security Guide, Release 24.1.301.0

Oracle welcomes customers' comments and suggestions on the quality and usefulness of this document.

Your feedback is important, and helps us to best meet your needs as a user of our products. For example:

- Are the implementation steps correct and complete?
- Did you understand the context of the procedures?
- Did you find any errors in the information?
- Does the structure of the information help you with your tasks?
- Do you need different information or graphics? If so, where, and in what format?
- Are the examples correct? Do you need more examples?

If you find any errors or have any other suggestions for improvement, then please tell us your name, the name of the company who has licensed our products, the title and part number of the documentation and the chapter, section, and page number (if available).

> **Note:**
>
> Before sending us your comments, you might like to check that you have the latest version of the document and if any concerns are already addressed. To do this, access the Online Documentation available on the Oracle Help Center (docs.oracle.com) web site. It contains the most current Documentation Library plus all documents revised or released recently.

Send your comments to us using the electronic mail address: retail-doc_us@oracle.com

Please give your name, address, electronic mail address, and telephone number (optional).

If you need assistance with Oracle software, then please contact your support representative or Oracle Support Services.

If you require training or instruction in using Oracle software, then please contact your Oracle local office and inquire about our Oracle University offerings. A list of Oracle offices is available on our web site at http://www.oracle.com.

Preface

This document serves as a guide for administrators, developers, and system integrators who securely administer, customize, and integrate the Oracle Retail Supplier Evaluation Cloud Service application.

Audience

This document is intended for administrators, developers, and system integrators who perform the following functions:

- Document specific security features and configuration details for the above mentioned product, in order to facilitate and support the secure operation of the Oracle Retail Product and any external compliance standards.
- Guide administrators, developers, and system integrators on secure product implementation, integration, and administration.

It is assumed that the readers have general knowledge of administering the underlying technologies and the application.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle Retail Supplier Evaluation Cloud Service documentation set:

- *Oracle Retail Supplier Evaluation Cloud Service Administration Guide*
- *Oracle Retail Supplier Evaluation Cloud Service Implementation Guide*
- *Oracle Retail Supplier Evaluation Cloud Service Release Readiness Guide*
- *Oracle Retail Supplier Evaluation Cloud Service User Guide*
- *Oracle Retail Supplier Evaluation Cloud Service Workspace User Guide*

For information on the Oracle Retail Supplier Evaluation Cloud Service modules, see the following documents:

- *Oracle Retail Supplier Evaluation Cloud Service Process User Guide*
- *Oracle Retail Supplier Evaluation Cloud Service Product User Guide*
- *Oracle Retail Supplier Evaluation Cloud Service Reports User Guide*
- *Oracle Retail Supplier Evaluation Cloud Service Supplier User Guide*

Improved Process for Oracle Retail Documentation Corrections

To more quickly address critical corrections to Oracle Retail documentation content, Oracle Retail documentation may be republished whenever a critical correction is needed. For critical corrections, the republication of an Oracle Retail document may at times **not** be attached to a numbered software release; instead, the Oracle Retail document will simply be replaced on the Oracle Help Center (docs.oracle.com) Web site, or, in the case of Data Models, to the applicable My Oracle Support Documentation container where they reside.

Oracle Retail documentation is available on the Oracle Help Center (docs.oracle.com) at the following URL:

`https://docs.oracle.com/en/industries/retail/index.html`

An updated version of the applicable Oracle Retail document is indicated by Oracle part number, as well as print date (month and year). An updated version uses the same part number, with a higher-numbered suffix. For example, part number E123456-02 is an updated version of an document with part number E123456-01.

If a more recent version of the document is available, that version supersedes all previous versions.

Oracle Retail Documentation on the Oracle Help Center (docs.oracle.com)

Oracle Retail product documentation is available on the following web site:

`https://docs.oracle.com/en/industries/retail/index.html`

(Data Model documents can be obtained through My Oracle Support.)

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1 Introduction

Oracle Retail Supplier Evaluation Cloud Service is a collaborative cloud service for the on-boarding and evaluation of merchandising suppliers, enabling the assessment and governance of ethical, environmental, safety, and quality performance. It manages the selection of suppliers against Environmental, Social, and Governance (ESG), brand standards and governance policies, incorporating supplier self-certification survey and assessment, audit and action management, vendor performance, and incident alert notifications.

Oracle Retail Supplier Evaluation Cloud Service is composed of the following modules:

- Library enables the issue, receipt, and acceptance of policies, guidelines, and key working documents.
- Process supports the development of process briefs, plans, and workflow management.
- Product supports the development and assessment of products.
- Reports provides a reporting tool for reporting across the system, using standard templates and custom reports.
- Supplier enables the identification, selection, and approval of suppliers.

This document is divided into six main sections:

- Responsibilities - discusses the shared responsibility model of security.
- Oracle Retail SaaS Security - outlines the policies and procedures Oracle Retail uses to meet its security responsibilities.
- Supplier Evaluation Architecture - details the architecture of the Supplier Evaluation Cloud Service, particularly as it relates to security.
- Supplier Evaluation Authentication and Authorization - describes how Supplier Evaluation Cloud Service performs authentication and authorization.
- Supplier Evaluation Permissions - describes the Supplier Evaluation Cloud Service role-based security model of roles, authority profiles and permissions.
- Frequently Asked Questions - a number of specific questions related to security that are frequently asked by prospects, customers, and implementers.

The goals of this document are to:

- Explain the security responsibilities of Oracle and the retailer/portal owner in the SaaS model.
- Educate retailers/portal owners about Oracle's cloud security policies and controls.
- Describe Supplier Evaluation Cloud Services:
  - general architecture, particularly as it relates to security
  - security features
- Define additional steps customer IT staff must perform to communicate securely with Supplier Evaluation Cloud Service.
- Guide customer administrators in the actions they need to perform to:
  - create application users

  - assign roles to application users
- Provide answers to frequently asked questions about Supplier Evaluation Cloud Service security.

