Oracle Warehouse Management Cloud

Security Guide

Release 26D

Oracle Warehouse Management Cloud
Security Guide

Release 26D

G58449-01

Copyright © 2026, Oracle and/or its affiliates.

Author: Oracle WMS Cloud Product Team

Contents

Get Help i

1 Shared Security Responsibiiity 1

Shared Security 1
General Principles 2
Service Components 3
Service Security Features 3

2 Secure Configuration 19

Secure Configuration Overview 19

3 Break Glass Support for Environments 21

Break Glass for Oracle WMS 21
Oracle Managed Access (Break Glass) 21
Customer Managed Keys for Oracle Break Glass 23

4 Security Considerations 33

Security Considerations 33

5 Appendix 35

Group Permissions 35

Get Help

In addition to the resources available in Oracle Help Center, you can explore training, connect with the Oracle community, and share your feedback.

Get Training

Increase your knowledge of Oracle Cloud by taking courses at *Oracle University*.

Join Our Community

Use *Cloud Customer Connect* to get information from industry experts at Oracle and in the partner community. You can join forums to connect with other customers, post questions, suggest *ideas* for product enhancements, and watch events.

Share Your Feedback

We welcome your feedback about Oracle Applications user assistance. If you need clarification, find an error, or just want to tell us what you found helpful, we'd like to hear from you.

You can email your feedback to *oracle_fusion_applications_help_ww_grp@oracle.com*.

Thanks for helping us improve our user assistance!

1 Shared Security Responsibiiity

Shared Security

This document contains recommendations on how to make software installation more secure. All of these recommendations should be evaluated carefully and implemented based on the unique needs of the customer and the compliance requirements for internal security procedures and guidelines.

This guide applies generally to **Oracle Fusion Cloud Warehouse Management.** This document lays down the guidelines that ensures that users have the proper authority to see data, load new data, or update existing data as this is an important aspect of the Oracle WMS Cloud Application.

A few points for you to consider:

- Do all users need the same level of access to the data and to the functions provided on customers side of applications?
- Are there subsets of users that need access to privileged functions?
- Are some documents restricted to certain classes of users?

This document will serve as answers to questions like these which helps to provide the basis for the security requirements for the application.

Acronyms

Term	Definition
CPUs	Critical Patch Updates
Machine	The physical (or virtual) server.
IHT	Inventory History Transactions

The Oracle Warehouse Management Cloud Service implements many security measures to ensure the service is secure by default. However, cloud customers share the responsibility to ensure the security of their service. It is absolutely critical for customers to read this Security Guide and follow the recommendations and best practices.

Overall Goals of Security

There are two main goals to Security System.

1. Preventing unauthorized access consists of the following larger pieces:
    - **Authentication**: is the person or process that is attempting to access the system who they say theyare?
    - **Authorization**: is the person or process allowed to be doing what they are attempting todo?
    - **Data Access**: does the person have the right level of access permissions for what kind of data they canaccess?
    - **Auditing**: is there a way to tell that some aspect of security has beencompromised?

2. Both preventing unauthorized access and keeping the system up and running are vital aspects to consider. Both can be compromised by deliberate acts and accidental failures.
    - Ensuring that the service stays up and running is vitally important, of course, and is therefore an essential part of security. Deliberate attempts to bring a system down are called Denial of Service attacks, and the base components along with the service itself are configured by default to guard against these attacks. Performance problems can also bring a system down, which has the same effect as someone maliciously targeting the system, so this document will on occasion point out ways in which performance can be affected.

Finally, there are security issues that do not fall cleanly into either of these broad categories, but they will be talked about and addressed further in this document.

General Principles

The following principals are fundamental to any software security plan.

Keep Software Up to Date

One of the foundations of good security practice is to keep all software versions and patches up-to date across the technology stack. The Oracle WMS Cloud Service will be updated to include any relevant Oracle Critical Patch Updates (CPUs). Oracle releases these Critical Patch Updates multiple times a year. These CPUs will be applied to customers instances to keep the service as secure as possible. There is nothing a cloud customer needs to do to get these CPU patches. However, a cloud customer needs to make sure these scheduled application updates happen on-time four times a year and they need to test their scenarios when their Test instance is updated.

In addition, it is recommended that clients keep any of their custom applications or external systems that interface with their Oracle WMS Cloud Service patched and up to date with any relevant security patches as well.

Follow the Principal of Least Privilege

The principal of least privilege states that users should be given the least amount of privilege to perform their job responsibilities. Over-ambitious granting of responsibilities, roles, permissions, etc., especially early on in an organization or

during an implementation's life cycle irrespective of the number of people or implementation timelines; can leave an application or cloud services open for abuse. All user access and privileges should be reviewed periodically to determine relevance to current job responsibilities.

Monitor System Activity

System security stands on three pillars: recommended security protocols, proper system configuration, and system monitoring.

- Security protocols - Oracle addresses the good security protocols and the proper system configuration pillars within

  the Oracle WMS Cloud Service.

- Proper system configuration - When interfacing to the service with custom applications and external systems, it is the

  responsibility of the customer to use good security protocols and the proper system configuration.
- System monitoring - Auditing and reviewing audit records address this third requirement and is the responsibility of

  the customer . The Oracle WMS Cloud service has sufficient degree of monitoring capabilities and customers are advised to make use of it as needed.

Keep Up to Date on the Latest Security Information

Oracle continually improves its software and documentation. Check this document regularly for revisions as well as Oracle SaaS Security

Note: For more detailed information about SaaS Security, see *OCI SaaS Security*

Service Components

The **Oracle WMS Cloud Service** is composed of many different applications and components, and these can be used by many different users in a variety of roles. Some of the users will be internal to customer companies, while others could be external. Data can be exchanged between the applications both internally and to customers external systems.

Each access path should be looked at individually and decisions should be made appropriately as to what activity will be permitted or blocked, and how controls will be put in place to enforce those decisions.

"It is crucial to document it, and make sure to keep the documentup-to-date!" Thisreally cannot be stressed enough, if this is a production system, time will be of the essence, and the time needed to pull together the right people to create one on the fly could be critically detrimental.

Production vs. Pre-Production Environment

Test and Stage environments often have data in them that is every bit as important to secure as the real Production data. These systems should be secured as if they were Production systems.

Service Security Features

Security Model Overview

The Oracle WMS Cloud Service provides security for components via the configuration of Users, User Authentication, Authorization/Access Control, and Auditing functionality. The service supports built-in authentication, Single Sign-On (SAML) and OAuth2.0 (Custom Authentication) in an application model. Authorization/Access Control is system supported, and no external support is required or supported.

Companies and Facilities

Every Oracle WMS instance needs setting up of company and facility configuration as a basic requirement. There is a provision in Oracle WMS to keep data separate and secure it in a shared web-based environment as 'Facilities' are kept separate on creation under the same company.

Oracle WMS supports structure where top level companies are segregated at all levels. A crucial requirement to consider about Oracle WMS Cloud Service structure is the creation of at-least one 'top-level parent company and a default facility' for every customer. For creation of a top-level parent company, only the Application Administrator user (APP-ADMIN) has the necessary permissions. The WMS 'Administrator' user role has the eligibility to perform actions without restrictions in Top Level parent companies and default facilities. It is after establishment of these parameters that customers can log into the WMS using the ADMIN user and create other facilities, child companies and different user roles.

Note:

- The Application Administrator user role is not customer accessible and is managed by oracle.
- Multiple parent companies (also known as "tenants") can reside on a single WMS instance.
- The WMS 'Administrator' user role is created by Application Administrator user.

The Oracle WMS Cloud Service also supports 3PL Hierarchy. A 3PL configuration is one in which the companies are divided into parent and child companies. The 3PL operator is the parent and its clients are the child companies. This structure exists in order to help 3PLs view and manage their clients' inventory separately. Depending on the 3PL, the number of facilities under the same Parent Company, views can be managed so that data of each facility is separate and secured. Different user roles in Oracle WMS carry different permission levels to manage the data visibility and usage within and across different facilities and companies in the 3PL hierarchy configured the facility.

The creation of child companies and facilities has two important methods which can only be addressed at the time of creation and cannot be changed later.

Points to review in the 3PL Hierarchy Method:

- While creating a 3PL hierarchy, the 3PL operator typically owns one or more facilities where Oracle WMS activities are managed for multiple child companies across these facilities.
- The parent company is created for the 3PL operator and child companies are created for each company that is operated within these facilities.
- Users are created at the parent company level.
- ADMINSTRATOR role users automatically receive eligibility to all child companies.
- Other user roles need to be explicitly assigned company level eligibility and facility level eligibility to access specific

  company and facility data.