2
Responsibilities

As retailers migrate to the cloud, they must consider how the cloud, and more specifically SaaS, will impact their privacy, security, and compliance efforts. As the cloud service provider, Oracle Retail works together with customers to meet cloud security objectives.

Retailer/Portal Owner Responsibilities

At a high level, retailers/portal owners are responsible for:

- Understanding Oracle's security policies.
- Implementing their own corporate policies by using Oracle tools.
- Creating and administering users by using Oracle tools.
- Ensuring data quality and enforcing end-user devices security controls, so that anti-virus, malware and other malicious code checks are performed on data and files before uploading data.
- Ensuring that end-user devices meet the minimum security requirements.

To securely implement Supplier Evaluation Cloud Service, retailers/portal owners and their implementation partners should read this document to understand Oracle's security policies. This document summarizes information and contains links to many other Oracle documents.

Oracle Responsibilities

As the cloud service provider, at the highest level Oracle Retail is responsible for:

- Building secure software.
- Provisioning and managing secure environments.
- Protecting the customer’s data.

Supplier Evaluation Cloud Service fulfills its responsibilities by a combination of corporate level development practices and cloud delivery policies. Sections in this document will describe this information in great detail later in this document.

3

Oracle Retail SaaS Security

Security is a many faceted issue to address. To discuss Oracle Retail SaaS security, it helps to define and categorize the many aspects of security. For the purposes of this document, we discuss the following categories of SaaS security:

- Secure Product Engineering
- Secure Deployment
- Secure Management
- Assessment and Audit

Secure Product Engineering

Oracle builds secure software through a rigorous set of formal, always evolving security standards and practices known as Oracle Software Security Assurance (OSSA). OSSA encompasses every phase of the product development lifecycle.

More information about OSSA can be found at:

https://www.oracle.com/corporate/security-practices/assurance/

The cornerstones of OSSA are Secure Coding Standards and Security Analysis and Testing.

Secure Coding Standards include both general use cases and language specific security practices. More information about these practices can be found at:

https://www.oracle.com/corporate/security-practices/assurance/development/

Security Analysis and Testing includes product specific functional security testing and both static and dynamic analysis of the code base. Static Analysis is performed using tools including both internal Oracle tools and HP's Fortify. Dynamic Analysis focuses on APIs and endpoints, using techniques such as fuzzing to test interfaces and protocols.

https://www.oracle.com/corporate/security-practices/assurance/development/analysis-testing.html

Specific security details of the Supplier Evaluation Cloud Service are discussed in detail later in this document.

Secure Deployment

Secure deployment refers to the security of the infrastructure used to deploy the SaaS application. Key issues in secure deployment include Physical Safeguards, Network Security, Infrastructure Security, and Data Security.

Physical Safeguards

Oracle Retail SaaS applications are deployed through Oracle Cloud Infrastructure data centers. Access to Oracle Cloud data centers requires special authorization that is monitored and audited. The premises are monitored by CCTV, with entrances protected by physical

barriers and security guards. Governance controls are in place to minimize the resources that are able to access systems. Physical security safeguards are further detailed in Oracle's Cloud Hosting and Delivery Policies.

http://www.oracle.com/us/corporate/contracts/ocloud-hosting-delivery-policies-3089853.pdf

Network Security

The Oracle Cloud network is isolated from the Oracle Corporate Network. Customer instances are separated down to the VLAN level.

Infrastructure Security

The security of the underlying infrastructure used to deploy Oracle Retail SaaS is regularly hardened. Critical patch updates are applied on a regular schedule. Oracle maintains a running list of critical patch updates and security alerts. Per Oracle's Cloud Hosting and Delivery Policies, these updates are applied to all Oracle SaaS systems.

https://www.oracle.com/technetwork/topics/security/alerts-086861.html

Before Oracle Retail deploys code to SaaS, Oracle's Global Information Security team performs penetration testing on the cloud service. This penetration testing and remediation prevents software or infrastructure issues in production systems.

https://www.oracle.com/corporate/security-practices/assurance/development/ethical-hacking.html

Data Security

Oracle Retail uses a number of strategies and policies to ensure the Retailer's data is fully secured.

- Data Design - Oracle Retail applications avoid storing personal data. Where personal information data exists in a system, Data Minimization, Right to Access, and Right to Forget services exist to support data privacy standards.
- Storage - Oracle Retail applications use encrypted tablespaces to store sensitive data.
- Transit - All data is encrypted in transit, Retail SaaS uses TLS for secure transport of data, as documented in Oracle's Cloud Hosting and Delivery policy.

https://www.oracle.com/assets/ocloud-hosting-delivery-policies-3089853.pdf

Secure Management

Oracle Retail manages SaaS based on a well-documented set of security-focused Standard Operating Procedures (SOPs). The SOPs provide direction and describe activities and tasks undertaken by Oracle personnel when delivering services to customers. SOPs are managed centrally and are available to authorized personnel through Oracle's intranet on a need-to-know basis.

All network devices, servers, OS, applications and databases underlying Oracle Retail Cloud Services are configured and maintain auditing and logging. All logs are forwarded to a Security Information and Event Management (SIEM) system. The SIEM is managed by the Security Engineering team and is monitored 24/7 by the GBU Security Operations team. The SIEM is configured to alert the GBU Security Operations team regarding any conditions deemed to be

potentially suspicious, for further investigation. Access given to review logs is restricted to a subset of security administrators and security operations personnel only.

Assessment and Audit

Oracle Cloud meets all ISO/IEC 27002 Codes of Practice for Information Security Controls. Third Party Audit Reports and letters of compliance for Oracle Cloud Services are periodically published.

4

Supplier Evaluation Cloud Service Architecture

The Supplier Evaluation Cloud Service application is deployed on Oracle's Global Business Unit Cloud Services Foundation Services. The application is deployed in a highly available, high performance, horizontally scalable architecture. Supplier Evaluation Cloud Service uses either Oracle Identity Cloud Service (IDCS) or Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) as its identity provider (IDP). Information about logical, physical and data architecture in this document focuses on how the architecture supports security.

Architecture Overview

Most customer access to the Supplier Evaluation Cloud Service is through the web tier. The web tier contains the perimeter network services that protects the Supplier Evaluation application from the internet at large. All traffic from the web tier continues to the Web Tier Security Server (WTSS), which in turn uses the customer's Oracle Identity Cloud Service (IDCS) or Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) tenancy to perform authentication. More information about authentication through IDCS or OCI IAM is provided later in this document.

The Supplier Evaluation application is deployed on a Kubernetes cluster. Reporting is provided by Oracle BI Publisher which can connect to the underlying database.

The underlying container DBaaS includes one pluggable database (PDB) for Supplier Evaluation. Applications are able to access the Supplier Evaluation schema on the Supplier Evaluation PDB. Transparent data encryption (TDE) is set during provisioning. Tablespaces that contain personal data are encrypted.

Supplier Evaluation Cloud Service applications integrate with external business systems by using:

- Native files upload/download. All inbound files are scanned by anti-virus and anti-malware software.
- Native Rest Services.

Supplier Evaluation Cloud Service authenticates native rest services using OAUTH2.0 through IDCS or OCI IAM. As a common authentication pattern is used, web service users are subject to the same strong controls as application users.

All rest service calls are logged in the application logs.

Access Flow

This document does not explain the full access flow of the Supplier Evaluation Cloud Service, but instead focuses on the high level aspects of this data flow that relate to security.

Supplier Evaluation Cloud Service is deployed on a Kubernetes cluster. Each application resides in an appropriate tier and each tier resides in its own subnet. Communication between tiers within the Supplier Evaluation Cloud Service is limited by subnet ingress security lists.

To reduce attack surface, access to the Supplier Evaluation Cloud Service from the open internet is very limited.

Business Users (using a web browser) and external web service endpoints access application over https/443. Firewall and load balancer in the DMZ route to the customer tenancy by using reverse proxy forward to WTSS. WTSS forwards unauthenticated requests to the customer's IDCS or OCI IAM tenancy using the NAT Gateway. IDCS or OCI IAM sends authentication HTML content to the end user (IDCS or OCI IAM Logon page). On successful AuthN, WTSS sends a call to the reverse proxy ingress controller, which routes to the appropriate application component.

Access to the underlying DBaaS is only available through the application M-Tier. The M-Tier is able to get and place files into object storage. Both outbound web service traffic (811) and replication of data (912) are routed through the outbound proxy in the DMZ.

A subset of Oracle Retail AMS has very limited access to the underlying M-Tier. This access is limited to a small subset of Oracle employees as described in Oracle's Cloud Hosting and Delivery policy.

https://www.oracle.com/assets/ocloud-hosting-delivery-policies-3089853.pdf

5

Supplier Evaluation Cloud Service Authentication and Authorization

Authentication confirms the identity of a user (is this user John Smith?). Authorization determines what parts of an application a user can access and what actions the user can perform (is John Smith allowed to create a supplier account?).

Authentication and IDCS or OCI IAM

Supplier Evaluation Cloud Service uses either Oracle Identity Cloud Service (IDCS) or Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) as its identity provider (IDP):

- Oracle Identity Cloud Service (IDCS):

  https://www.oracle.com/cloud/paas/identity-cloud-service.html

- Oracle Cloud Infrastructure Identity and Access Management (OCI IAM):

  https://docs.oracle.com/en-us/iaas/Content/Identity/home.htm

When a user connects to the Supplier Evaluation Cloud Service UI, application UR requests are redirected to the IDCS or OCI IAM login screen. IDCS or OCI IAM authenticates the user. When a user logs out of the Supplier Evaluation Cloud Service, Supplier Evaluation invokes an IDCS or OCI IAM logout to disable session authentication.

IDCS and OCI IAM

IDCS and OCI IAM are Oracle's cloud native security and identity platforms. They provide a powerful set of hybrid identity features to maintain a single identity for each user across cloud, mobile, and on-premises applications. Both IDCS and OCI IAM enable single sign on (SSO) across all applications in a customer's Oracle Cloud tenancy. Customers can also integrate IDCS or OCI IAM with other on premise applications to extend the scope of this SSO.

Both IDCS and OCI IAM are available in two tiers: Foundation and Standard.

- Oracle Identity Cloud Service Foundation: Oracle provisions this free version of Oracle Identity Cloud Service for customers that subscribe to Oracle Software-as-a-Service (SaaS), Oracle Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) applications. A customer can use this version to provide basic identity management functionality, including user management, group management, password management, and basic reporting.
- Oracle Identity Cloud Service Standard: This licensed edition provides customers with an additional set of Oracle Identity Cloud Service features to integrate with other Oracle Cloud services, including Oracle Cloud SaaS and PaaS, custom applications hosted on-premises, on Oracle Cloud, or on a third-party cloud, as well as third-party SaaS applications. Features listed in this pricing tier are applicable for both Enterprise users and Consumer users.

Details of the specific features available in each tier and IDCS or OCI IAM Standard Tier licensing model are available in Administering Oracle Identity Cloud Service. Supplier Evaluation Cloud Service only requires the Foundation Tier, as the Foundation Tier includes

key features such as User and Group Management, Self-Service Profile Management and Password Reset, SSO. However, Oracle Retail customers may wish to consider licensing the Standard Tier of IDCS or OCI IAM to also have access to more advanced identity features including Identity Synchronization with Microsoft Active Directory, SSO for Third Party Cloud Services and Custom Applications, Multi-Factor Authentication, and generic SCIM Templates.

IDCS, OCI IAM, and Application Users

Upon provisioning a new cloud service instance, Oracle Retail creates a single delegate customer administrator user.

The customer administrator user has the ability to define password complexity and rotation rules. All Application User maintenance is performed by Customer Administrators by using IDCS or OCI IAM. A key feature of IDCS or OCI IAM is that basic user maintenance can be further delegated through identity self-service.

When application users are created in IDCS or OCI IAM, they must be associated with an appropriate Oracle Retail Enterprise Role to access Supplier Evaluation Cloud Service. For more detailed information and procedures, see Managing Oracle Identity Cloud Service Users in *Administering Oracle Identity Cloud Service*.