Note: In the browser-based application UI, users can select which specific eligible company and facility they are operating on at any time. While in the Mobile RF application, users can switch between their eligible facilities but not their companies. This is intentional as warehouse workers may not necessarily know which 3PL clients they are working on.

They are still restricted by their eligible companies list. However, users belonging to the parent company will always have parent company eligibility. This does not pose a problem as parent company is a placeholder which means it does not hold any inventory or other configurations. If a user needs to have access to a specific child company, that can be created as a child company.

For the Completely Isolated Child Companies Method, the users and facilities are created at the child company level, so their access is restricted to the specific child company level it has been created under.

General Parameters to consider while setting up the Facility and Company.

Task Description	WMS Module	Overview/Comments
Facility Set Up	Facilities	New facility is required to be created if the company being added is in a new/non- existing Facility in Oracle WMS Cloud.
Add Facility to user	Users	A new created Facility needs to be added to the user profile.
Non-existing Company Set Up	Companies	(Non-existing Company in New or Existing Facility.)
Existing Company Set Up (Existing Company in new or existing Facility)	Facilities	Existing Companies do not need to be re-created but need to be added to the specific facility.

Note: For more details on configuring facilities and companies, refer to the *Implementation Guide.*

Users

Oracle WMS Cloud includes a built-in authentication mechanism where users can be setup with their own user-id and passwords to access the Oracle Warehouse Management (WMS) Web UI and Mobile RF application. In addition, it also supports authenticating users against external identity providers (IDP). It supports multiple authentication mechanisms:

- SAML2 based Single Sign On, or SSO in short - A web-based authentication standard that can be used only to login to the WMS Web UI.
- OAuth2 - Another authentication standard that can be used for the WMS Web UI and Mobile RF.

Note: Application User Password Restrictions

- Password should be at least 6 Characters long.
- Password cannot be all alphabetic or all numeric.
- Please note that there are forbidden characters that cannot be used for any users' passwords. The following "#", "[","]", “!”, “@”, “$” characters cannot be used in passwords for any users. Special characters cannot be used.
- Password will never be used if integrated with external IDP.
- Company level password policy can override ‘user password’ policy.
- ‘User Password’ can be configured within the Oracle Warehouse Management Service Web UI in Company Security Configuration.

The Oracle WMS Cloud Service user record contains numerous attribute fields for defining and controlling users. There are attributes that control authentication capability like Effective Date and Expiration Date. Some of these fields like First Name, Last Name, and Email Addresses are purely informational. There are fields that are set internally from the application after successful login like default printers.

In order to successfully login to the Oracle WMS Cloud Service through Federated Single Sign-On, Single Sign-On (SSO) or OAuth2, you must provide an alternate user on the user record in the Oracle Warehouse Management service. The alternate user is the key field which links a user to the Single Sign-On solution. These logins are also case-sensitive.

Note: Every Oracle Warehouse Management user requires a password within the service. It is recommended to provide a strong password for every user. Although, Oracle WMS Cloud provides a maximum password lifecycle of 365 days, users should change passwords frequently as a best practice. Application Administrators should use their organizations password rotation policy. The created password must be changed and updated once before the password life cycle ends to ensure the account accessibility.

When provisioning users, it is necessary to specify the correct company/facility. By default, users created in one company/facility will only have access to data defined in their own company/facility. The Oracle WMS Cloud service has and requires different user roles that are utilized within the application. Permissions to access data for different user roles are as follows:

Administrator User Role – Permissions

Category	Permissions
Company / Facility	Add, Delete, and Change Company; Add, Delete, and Change Facility;
User	Add, Delete,and Change User

Category	Permissions
Group	Add, Delete, and Change Group
Menu	Modify Menu, Save Company Menu, Save Group Menu
Columns	Modify View Columns, Reorder View Columns
View	Save Company View, Save Group View, Save User View

Note: By default, Administrators have access to all companies that the facility is eligible for.

Management User Role – Permissions

Category	Permissions
Facility	Add, Delete, and Change Facility;
User	Add and Change User
Menu	Modify Menu, Save Group Menu
Columns	Modify View Columns, Reorder View Columns
View	Save Group View, Save User View

Supervisor User Role – Permissions

Category	Permissions
Facility	Change Facility
User	Change User
Menu	Modify Menu, Save Group Menu
Columns	Modify View Columns, Reorder View Columns
View	Save Group View, Save User View

Guard User Role – Permissions

- Read-only access. Users cannot create, copy, edit or delete.

Employee User Role – Permissions

- Read-only access. Users cannot create, copy, edit or delete.

Support User

In some instances, it is necessary to view log files as the Oracle WMS Cloud (WMS) support team is assisting with any existing issues. To initiate this process, customers need to create a support user in WMS. Once a customer creates a support user, the support team will have access to log files and other tools required to analyze customer issues.

> **Note:** The Create Support User option is available only if the customer selects a user that is not currently a support user (refer to support user column). The reason is that the selected user serves as a template for the support user that is about to be created and it cannot be an existing support user's template. As soon as any issues triaged with the support user are resolved, customers can disable the support user. If you do not delete the support user, the system will automatically disable the support user cannot be reactivated at this point life in days is reached, and the support user cannot be reactivated at this point.

Authentication Policy

The Oracle Warehouse Management Service provides the ability to setup different expiration dates for different users by enforcing password life in days. A few of these Account Policy settings are only checked and enforced during an interactive end user login or during web services http Basic Authentication user login. Some of the others Account Policy settings are checked when the user themselves is conducting an Oracle Warehouse Management service password change, or during an administration user maintenance update though the UI.

> **Note:** With Oracle Single Sign-on, most users do not use the password in Oracle Warehouse Management Cloud for authentication. The exception to this is Integration users that are local and built-in users.

Account Policies provide control over password definitions, password renewal rules and login behavior. Account policies allow you to configure the following password rules:

- Password Rules: validation rules for password strength
- User Password Expiration
- Warning period for password expiration
- Duplicate password prevention, including configurable number of historical passwords

User Level Account Policy

The Account Policies provide control over password definition, password renewal rules and login behavior. Account policies allow you to configure the following password rules:

- Password cannot match username
- Password must be at least 6 characters. The password character length can be overridden per company by an ADMIN
  role user.

- Password must have a combination of alphabetic and numeric characters.
- Password should not have too many repeated characters.
- Password cannot be a reverse of the username.
- Password cannot be a portion of the username.
- Username cannot be a portion of the password.
- Use a more complex rather than simple password. Examples of a simple password: using 123, 1234, abc, abcd, admin,

  logfire, or the word “password” as part of the password.)
- Cannot repeat recently used password.

Company Level Account Policy

The company account policy helps manage when the customers password expires via Company level security settings. From Companies, ADMIN users can go to Company Security Configuration to adjust the values as needed. The values and their functionality are described below:

Company Security Configuration Fields:

Field Name	Functionality Description
Minimum Password Life in Days	This field defines the user password life validity for minimum number of days in a year.
Maximum Password Life in Days	This field defines the user password life validity for maximum number of days in a year.
Minimum Password Length	his field defines minimum number of characters used in a user password.
Minimum failed login attempts	This field defines maximum number of logins attempts that weren’t successful before locking the account.
Password History Count	This field defines number of last reused passwords for changing/updating the password.

User Activity and Administrator Role Recommendations

All failed attempts to login to the Oracle Warehouse Management Cloud service are automatically logged as exceptions. User Activity Screen and User Screen captures important actions of the active users after logging in the Oracle Warehouse Management Service Web UI. This user activity is provided for informational purposes. These activities are described in the below tables:

User Activity Screen

This screen shows activity of all the users that belong to the same facility and company.

User Activity Screen

Field Name	Functionality Description
Facility, Company, and Parent Company Code	These fields show the activity of users that belong to respective facility/company and Parent company
Date	This field shows when the users from the specific facility/company have logged in.
Hour	Users from the specific facility/company that have logged in the Oracle Warehouse Management Web UI in the previous hours of the specific date.
Number of Users	Number of users that logged in the Oracle Warehouse Management Web UI from the specific facility/company

Note: Login Activity of the individual users who have logged in the previous hours of the specific date of the same facility/company can be tracked through User Activity > User Activity Detail Console. Individual user's login date and time can be viewed from the 'Create Timestamp' Field in the 'User Activity Detail Console'.