> **Note:**
>
> IDCS or OCI IAM username will be passed to Supplier Evaluation as the application user id. It will be persisted on the database as part of the basic Supplier Evaluation transaction audit trail. If corporate email address is used as the IDCS or OCI IAM username, corporate email address will be persisted to the Supplier Evaluation database.
>
> To fully inform Supplier Evaluation users that their corporate email address will be saved, we recommend that retailers implement IDCS or OCI IAM Terms of Use functionality.
>
> The IDCS or OCI IAM Terms of Use feature enables retailers to set the terms and conditions for users to access an application, based on the user's consent. This feature allows the identity domain administrator to set relevant disclaimers for legal or compliance requirements and enforce the terms by refusing the service. The Terms of Use feature can be used to explicitly obtain user consent to persist corporate email address for Supplier Evaluation auditing. See *Administering Oracle Identity Cloud Service* for more information about Terms of Use.
>
> https://docs.oracle.com/en/cloud/paas/identity-cloud/uaids/understand-terms-use.html

Authorization

While IDCS and OCI IAM have some authorization features, Supplier Evaluation Cloud Service manages application functional security using a role-based model that employs permissions security where resources are protected by roles and authority profiles that are assigned to users. The application includes a number of default roles.

6

Supplier Evaluation Cloud Service Permissions

In Supplier Evaluation Cloud Service, role-based permission security is implemented to control:

- Access to navigational links/tasks in the application. The role associated with the user (for example, a Technologist or Buyer) determines the set of links visible in the task pane.
- Access to various UI widgets in the screens such as buttons, menu items, LOVs, Panels, and so on. The role determines if the UI widgets are to be shown or hidden and if shown whether they need to be enabled or disabled.
- How the screens will be opened, such as in an edit or view only mode based on the role the user belongs to and the permissions mapped to that role.

Roles and authority profiles are assigned to users to define their permissions, or access rights, to data and functionality within the application (including workflow, actions, screens, and in some cases specific fields). Roles are logical groupings of authority profiles that permit a user to perform a complete task to fulfill responsibilities within the context of their job. Authority profiles are associated to a set of permissions which provide different access rights. In this manner, an application role becomes the container that grants permissions to its members to access the application tasks, screens and the functionality within. The default configuration includes a number of default roles.

Authority profiles are intended to build on one another and work in a hierarchical manner. The example in Table 6-1 illustrates how this works using Audits as an example. The most basic level of access is Audit Reader, which grants the user permission to search and view audits. The next level of access is Audit Editor, which grants the user the ability to search and view audits, but also to create, maintain, and approve them. The final level of access in this example is Audit Administrator, which grants the user the access right of Audit Editor, but with the additional rights to delete audits (subject to other business rules), plus the administrative rights for maintaining the different types of audit templates, and supporting glossaries and configuration settings.

Table 6-1 Authority Profiles and Permissions

Authority Profile	Permissions
Audit Reader	• Search Audits • View Audits
Audit Editor	• All Privileges of Audit Reader • Create Audits • Maintain Audits • Approve Audits
Audit Administrator	• All Privileges of Audit Editor • Delete Audits • Maintain Audit Templates & Glossaries

Permissions are essentially what actions that a user can perform, and on what data - controlled by collections of roles and authority profiles. The system determines the *best case* level of access based on the user's allocated authority profiles For example, if a user possesses both

Audit Reader and Audit Editor authority profiles, the system will grant the user edit access over read access. The predefined permissions associated to each authority profile may be customized by configuring the Supplier Evaluation Permissions rules.

Roles and authority profiles are assigned to a user by another user with User Administrator access rights and the permission to grant those roles or authority profiles. A user cannot assign their own permissions.

While the configurability of roles and permissions allow for custom levels of access to be defined, the Supplier Evaluation application also applies various implicit permissions rules which cannot be overridden through configuration. For example, hard-coded security rules ensure that a supplier user does not have access to data of other supplier organizations, and that only retailer/portal owner users (with the necessary access rights) have access to the Administration and Reporting modules, and so forth.

Roles

Also referred to as User Roles, roles align with titles or jobs within an organization, such as a Technologist or Buyer. Roles are used to classify users based on job responsibilities and actions to be performed in the application. One or more roles as well as additional individual authority profiles, if desired, are assigned to each user. When a user logs into the application, based on the authority profiles assigned to the user, the system determines which permissions have been granted to the user and the system features are enabled accordingly.

For example, within Supplier Evaluation, a Technologist may have the ability to create and progress Audits, but not the ability to create new Audit templates. Specific users who have the responsibility for maintaining the templates will be granted an additional Audit Administrator authority profile that provides them with the necessary level of access to maintain the Audit templates.

Roles Provided at Initial Setup

A default security configuration is provided with the application during installation and is intended to be used as a starting point as you define the roles that align for your business and users. The provided roles can be modified by adding or removing authority profiles to adjust the access granted to the role, or the roles can be deleted completely. Additional roles can be created and mapped to the desired authority profiles. Administrator users can maintain the roles, authority profiles and permissions in the Supplier Evaluation Admin area.

Details about how to manage these application security policies are available in the Managing User Access chapter in the *Oracle Retail Supplier Evaluation Cloud Service Administration Guide*.

These roles are provided in the default security configuration:

- **Assistant Technologist** - Assists the Technologist in collaborating with suppliers for the on-going management of supplier sites and their products. Similar level of access as Technologist.
- **Auditor** - Carries out site audits and visits. May be a third-party user.
- **Buyer** - Develops business strategies and seasonal assortment for a brand. Similar access as Technologist, but typically read-only.
- **Laboratory** - Third-party users with basic level of access for reading documents and alerts.