User Screen

This screen will display individual user activities after the user has logged in Oracle Warehouse Management Web UI and the previously changed password activity. Below fields and the functional description of these fields will track the individual user activity:

User Screen:

Field Name	Functionality Description
Modification Timestamp	These fields shows if the created user is still active in the system
Active	This field shows last login time and date
Last Login	The time and date of the modification activity made by/made to this user in the system

User Change History Screen

This screen will display individual actions taken by the user in the Oracle Warehouse Management Web UI. It mainly highlights the modifications made by the user in the Web UI or the modifications made to the user.

User Change History Screen

Field Name	Functionality Description
User	The active user.

Field Name	Functionality Description
Mod User	The user which creates or deletes another user in the system. This user can also update any changes to another user (which will be displayed in the User field).
Action	Add, Delete or Update are the actions taken by the user. User can update different fields and can add or delete another user in the system.
Modification Timestamp	The time and date of the modification activity made by/made to this user in the system
Modification Field	Field that is updated.

Oracle Warehouse Management Administrator Role Recommendations

- It is strongly recommended not to use the Administrator user role for any actual end user performing daily business activity.
- It is strongly recommended to create a dedicated user that does not typically log into the service to run recurring processes
- Every Oracle Warewhouse Management Service user requires a password within the service. It is recommended to provide a strong password for this user.
- Create and use an Account Policy that at the very least has strong basic password requirements.

Oracle Public Cloud Identity Management Users

Oracle Identity Cloud Service (IDCS) Identity Providers

A local user is mandatory in Warehouse Management System to be able to login using Single Sign-On Authentication. And a user record is required in Oracle Identity Cloud Service (IDCS) for interactive end user to log-in to the Oracle Warehouse Management Service. Please refer to the *Single Sign-On (SSO)* section in the Oracle Warehouse Management Cloud SSO and Alternate Authentication Setup Guide for logging in to the Warehouse Management System using SSO.

Oracle Identity Cloud Service (IDCS) and Azure AD/ADFS are Identity Providers that have been tested with Oracle WMS Cloud. Other providers that support these standards may also work. Customers can request their environments to be configured to use SSO and/or Oauth2 by raising a Service Request (SR).

Authentication

Signing in using SSO Authentication

SSO Authentication

SAML2 SSO works a bit differently. The username and password are not entered in the WMS Cloud login page. The user instead clicks the “Login using SSO” button (which will be available after the SSO configuration has been setup by following SR process mentioned earlier). The page gets redirected to the Identity Provider’s login page where the user

will login using their username linked to the IDP (this is stored in the “Alternate username” field in WMS Cloud). If the authentication succeeds, a token is returned to the WMS Cloud and the user is logged in to the application.

> **Note:** SAML2 SSO backends that have been validated against WMS Cloud are Oracle IDCS and Azure AD. Technical Configuration for SSO.

OAuth2 Authentication

OAuth2 Authentication can be accessed by submitting an SR to My Oracle Support (MOS) for the setup. Oauth2 authentication can be used to login via Oracle Cloud WMS web UI or the RF handheld application. RF Handheld application authentication only works using local authentication or Oauth2. Due to technical reasons RF Handheld application cannot use SSO.

Please refer to the *Administering Oracle Cloud Identity Management* (Oracle IDCS reference) to understand the technical details.

Warehouse Management System Configuration for Alternate Authentication

Oracle WMS Cloud allows any user to be external authentication enabled. This has to be done at the individual user level. There is no global flag to enable external authentication for all Oracle WMS Cloud users.

Once the WMS Cloud environment has been setup for SSO or OAuth2 authentication, usernames in WMS Cloud have to be associated with a corresponding username in the external Identity Provider. This is the “Alternate username” field in WMS Cloud and must have the following format: **<username>@<domain>**

WMS Cloud users can be created/configured from the Users screen or by uploading a User Excel file from the Input Interface screen. It is possible to have some WMS users be locally authenticated, and others externally authenticated. It’s possible to have both SSO and OAuth2 backends configured for one customer.

Authentication

For **Single Sign-On Authentication** and **OAuth2 Authentication** see the *SSO and Alternate Authentication Setup Guide*.

Staying Logged into the Service: End User Session Timeout

The Oracle Warehouse Management Cloud service has http session timeouts of 45 minutes for invalidating inactive user sessions. This means that any user after 45 minutes will have to re-authenticate when the session gets timed out, and then try to use a service resource.

Integration User Authentication

REST

Incoming REST API’s support the following authentication methods:

- basic auth (username and password)
- simple token based authentication
- OAuth2 token based authentication (for grant types ROPC and Authorization Code to obtain a token)

  There are also API related permissions to be setup within the WMS that controls the ability to read, modify or delete data. Outgoing REST API’s support only basic auth. Outgoing touch points can also be configured to send the payload to external SFTP or SFTP sites.

HTTP Request

The APIs may utilize the following five HTTP methods in order to provide users with Create-Read-Update-Delete (CRUD) functionality. Note that not all APIs support all methods.

GET: Return a read-only representation of the selected resource(s) in the response body.

HEAD: Read-only check for resource existence and/or modification. Does not return a response body. POST: Create resources or submit data to be processed by a resource operation.

PATCH: Modify existing resource(s).

DELETE: Remove/deactivate existing resource.

Supported Entities

The lgfapi entity module is used to access and modify OCWMS application data. It exposes specific methodologies for identifying subsets of data and obtaining their representations as well as allowing for the creation of certain resources. The entities supported and corresponding functionality will continue to be expanded through subsequent releases.

The entity module has a documenting feature that can be accessed via a GET request to the top-level (root) URL (.../lgfapi/v10/entity/). This will return a sorted list of supported entities for the given lgfapi version and an accompanying base URL.

Each entity represents an object or combination of objects within OCWMS that is accessible via lgfapi. However, not all entities support all HTTP methods. Furthermore, these entities may share characteristics with their respective counterparts in other areas of the OCWMS application, but as a whole should be considered independent of other application functionality.

Application Permissions

Making a request to lgfapi not only requires user authorization, but also one or more of the CRUD application-level permission to access the supported HTTP methods. These are configurable in the user's group-level permissions.

"lgfapi_read_access" – GET, HEAD

"lgfapi_create_access" – POST

"lgfapi_update_access" – PATCH

"lgfapi_delete_access" – DELETE

> **Note:** this access is also required in order to run resource operations.

It is recommended to create dedicated user(s) with appropriate lgfapi permissions and different facility/company eligibility to protect the integrity of data. For instance, it is safe to give users read access but may not be appropriate to grant them permission to create or modify data.

The legacy API permission, "can_run_ws_stage_interface", has been replaced by the new permission, "lgfapi_update_access". This permission now applies to both lgfapi and the legacy APIs. For legacy API's, this is the singular permission required to access all APIs. For lgfapi, this is one of several new permissions used to control user access.

Please refer to the *Rest API Guide* for more details.

Authorization/Access Control

Authorization Overview

User Profiles

Task Description	WMS Module	Overview/Comments
Add Profiles for new Users	Users	Users created at the 3PL Parent Company will have visibility across all companies in the specific facilities they have access to. Users created at the customer company level will only have visibility and access to that customer company.
Add Facility-Company to New and Existing Users	Users	New users will be created with a default facility. Additional facilities can be added to users.

Default User Roles

User Role	Description	Required
ADMINISTRATOR	Super User. One administrator is provided as part of provisioning.	Yes
MANAGEMENT	Management User role has few edit permissions in facility, user, menu and columns section of the Oracle WMS UI	Optional
SUPERVISOR	Supervisor User role has change permissions for facility & user while has modify permissions for menu and columns section of the Oracle WMS UI	Optional
GUARD	Guard User role has read only access in the Oracle WMS UI	Optional
EMPLOYEE	Employee User role has read only access in the Oracle WMS UI	Optional

Note: Management, Supervisor, Guard and Employee User roles are optional. These roles can be added with the adequate permissions as per the customer need basis. Administrator User role is required for all the creating, editing, and modifying permissions in the Oracle WMS UI.

Access Control Lists/Functional Security

Oracle Cloud WMS allows Super Users to grant/revoke functional access to business processes. A detailed list of these ACL/Functional Security Overview is available in the appendix.

Hardware Access

See the *Technical Requirements Guide* for Network Requirements and for various Hardware devices used to access the Oracle Warehouse Management (WMS) application or devices that are accessed by the application. Customers IT department is responsible for setting up and configuring the hardware devices for access.