- **Oracle Authorized User** - An administrator with the highest level of access to the configuration of the system. Has full access to the Admin area, including system parameters, custom fields, permissions and system text.
- **Power User** - An administrator with similar access as System Administrator, plus the ability to maintain system text and delete unused supplier and site accounts.
- **Process Administrator** - A retailer/portal owner with the administration responsibility for configuring templates for process projects, their activities and teams.
- **Process Manager** - A retailer/portal owner user with responsibility for scheduling and progressing projects and their activities.
- **Product Development Manager** - Develops product ranges and selects suppliers. Similar access as Technologist, but typically read-only.
- **Restricted Auditor** - An auditor who is restricted to accessing the audits and visits of only specific supplier sites. May be a third-party user.
- **Retailer Supplier Administrator** - A retailer/portal owner with the ability to administer additional supplier account information on behalf of the supplier, such as their users and contact details.
- **Site Administrator** - A user at a supplier site with responsibility for managing accounts for other users and contacts at the site.
- **Site Inspector** - A user responsible for quality assurance. Has a basic level of access.
- **Site User** - A user at a supplier site who collaborates with the retailer/portal owner in the on-going management of the site and its products.
- **Supplier Administrator** - A user at a supplier with responsibility for managing accounts for other users and contacts at the supplier and its sites.
- **Supplier User** - A user at a supplier who collaborates with the retailer/portal owner in the on-going management of the supplier's sites and its products.
- **Surveillance Laboratory User** - Uploads the laboratory test results for products. No access to other areas of the system. May be a third-party user.
- **System Administrator** - An administrator with responsibility for maintaining glossaries, users and documents.
- **Technologist** - Evaluates new suppliers and has general due diligence responsibility for the safety and quality aspects of the supplier's sites and products. Accesses most areas of the system.

For further information on the default set of roles, see the Appendix: Roles and Appendix: Authority Profile to Role Mappings.

Authority Profiles

Authority profiles grant access to specific tasks, links, and actions within the application. The access controlled by a particular authority profile is fixed and can only be changed by an enhancement to the application. You can control the functions and features to which a user has access by grouping the desired authority profiles into roles, or can assign individual authority profiles in addition to roles.

An authority profile may be part of a set that provides varying degrees of access to an area, for example Audit Reader, Audit Editor, and Audit Administrator as described in the Table 6-1 example. Alternatively, an authority profile may just control a specific feature, which is granted to individual users who perform the related function. For example, the Library Administrator

authority profile is granted to individuals who have the responsibility of publishing documents in addition to their main role.

Authority profiles are classified as being for a retailer/portal owner user or for a supplier/site user; they can therefore only be granted to the relevant types of users.

Authority profiles are coded into the system to control the related behavior. Therefore it is not possible to configure new authority profiles in the same way that new roles can be created. The supplied set of authority profiles are can be renamed, but cannot be deleted.

A user's *best case* level of access is determined by Authority Profile Groups, where related authority profiles are grouped in a hierarchy (for example Audit Administrator, Audit Editor, Audit Reader). If through the user's allocation of roles and authority profiles they have conflicting access right (for example Audit Editor and Audit Reader), the system will grant the highest level of access (for example edit rights) based on the hierarchy.

For the full list of Authority Profiles, see the Appendix: Authority Profiles. For the full list of Authority Profile Groups, see the Appendix: Authority Profile Groups. For the mapping of Authority Profiles to Roles, see the Appendix: Authority Profile to Role Mappings.

Permissions

The rules for what data and functionality each authority profile has access to is defined in the Supplier Evaluation Permissions rules. The rules are configurable and are maintained by a spreadsheet download/upload facility within the Admin area.

The Permissions spreadsheet consists of a page for each module or area, containing a matrix of the access permitted to data and functionality elements by authority profile.

The data elements can be defined for an entire record type, or for specific pages, sections or individual fields within the record. The functionality elements are defined for menu options, actions and buttons.

The available levels of access are:

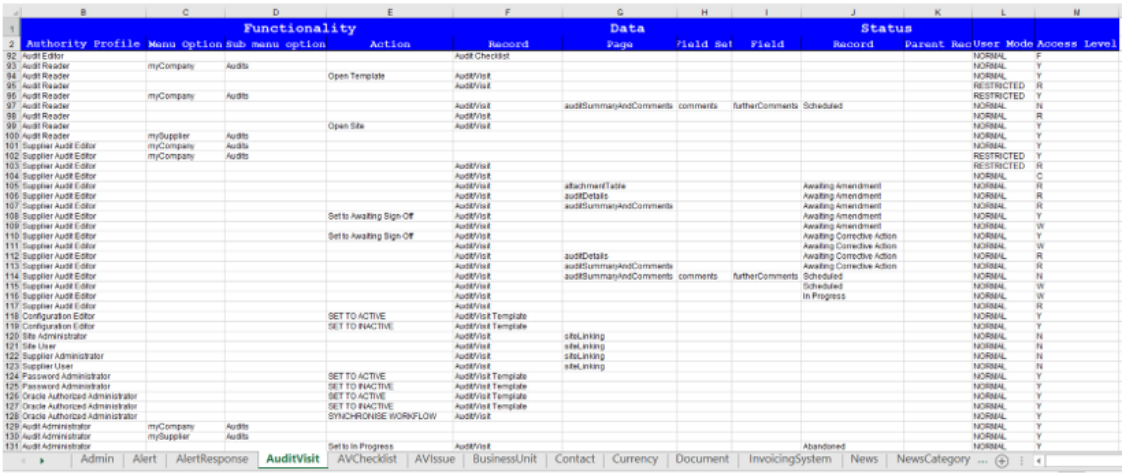
- R - read access
- W - write access
- C - record creation
- F - full access
- Y - access permitted
- N - access not permitted

The matrix can therefore be configured in a way that gives an authority profile full access to a data record and its functionality, or more granular access rights, such as to only view or edit certain aspects of a record, with a specific set of actions available.

By default, no access to data and functionality is assumed. Access must be specifically grated to the appropriate authority profiles, by defining Permissions rules.

Figure 6-1 shows an example of the Supplier Evaluation Permissions spreadsheet.