User Access

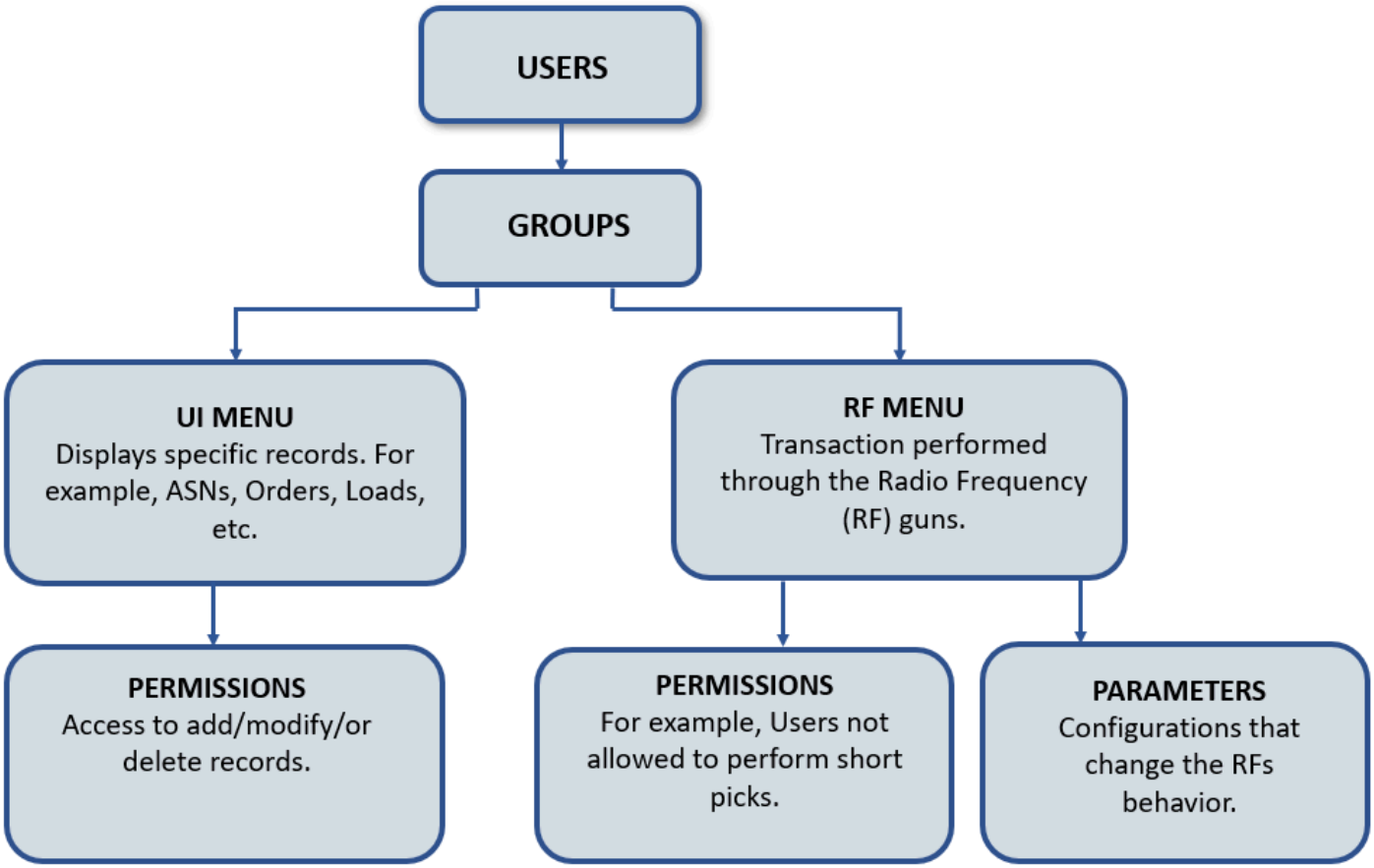
Users are configured at the company level and are granted access to one or more facilities. One facility/company will be the default for every user. Users belong to one of the pre-defined roles and can belong to one or more groups. The pre-defined roles are roles like Administrator, Management, Supervisor, or Employee.

Groups are logical entities that contain permissions and menu. 'Permissions' can be defined as access privileges or rules that enable/disable a specific feature in the application and 'Menu' is nothing but grouping of the screens. A group can have multiple permissions enabled under it.

Some roles have pre-defined permissions automatically granted. An Administrator has access to any permission available in the system without being explicitly granted it. An Administrator will also have automatic access to all child companies. A Management role user has some limited permissions for facility-level entities. Other roles only have read access to the screens that they are given access to. Any additional permissions must be granted by assigning them to a group to which those permissions have been granted.

Most users should be assigned to the role Employee and then added to specific groups with specific permissions they need to use to perform their job. This ensures that no one has more access than is needed to perform their job. The role of Administrator should be limited to only those that need access to everything.

When a User is assigned to a Group, the accessibility control for that user is created by the predefined group permissions and menu access privileges for specific screens. Check the diagram below to understand the User Accessibility flow:



Note: If we set up the menus and groups at the Parent company level, Assigning Groups to the child company User will not be impacted (i.e., the system will show default group Screens.)

Group Permissions

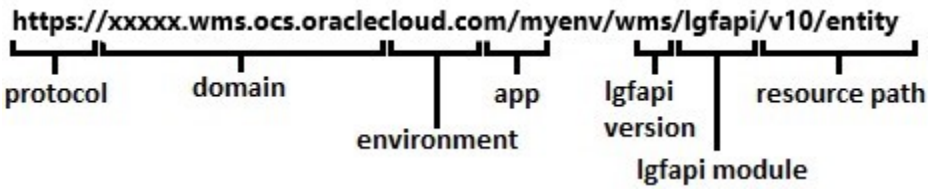
Group Permissions allow you to access privileges or rules that enable/disable a specific feature in the WMS Web UI. Customers can define User accessibility group permissions. See the Group Permissions document for more details.

Note: To find the latest Group Permissions document, from the *Info Center*, click the Documentation tab -> then **Current Documentation**. .

Auditing

LGFAPI - URI Format

The lgfapi URI structure is broken down into several components. In general, lgfapi URIs is using the following schema:



The first portion of the URI (protocol, domain, environment, and app) is consistent with the URL of the environment's UI accessed via a web browser. The remaining pieces after "lgfapi" are specific to the lgfapi and designate the version and path to any child modules and/or resources.

Versioning

Lgfapi requires a version number in all URIs. The format is "v#', starting with "v9" as the first release. New versions are created only for major releases of the Oracle WMS Cloud application, not for minor versions. For example, the release of WMS 9.0.0 included the lgfapi v9 release, but there will not be a new lgfapi version number with the release of WMS 9.0.1. However, the APIs will continue to be updated with new features and improvements along with the minor releases of WMS.

The purpose of version control is to give customers some ability to remain on their current integrations until they can complete any changes required to handle the newest lgfapi version. It is strongly encouraged that all customers use the latest version of lgfapi. Version control is a tool to assist with upgrades and testing, it is not meant to be used in production for extended periods of time. The previous versions of lgfapi will unavoidably become out of sync with newer versions of WMS, and eventually will no longer be compatible.

Oracle will not make changes to previous versions of lgfapi to maintain expired functionality or compatibility. Therefore, it is always in the best interest to use the latest version. New API versions are planned approximately once a year. Older API versions will be supported approximately one year after a newer one is released.

lgfapi Modules

Lgfapi contains modules that can be utilized by customers. These are groupings of functionality that may have their own formats and requirements.

For example, lgfapi's "entity" module is designed to allow customers to examine and interact with OCWMS business resources from outside the application.

Resource Path : The final component to the URI is the resource path. This may take many different forms depending on the HTTP method and any module-specific requirements.

Optional Trailing Slashes: A trailing slash at the end of and lgfapi URIs is optional and does not affect functionality.

LGFAPI - Resource Result Set Filtering

Lgfapi offers the ability to apply filters to GET and HEAD requests to narrow down the final result set. This is done by adding query string filter parameters to the URI. Furthermore, lgfapi supports several built-in lookup functions to assist in common filtering tasks.

It is important to note that all entity data is automatically filtered by the user's eligible facilities and companies. This prevents users from being able to access and/or change data outside of their assigned scope that same way that data is isolated in the UI or RF features. The difference with lgfapi is that users may access data from multiple eligible facilities and companies in a single request. In the UI and RF, this typically requires manually changing the user's context.

- The most basic format for a filter simply uses the exact operator ("="): .../?field=value
- This can be chained to apply multiple filters: .../?field1=value1&field2=value2

Lgfapi uses double underscore (“ ”) notation to join multiple fields or functions in the query string filters. The double underscore is used to distinguish the field names when filtering on a related resource’s attributes or when applying a lookup function.

- Applying a lookup function: .../?field lookup=value
- Filtering on a related resource: .../?relation_id related_field=value
- Applying a lookup function on a related resource: .../?relation_id related_field lookup=value

Please refer to the *Rest API Guide* for more information.

Framework Log

Framework Log Screen provides User Authentication Logs. Framework Log module can be added as a screen that provides information about the user login / logout events with details where possible like client IP address (UI Application only). Mobile RF Application logs the authentication events / user session timeouts with time stamp.

Framework Log Screen

Field Name	Functionality Description
Company and Facility	These fields show the activity of users that belong to respective facility/company.
Module	This field shows when the users from the specific facility/company have logged in or logged out.
Key	Users from the specific facility/company that have logged in the Oracle Warehouse Management Web UI.
Description	This field updates about the successful or failed attempts to logins. ‘Automatic Logout’ log when the application is idle. And the ‘Client IP’ address (only when using web application)
Create Timestamp	Time and date of the login attempted.

Inventory History

Inventory history records are for various WMS transactions taking place in the facility for purposes of informing the ERP or any other external system that may be interested.

For more information about the Inventory History UI fields, see the Interface Specifications Formats document. To find the latest Interace Specifications document, from the *Info Center*, click the Documentation tab - then**Latest Documentation**.

Note: Not all columns will be included in each IHT record.

2 Secure Configuration

Secure Configuration Overview

As explained in the Service Security Features Chapter, the Oracle Warehouse Management Cloud Service has many different administrator user accessible security configuration mechanisms to configure the service for users accessing the service. This section outlines the secure configurations and describes several recommendations.

There is never a one size fits all secure configuration for all the Oracle Warehouse Management Cloud Service customers. However, there are definitely general recommendations and general Dos and Don'ts that can be given. Failure to follow these recommendations may lead to bad configurations, unintended access, data access, and performance issues or data corruption.

User Roles Recommendations

- Usecaution in giving out the ADMIN user role to individual users. This is an elevated user role and has service privileges to everything but reduced domain data visibility.
- Itis recommended to create custom user roles for every role within customers organization so that one can easily control and maintain groups of users' service privileges and data visibility.

User Recommendations

- Do not use commonly known or previously known passwords for the Oracle Warehouse Management Users. Use a strongand unique password by at least utilizing the default BASIC PASSWORD RULES Account Policy.
- Do not use commonly known or previously known passwords for the Oracle Identity Cloud Service (IDCS) Users or external IDPs. Use a strong and uniquepassword.
- Deactivate unneeded Oracle Warehouse ManagementUsers.
- Do not deactivate or delete users who have recurringprocesses.

User Access Recommendations

- Create custom menus for users based on individual roles. These custom Menus should only contain what one want the user tosee.
- Create custom Screen Sets for users based onroles.
- Create custom views for users based onroles

Company Security Configuration Policies (Recommendations)

- Do not set max password length toolong
- Main password length to be set to min of 6characters
- Max field login attempts to be set to a reasonablevalue
- Password history count should be kept atdefault

General Recommendations

- Use caution when granting access to upload files into theservice.
- Use caution when granting access to upload raw data viaCSV.
- Use caution when granting access to use external integrationfunctionality.
- Use caution when granting abilities to define ExternalSystems.
- Disable or delete obsolete and unused External Systems to prevent accidentalusage.

3 Break Glass Support for Environments

Break Glass for Oracle WMS

Break Glass for Oracle WMS provides you with additional security by restricting administrative access to systems and services. When you use Break Glass, Oracle Support representatives can access your cloud environment only after relevant approvals and authorization to troubleshoot any issues that may arise in your cloud environment.

In addition to such controlled access, data at rest is secured using Oracle's Transparent Data Encryption (TDE) and Database Vault. You can control the TDE master encryption key and manage its lifecycle.

Key features:

- Your data in the Oracle Cloud environment is encrypted at rest using TDE, and it is protected and audited using Data Vault.
- Break Glass access is time bound; it secures your data by providing only temporary access to Oracle support personnel.
- Break Glass provides access windows that you can configure; access credentials are programmatically reset after each access.
- Break Glass access is audited, logged, and detailed reports are available.
- You can upload, remove, or restore your TDE master encryption key from the Oracle Cloud Console.

Oracle Managed Access (Break Glass)

Occasionally, Oracle-authorized personnel need to access resources to troubleshoot or help resolve an issue with your applications environment. Break Glass provides you with the ability to temporarily grant access to Oracle Support using a securely administered workflow.

The Break Glass access control and approval workflow is enabled only for specific Oracle Applications bundles, or if you have specifically purchased the subscription. When you subscribe to Oracle Break Glass service, you get access to Oracle Managed Access, where you enable and manage requests for temporary access to your organization's cloud resources from authorized support operators.

Key features of Break Glass with Oracle Managed Access include:

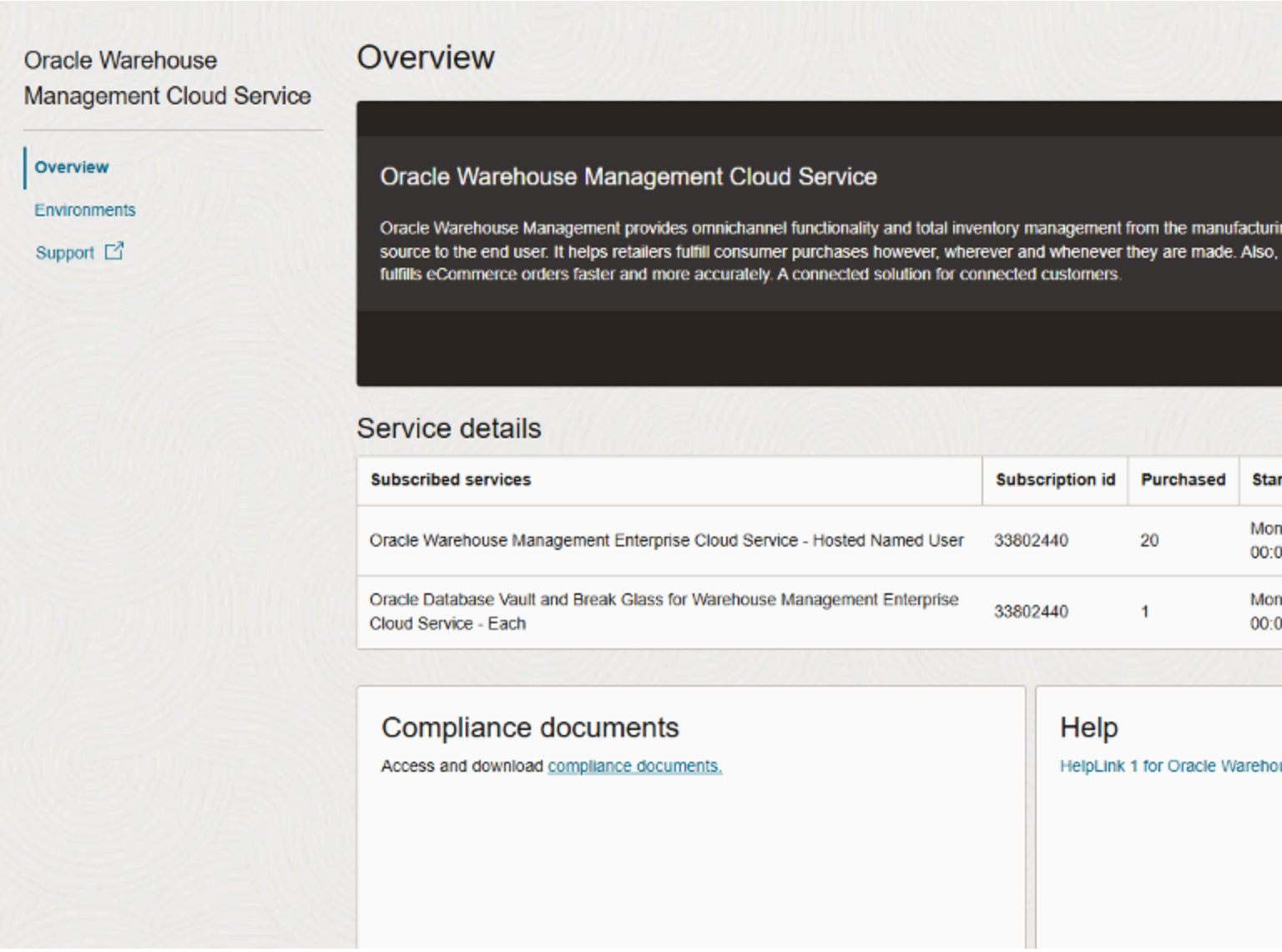
- Provides the operator temporary user credentials for a specific duration.
- Specifies the access level for the representative.
- Creates logs of all actions, providing an audit trail.