Figure 6-1 Permissions Spreadsheet



	B	C	D	E	F	G	H	I	J	K	L	M
1	Functionality				Data				Status			
2	Authority Profile	Menu Option	Sub menu option	Action	Record	Page	Field Set	Field	Record	Parent Rec	User Mode	Access Level
92	Audit Editor				Audit Checklist						NORMAL	F
93	Audit Reader	myCompany	Audits								NORMAL	Y
94	Audit Reader			Open Template	AuditVisit						NORMAL	Y
95	Audit Reader				AuditVisit						RESTRICTED	R
96	Audit Reader	myCompany	Audits								RESTRICTED	Y
97	Audit Reader				AuditVisit	auditSummaryAndComments	comments	furtherComments	Scheduled		NORMAL	N
98	Audit Reader				AuditVisit						NORMAL	R
99	Audit Reader			Open Site	AuditVisit						NORMAL	Y
100	Audit Reader	mySupplier	Audits								NORMAL	Y
101	Supplier Audit Editor	myCompany	Audits								NORMAL	Y
102	Supplier Audit Editor	myCompany	Audits								RESTRICTED	Y
103	Supplier Audit Editor				AuditVisit						RESTRICTED	R
104	Supplier Audit Editor				AuditVisit						NORMAL	C
105	Supplier Audit Editor				AuditVisit	attachmentTable			Awaiting Amendment		NORMAL	R
106	Supplier Audit Editor				AuditVisit	auditDetails			Awaiting Amendment		NORMAL	R
107	Supplier Audit Editor				AuditVisit	auditSummaryAndComments			Awaiting Amendment		NORMAL	R
108	Supplier Audit Editor			Set to Awaiting Sign-Off	AuditVisit				Awaiting Amendment		NORMAL	Y
109	Supplier Audit Editor				AuditVisit				Awaiting Amendment		NORMAL	W
110	Supplier Audit Editor			Set to Awaiting Sign-Off	AuditVisit				Awaiting Corrective Action		NORMAL	Y
111	Supplier Audit Editor				AuditVisit				Awaiting Corrective Action		NORMAL	W
112	Supplier Audit Editor				AuditVisit	auditDetails			Awaiting Corrective Action		NORMAL	R
113	Supplier Audit Editor				AuditVisit	auditSummaryAndComments			Awaiting Corrective Action		NORMAL	R
114	Supplier Audit Editor				AuditVisit	auditSummaryAndComments	comments	furtherComments	Scheduled		NORMAL	N
115	Supplier Audit Editor				AuditVisit				Scheduled		NORMAL	W
116	Supplier Audit Editor				AuditVisit				In Progress		NORMAL	W
117	Supplier Audit Editor				AuditVisit						NORMAL	R
118	Configuration Editor			SET TO ACTIVE	AuditVisit Template						NORMAL	Y
119	Configuration Editor			SET TO INACTIVE	AuditVisit Template						NORMAL	Y
120	Site Administrator				AuditVisit	siteLinking					NORMAL	N
121	Site User				AuditVisit	siteLinking					NORMAL	N
122	Supplier Administrator				AuditVisit	siteLinking					NORMAL	N
123	Supplier User				AuditVisit	siteLinking					NORMAL	N
124	Password Administrator			SET TO ACTIVE	AuditVisit Template						NORMAL	Y
125	Password Administrator			SET TO INACTIVE	AuditVisit Template						NORMAL	Y
126	Oracle Authorized Administrator			SET TO ACTIVE	AuditVisit Template						NORMAL	Y
127	Oracle Authorized Administrator			SET TO INACTIVE	AuditVisit Template						NORMAL	Y
128	Oracle Authorized Administrator			SYNCHRONISE WORKFLOW	AuditVisit						NORMAL	Y
129	Audit Administrator	myCompany	Audits								NORMAL	Y
130	Audit Administrator	mySupplier	Audits								NORMAL	Y
131	Audit Administrator			Set to In Progress	AuditVisit				Abandoned		NORMAL	Y

Admin | Alert | AlertResponse | AuditVisit | AVChecklist | AVIssue | BusinessUnit | Contact | Currency | Document | InvoicingSystem | News | NewsCategory

For further details on the Supplier Evaluation Permissions and configuring the spreadsheet see the Managing User Access chapter in the *Oracle Retail Supplier Evaluation Cloud Service Administration Guide*.

Various implicit permissions rules are hard-coded into the Supplier Evaluation security model and cannot be overridden through the configurable permissions rules. These include the segregation of data to ensure that a supplier users only have access to the data of their own organization.

7

Frequently Asked Questions

This chapter includes a number of specific questions related to security that are frequently asked by prospects, customers and implementers.

Table 7-1 Frequently Asked Questions

Question	Answer
Does Supplier Evaluation Cloud Service support data encryption?	Yes. All data is stored in encrypted tablespace at rest, and is encrypted in transit. Supplier Evaluation Cloud Service uses TLS for secure transport of data.
Does Supplier Evaluation Cloud Service provide network segregation?	Yes. The Oracle Cloud network is isolated from the Oracle corporate network.
Does Supplier Evaluation Cloud Service provide secure backups?	Yes. Backup is a standard process for Supplier Evaluation Cloud Service. Database and application servers are backed up both incrementally (daily) and fully (weekly). Backups are stored for at least 60 days.
Does Supplier Evaluation Cloud Service provide centralized logging?	Yes. All application and infrastructure logs are forwarded to a centralized Security Information and Event Management system.
Does Supplier Evaluation Cloud Service provide anti-virus?	Yes. All files uploaded into Supplier Evaluation Cloud Service are scanned by anti-virus and anti-malware software. All hosts in the cloud service are regularly patched with the latest critical patch updates.
Does Supplier Evaluation Cloud Service provide strong authentication options such as 2-factor, one-time Password?	Multi-Factor Authentication is an option if a customer chooses to license the Standard Tier of IDCS or OCI IAM.
Does Supplier Evaluation Cloud Service include a configurable warning banner which is presented upon login?	Terms of Use is an option if a customer chooses to license the Standard Tier of IDCS or OCI IAM. It presents disclaimers and acceptable use policies to users. The Supplier Evaluation application also allows for the configuration of portal specific terms and conditions, which are presented for the user to accept or reject upon first login.
Does Supplier Evaluation Cloud Service implement access lists to secure each tier of the solution?	Yes. Communication between tiers within Supplier Evaluation Cloud Service is limited by subnet ingress security lists.
Does Supplier Evaluation Cloud Service include and support the capability to change default account passwords?	All user password management occurs in IDCS or OCI IAM.
Does Supplier Evaluation Cloud Service support Roles with defined access levels?	Yes. Oracle Retail Enterprise roles span Oracle Retail applications. Within Supplier Evaluation Cloud Service, privileges and duties can be assigned to roles to define what is accessible to certain types of users.
Does Supplier Evaluation Cloud Service support synchronizing with an external time source?	All hosts within the solution are synchronized to the same time source.