This feature allows customers to approve Oracle Administrator access to their cloud environment for analyzing and resolving environment issues.

Prerequisite

- A subscription that includes Break Glass has been added to the environment family.

You can verify that you subscription includes the Break Glass Entitlement on the Overview page for Oracle Warehouse Management.



When you provision an environment that has a break glass subscription included in the subscription, the lockbox is automatically created for the environment in Oracle Managed Access with the following default settings:

- Password expiration time: 96 hours
- Auto-approval: Enabled

Follow the *Managed Access documentation* to setup the lockbox and approvals for your environments.

Customer Managed Keys for Oracle Break Glass

By default, your Warehouse Management environments are protected by Oracle-managed encryption keys. By subscribing to the Oracle Break Glass service, you are offered the customer-managed keys feature that allows you to provide and manage the encryption keys that protect your environments. You can also purchase this option as an add-on subscription.

Warehouse Management leverages the OCI Vault service to enable you to create and manage encryption keys to secure the data stored at rest in your production and non-production environments. You can set up keys on your environment either during environment creation or you can add the key to an existing environment.

For best practices in setting up and managing vaults and keys, click *here*.

IMPORTANT: Production-to-test refreshes where the test environment uses customer-managed keys will also consume key versions. Therefore, frequent P2Ts will reduce the number of remaining key versions more quickly in a vault.

For an overview of setup tasks and roles, click *here*.

Setup Tasks for the Tenancy Administrator

The tenancy administrator performs the tasks to set up the tenancy for the Security Administrator and Applications Administrator to enable and manage customer-managed keys.

1. Create the Security Administrator Group

   It is recommended that you create a distinct Security Administrator group to limit access to the security features of your environments.

   The policy for the Security Administrator group allows the group to manage vaults and keys but does not allow deletion. The policy is:

   ```
   allow group <group-name> to manage keys in tenancy where request.permission not in ('DELETE_KEY')
   allow group <group-name> to manage vaults in tenancy where request.permission not in ('DELETE_VAULT')
   ```

2. Add Permissions for the Applications Administrator

   The Applications administrator needs `read` permissions for vaults and keys. The `read` permission enables the Administrator to:

   - Choose the vault and key during configuration.
   - Verify key rotation.
   - View the vault and keys in the OCI Vault service for troubleshooting.

   To add the permissions for the Applications Administrator:

   a. See the section ***Adding Oracle Cloud Users with Specific Job Functions*** , which describes creating the Applications Administrator role.
   b. Add the following statements to the Applications Administrator role, if not already present:

      ```
      Allow group <your-group-name> to read vaults in tenancy
      Allow group <your-group-name> to read keys in in tenancy
      ```

3. Add the System Policy to Enable Customer-Managed Keys in Your Tenancy

IMPORTANT: This policy must be added before you add the vault and key to your environment. If this policy is not added, your environment will not complete provisioning (if added during environment creation) or will not complete the maintenance cycle (if added to an existing environment).

Create a policy with the following statements:

```
define tenancy saas-ocwms as ocid1.tenancy.oc1..aaaaaaaaloqmqzqpv47kk6afzmxl2njlvstu5cqgeukhjlrutsffjxixk25q
define dynamic-group saas-ocwms-dg as
 ocid1.dynamicgroup.oc1..aaaaaaaammjkmgv2tzdhlt3vcazewcqyyoonatjjhwejs6hfqxpsimvz5i5a
define group Administrators as ocid1.group.oc1..aaaaaaaad6hvivl2kbndzcrn2x6xqarsmzlyout4pm37k6gvhpdcs5ulu47q
admit dynamic-group saas-ocwms-dg of tenancy saas-ocwms to use vaults in tenancy
admit dynamic-group saas-ocwms-dg of tenancy saas-ocwms to use keys in tenancy
admit group Administrators of tenancy saas-ocwms to use vaults in tenancy
admit group Administrators of tenancy saas-ocwms to use keys in tenancy
allow service keymanagementservice to manage vaults in tenancy
```

If you create vaults and keys in multiple compartments, create a policy for each compartment. Alternatively, you can create the policy to allow access to the tenancy, which allows access to all compartments.

Setup Tasks for the Security Administrator

The Security Administrator sets up the vaults and keys and gives the information to the Applications Administrator to add them to the environment.

1. Create Vaults for the Environments

   Follow the procedure *Creating a Vault* in the Vault documentation.
2. Create Keys

   Follow the procedure *Creating a Master Encryption Key* in the Vault documentation.

   You must make the following selections when creating keys for Applications:

   - For **Key Shape: Algorithm**, select **AES (Symmetric key used for Encrypt and Decrypt** (you must select this option for Applications customer-managed keys).
   - For **Key Shape: Length**, select **256 bits**.

   It is recommended you create one key in the production vault for your production environment and one key for each non-production environment in your non-production vault.
3. Give the Vault and Key Information to the Applications Administrator

   After you create the vault and keys give the vault compartment name, vault name, and key name (and key compartment name, if different) to the Applications Administrator.

Setup Tasks for the Applications Administrator

The Applications Administrator adds the customer-managed keys to the environments. This can be performed either during environment creation or after the environment has already been created.

Prerequisites:

- The subscription has been added to the environment family. If the subscription has not been added, you won't see the option to choose customer-managed key.
- The Security Administrator has created the vault and key
- The Tenancy Administrator has set up the system policy to enable customer-managed keys in your tenancy.

- The Tenancy Administrator has created a policy for the Applications Administrator to read vaults and keys and **associate** them to Applications environments.

Replicate Vault

The vault which is created needs to be replicated to the DR region as follows:

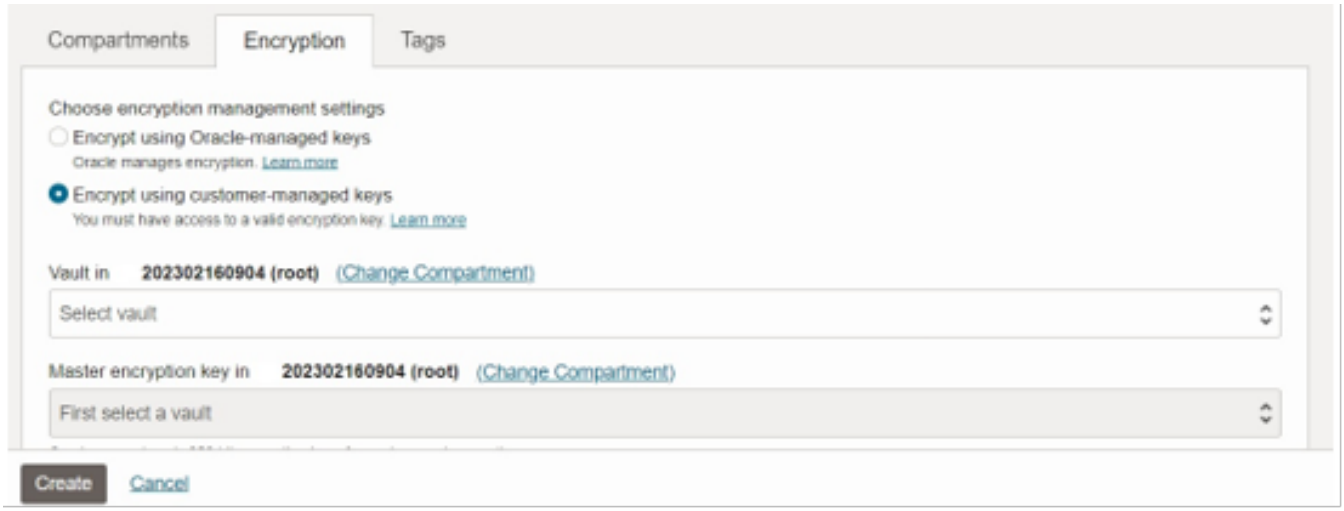
1. Click **Vault**.
2. Click the **Replicate Vault**.
3. View Replication Details and confirm if the vault is replicated.

Adding Customer-Managed Key During Environment Creation

Note: This procedure includes only the steps for enabling the customer-managed key.

On the environment creation page:

1. Click **Show advanced options**.
2. Click the **Encryption** tab.
3. Select **Encrypt using customer-managed keys**.



If you don't see this option, the subscription has not been added to the environment family.

4. Select the **Vault**. If your vault is not in the same compartment that you are creating your environment in, you need to click **Change Compartment** and choose the appropriate compartment.
5. Select the **Key**. If your key is not in the same compartment that you are creating your environment in, you need to click **Change Compartment** and choose the appropriate compartment. Only AES-256-bit keys are displayed.

After you complete all the steps to set up the environment, the provisioning process begins. Adding the customer-managed key adds time to the provisioning process. While the key is being enabled, you'll see a message alerting you that the environment is unavailable.

Adding a Customer-Managed Key for an Existing Environment

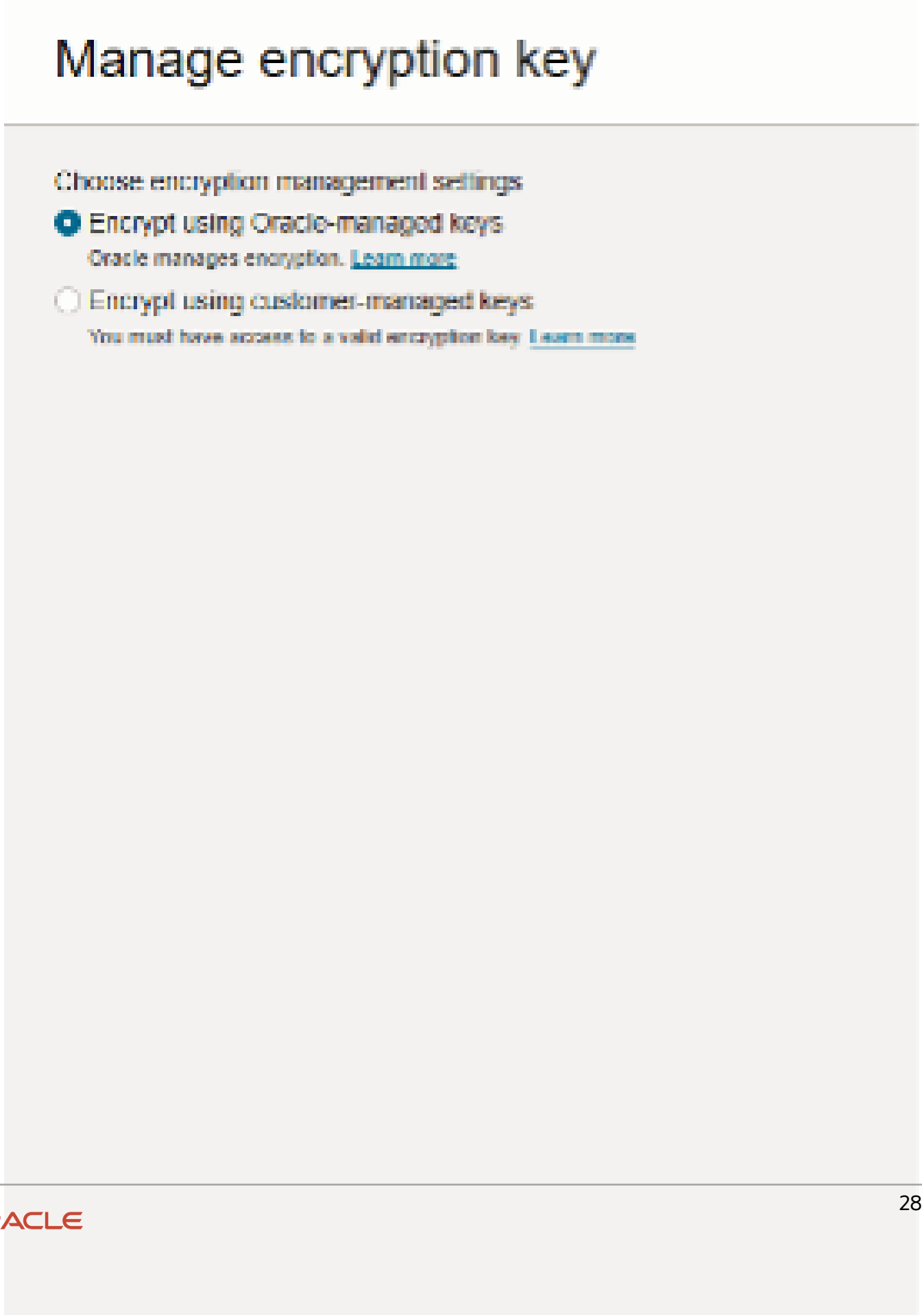
To enable a customer-managed key for an existing environment:

1. Navigate to the environment.

2. On the **Applications tab** of the Console, click **Oracle Warehouse Management**. On the **Environments** menu option, and then click the environment name.
3. On the Environment details page, click the **Encryption** tab.
4. By default, the **Type** is Oracle-managed. Click **Manage** to add your vault and key.

   If you don't see the **Manage** option, either you have not purchased the option, or the subscription for customer-managed keys has not been added to the environment family.

5. Select **Encrypt using customer-managed keys**.


Manage encryption key
Choose encryption management settings
Encrypt using Oracle-managed keys
Oracle manages encryption. Learn more
Encrypt using customer-managed keys
You must have access to a valid encryption key. Learn more

6. Click **Save changes**.

For more info on managing Oracle Cloud Users with specific job functions, click *here*.

Adding a Tenancy Administrator

This procedure describes how to add another user to your tenancy Administrators group. Members of the Administrators group have access to all features and services in the Oracle Cloud Console.

This procedure does not give the user access to sign in to the application service console. To add users to your application, see your application documentation.

To add an administrator:

1. On the Oracle Cloud Console home page, click **Add a user to your tenancy.** The list of Users in the Default domain is displayed.
2. Click **Create user**.
3. Enter the user's **First name** and **Last name**.
4. To have the user log in with their email address:
   - Leave the **Use the email address as the username** check box selected.
   - In the **Username / Email** field, enter the email address for the user account.

   OR

   To have the user log in with their user name:

   - Clear the **Use the email address as the username** check box.
   - In the **Username** field, enter the user name that the user is to use to log in to the Console.
   - In the **Email** field, enter the email address for the user account.
5. Under **Select groups to assign this user to**, select the check box for Administrators.
6. Click **Create**.

A welcome email is sent to the address provided for the new user. The new user can follow the account activation instructions in the email to sign in and start using the tenancy.

For more info on using compartments to group resources for job roles, click *here*.

Add a User with Specified Access for a Job Role

For users that shouldn't have full administrator access, you can create a group that has access to specific applications environments in the Oracle Cloud Console, but can't perform other administrative tasks in the Oracle Cloud Console.

To give users permissions to view your applications environments and subscriptions in the Oracle Cloud Console, you need to:

1. Create a group.
2. Create a policy that grants the group appropriate access to the resources.
3. Create a user and add them to the group.

The following procedures walk you through creating a group, policy, and user. The default administrator can perform these tasks, or another user that has been granted access to administer IAM resources.