Table 7-1 (Cont.) Frequently Asked Questions

Question	Answer
Does Supplier Evaluation Cloud Service provide strong password options such as complexity, history, aging, and account lockout?	IDCS or OCI IAM provides robust password policy management functionality. When a user creates a password, IDCS or OCI IAM validates the password against the password policies. More information about password policies is available at https://docs.oracle.com/en/cloud/paas/identity-cloud/uaids/manage-oracle-identity-cloud-service-password-policies1.html.

A
Appendix: Roles

Table A-1 lists the default set of Supplier Evaluation roles.

Each role has a description, a unique code, and is assigned a user type to control which type of users it may be granted:

- Retailer - retailer/portal owner users
- Supplier - supplier users at the level of the supplier account
- Site - supplier users at the level of individual sites

Table A-1 Roles

Role	User Type	Code
Assistant Technologist	Retailer	ASSISTANT TECHNOLOGIST
Auditor	Retailer	AUDITOR
Buyer	Retailer	BUYER
Laboratory	Retailer	LABORATORY
Oracle Authorized User	Retailer	ORACLE AUTHORIZED USER
Power User	Retailer	POWER USER
Process Administrator	Retailer	PROJECT ADMINISTRATOR
Process Manager	Retailer	PROJECT MANAGER
Restricted Auditor	Retailer	RESTRICTED AUDITOR
Retailer Supplier Administrator	Retailer	RETAILER SUPPLIER ADMINISTRATOR
Site Administrator	Site	SITE ADMINISTRATOR
Site Inspector	Retailer	SITE INSPECTOR
Site User	Site	SITE USER
Supplier Administrator	Supplier	SUPPLIER ADMINISTRATOR
Supplier User	Supplier	SUPPLIER USER
System Administrator	Retailer	SYSTEM ADMINISTRATOR
Technologist	Retailer	PRODUCT TECHNOLOGIST

B

Appendix: Authority Profiles

Table B-1 lists the Supplier Evaluation authority profiles.

Each authority profile has a description and a unique code.

Table B-1 Authority Profiles

Description	Code
Advanced Reporting Administrator	ADVANCED REPORTING ADMINISTRATOR
Advanced Reporting Reader	ADVANCED REPORTING READER
Advanced Reporting User	ADVANCED REPORTING USER
Alert Administrator	RETAILER ALERT ADMINISTRATOR
Alert Reader (Retailer)	RETAILER ALERT READER
Alert Reader (Supplier)	SUPPLIER ALERT READER
Alert Responder	SUPPLIER ALERT RESPONDER
Artwork User	MY ARTWORK USER
Assessment Administrator	SCORECARD ADMINISTRATOR
Assessment Editor	SCORECARD EDITOR
Assessment Reader	SCORECARD READER
Assessment Requester	SCORECARD REQUESTER
Audit Administrator	AUDIT ADMINISTRATOR
Audit Editor	AUDIT EDITOR
Audit Reader	AUDIT READER
Configuration Editor	CONFIGURATION EDITOR
Custom Field Administrator	CUSTOM FIELD ADMINISTRATOR
Dashboard Access	DASHBOARD ACCESS
Global Changes Administrator	GLOBAL CHANGES ADMINISTRATOR
Glossary Administrator	GLOSSARY ADMINISTRATOR
Integration Administrator	INTEGRATION ADMINISTRATOR
Library Administrator	LIBRARY ADMINISTRATOR
Library Reader	LIBRARY READER
News Administrator	NEWS ADMINISTRATOR
Oracle Authorized Administrator	ORACLE AUTHORIZED ADMINISTRATOR
Power Administrator	POWER ADMINISTRATOR
Process Administrator	PROJECT ADMINISTRATOR
Process Manager	PROJECT MANAGER
Product Administrator	PRODUCT ADMINISTRATOR
Product Record Codes Administrator	PRODUCT RECORD CODES ADMINISTRATOR

Table B-1 (Cont.) Authority Profiles

Description	Code
Restricted Auditor	RESTRICTED AUDITOR
Retailer Product Editor	RETAILER PRODUCT EDITOR
Retailer Product Reader	RETAILER PRODUCT READER
Retailer Score Viewer	RETAILER SCORE VIEWER
Site Administrator	SITE ADMINISTRATOR
Site Status Editor	SITE STATUS EDITOR
Site User	SITE USER
Supplier & Site Administrator	SUPPLIER & SITE ADMINISTRATOR
Supplier & Site Creator	SUPPLIER & SITE CREATOR
Supplier & Site Editor	SUPPLIER & SITE EDITOR
Supplier & Site Reader	SUPPLIER & SITE READER
Supplier Administrator	SUPPLIER ADMINISTRATOR
Supplier Assessment Editor	SUPPLIER SCORECARD EDITOR
Supplier Audit Editor	SUPPLIER AUDIT EDITOR
Supplier Contacts Administrator	SUPPLIER CONTACTS ADMINISTRATOR
Supplier Product Editor	SUPPLIER PRODUCT EDITOR
Supplier Site & Contact Editor	SUPPLIER SITE & CONTACT EDITOR
Supplier User	SUPPLIER USER
Supplier User Editor	SUPPLIER USER EDITOR
System Text Administrator	SYSTEM TEXT ADMINISTRATOR
Upload Administrator	UPLOAD ADMINISTRATOR
User Administrator	USER ADMINISTRATOR
User Editor	USER EDITOR

C

Appendix: Authority Profile Groups

Table C-1 lists the Supplier Evaluation authority profile groups.

Each authority profile group consists of a set of authority profiles, in a hierarchical order of level of access.

Table C-1 Authority Profile Groups

Authority Profile Group	Code	Authority Profiles
Alerts	ALERTS	Retailer Alert Administrator Retailer Alert Reader Supplier Alert Responder Supplier Alert Reader
Audit	AUDIT	Audit Administrator Audit Editor Restricted Auditor Audit Reader Supplier Audit Editor
Custom Field Administrator	CUSTOM FIELD ADMINISTRATOR	Custom Field Administrator
Dashboard	DASHBOARD	Dashboard Access
Document	DOCUMENT	Library Administrator Library Reader
Global	GLOBAL	Global Changes Administrator
Glossary Administrator	GLOSSARY ADMINISTRATOR	Glossary Administrator
Integration	INTEGRATION	Integration Administrator
Artwork	MYARTWORK	My Artwork User
Process	MYPROJECT	Process Administrator Process Manager
News	NEWS	News Administrator
Power Administrator	POWER ADMINISTRATOR	Power Administrator
Product Records	PRODUCT	Product Administrator Retailer Product Editor Retailer Product Reader Supplier Product Editor
Product Record Codes	PRODUCT RECORD CODES ADMINISTRATOR GROUP	Product Record Codes Administrator
Reporting	REPORTING	Advanced Reporting Administrator Advanced Reporting User Advanced Reporting Reader

Table C-1 (Cont.) Authority Profile Groups

Authority Profile Group	Code	Authority Profiles
Assessments	SCORECARDS	Assessment Administrator Assessment Requester Assessment Editor Supplier Assessment Editor Assessment Reader
Scoring	SCORING	Retail Score Viewer
Sites Status	SITESTATUS	Site Status Editor
Supplier, Site & Contact	SUPPLIERSITE&CONTACT	Supplier Contacts Administrator Supplier Site & Contact Editor
Supplier Site (Retailer)	SUPPLIERSITERET	Supplier & Site Administrator Supplier & Site Creator Supplier & Site Editor Supplier & Site Reader
Supplier Site (Supplier)	SUPPLIERSITESUP	Supplier Administrator Site Administrator Supplier User Site User
System	SYSTEM	Oracle Authorized Administrator Configuration Editor
System Text Administrator	SYSTEM TEXT ADMINISTRATOR	System Text Administrator
Upload Administrator	UPLOAD ADMINISTRATOR	Upload Administrator
User	USER	User Administrator User Editor Supplier User Editor

D

Appendix: Authority Profile to Role Mappings

Table D-1 maps the authority profiles to each of the default Supplier Evaluation roles.

Roles are assigned a user type to control which type of users it may be granted (Retailer, Supplier, or Site).

Table D-1 Authority Profile to Role Mappings

Role	User Type	Authority Profiles
Assistant Technologist	Retailer	Library Reader Audit Editor Supplier & Site Creator Site Status Editor Advanced Reporting User Alert Reader Assessment Editor Retailer Product Editor
Auditor	Retailer	Library Reader Audit Editor Supplier & Site Reader Advanced Reporting User Alert Reader Retailer Product Reader
Buyer	Retailer	Library Reader Audit Reader Supplier & Site Reader Advanced Reporting User Alert Reader Retailer Product Reader
Laboratory	Retailer	Library Reader Alert Reader
Oracle Authorized User	Retailer	Artwork User Custom Field Administrator Dashboard Access Glossary Administrator Integration Administrator Oracle Authorized Administrator System Text Administrator Upload Administrator

Table D-1 (Cont.) Authority Profile to Role Mappings

Role	User Type	Authority Profiles
Power User	Retailer	Assessment Reader Configuration Editor Site Status Editor Library Administrator News Administrator Audit Administrator Global Changes Administrator Supplier & Site Creator Advanced Reporting Administrator User Administrator Alert Administrator Assessment Administrator Power Administrator Process Administrator Product Administrator
Process Administrator	Retailer	Process Administrator
Process Manager	Retailer	Process Manager
Product Development Manager	Retailer	Library Reader Audit Reader Supplier & Site Reader Advanced Reporting User Alert Reader Retailer Product Reader
Restricted Auditor	Retailer	Library Reader Restricted Auditor Library Reader Alert Reader
Retailer Supplier Administrator	Retailer	Supplier & Site Administrator Supplier User Editor Supplier Contacts Administrator
Site Administrator	Supplier	Site Administrator Library Reader User Editor Supplier Site & Contact Editor Supplier Audit Editor Alert Responder Supplier Assessment Editor Supplier Product Editor
Site Inspector	Retailer	Library Reader

Table D-1 (Cont.) Authority Profile to Role Mappings

Role	User Type	Authority Profiles
Site User	Supplier	Site User Library Reader Supplier Audit Editor Alert Reader Supplier Assessment Editor Supplier Product Editor
Supplier Administrator	Supplier	Alert Responder Dashboard Access Library Reader Supplier Administrator Supplier Assessment Editor Supplier Audit Editor Supplier Site & Contact Editor User Editor Supplier Product Editor
Supplier User	Supplier	Supplier User Library Reader Supplier Audit Editor Alert Reader Supplier Assessment Editor Supplier Product Editor
System Administrator	Retailer	Advanced Reporting Administrator Advanced Reporting User Alert Administrator Assessment Administrator Audit Administrator Configuration Editor Global Changes Administrator Library Administrator News Administrator Process Administrator Site Status Editor Supplier & Site Creator User Administrator Product Administrator Dashboard Access

Table D-1 (Cont.) Authority Profile to Role Mappings

Role	User Type	Authority Profiles
Technologist	Retailer	Advanced Reporting User
		Alert Reader
		Assessment Editor
		Audit Editor
		Library Reader
		Retailer Score Viewer
		Site Status Editor
		Supplier & Site Creator
		Retailer Product Editor