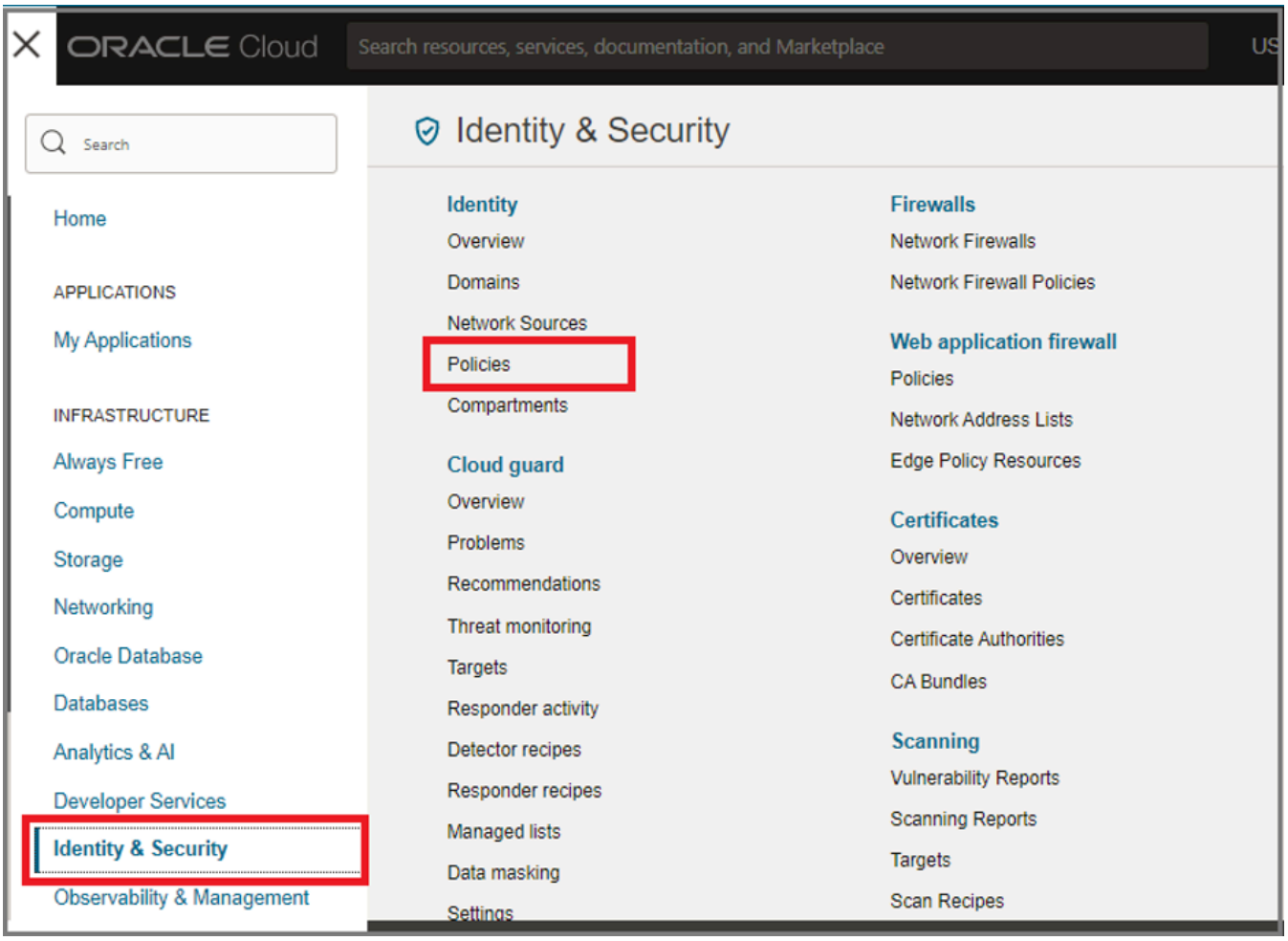
Create a group

1. From the Oracle Cloud Console home page, under **Quick actions**, select **Add a user to your tenancy**. This action takes you to the list of users in the current domain.
2. Under the list of resources on the left, select **Groups**.
3. Select **Create group**.
4. Enter the following:
   - **Name:** A unique name for the group, for example, "environment-viewers". The name must be unique across all groups in your tenancy. You cannot change this later.
   - **Description:** A friendly description. You can change this later if you want to.
   - **Advanced options - Tags:** Optionally, you can apply tags. If you have permissions to create a resource, you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see *Resource Tags*. If you are not sure if you should apply tags, skip this option (you can apply tags later) or ask your administrator.
5. Select **Create**.

Create the policy

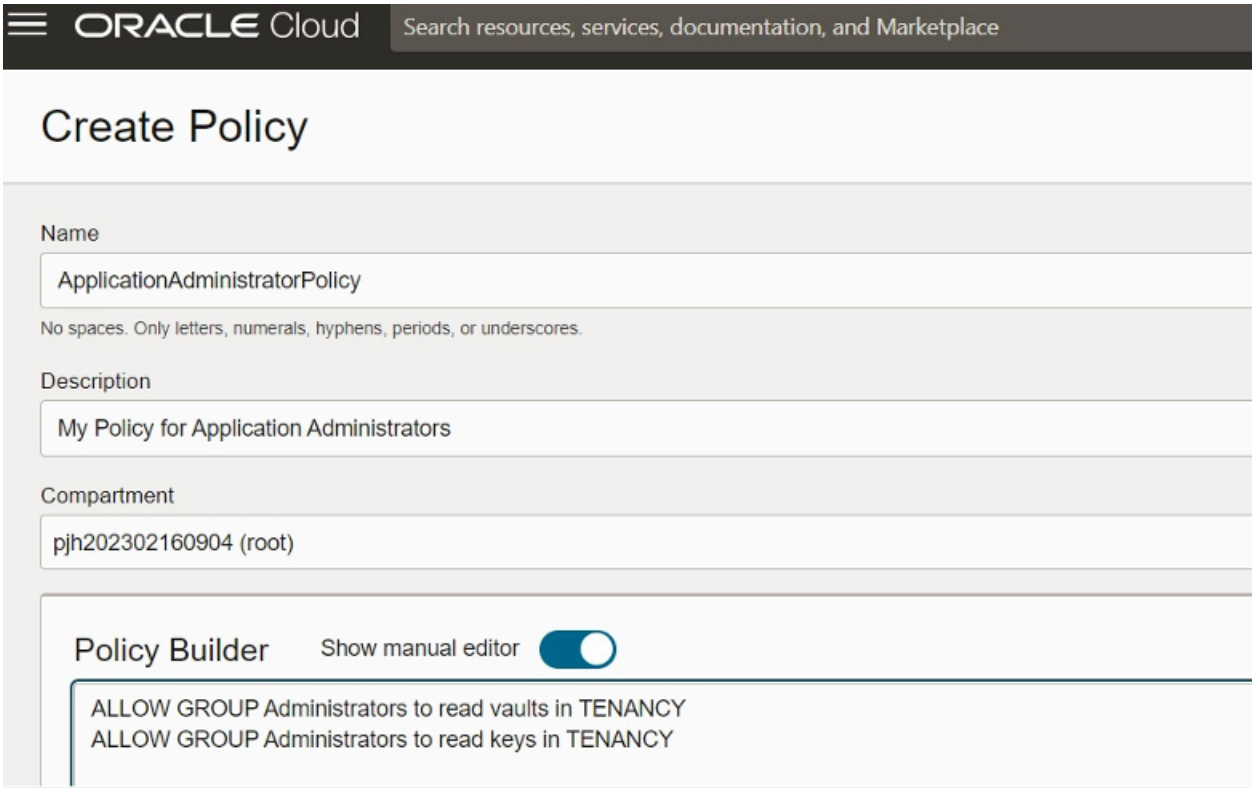
Before you create the policy, you'll need to know the resources you want to grant access to. The resource (or sometimes called *resource-type*) is what the policy grants access to.

1. Navigate to the Policies page of the Default domain:
   - If you are still on the **Groups** page from the preceding step, click **Domains** in the breadcrumb links at the top of the page. On the **Domains** page, click **Policies** on the left side of the page.
   - Otherwise, open the navigation menu, under **Infrastructure**, click **Identity & Security** to expand the menu, and then under **Identity**, click **Policies**. The list of policies is displayed.



2. Click **Create Policy**.
3. Enter the following:
   - **Name:** A unique name for the policy. The name must be unique across all policies in your tenancy. You cannot change this later.
   - **Description:** A friendly description. You can change this later if you want to.
   - **Compartment:** Ensure that the tenancy (root compartment) is selected.
4. On the **Policy Builder**, toggle on **Show manual editor** to display the text box for free-form text entry.

5. Enter the appropriate statements for the resources you want to grant access to.



6. Click **Create**.

Create a user

1. From the Oracle Cloud Console home page, under **Quick Actions**, click **Add a user to your tenancy**.
2. Click **Create User**.
3. Enter the user's **First name** and **Last name**.
4. To have the user log in with their email address:
   - Leave the **Use the email address as the username** check box selected.
   - In the **Username / Email** field, enter the email address for the user account.

   OR

   To have the user log in with their user name:

   - Clear the **Use the email address as the username** check box.
   - In the **Username** field, enter the user name that the user is to use to log in to the Console.
   - In the **Email** field, enter the email address for the user account.
5. To assign the user to a group, select the check box for each group that you want to assign to the user account.
6. Click **Create**.

4 Security Considerations

Security Considerations

Secure Evaluation or Penetration Test

Do not perform a Security Evaluation or Penetration Test on the Oracle Fusion Warehouse Management Cloud Service. Oracle performs these tests. Please see the following links for more details. Also note that performing certain Security Evaluation or Penetration Tests could lead to an outage of customer's service.

> **Note:** Penetration testing and vulnerability testing is not permitted for Oracle Software as a Service (SaaS) offerings. Please refer to *Oracle Cloud Security Testing Policy* and *FAQs about Cloud Secuirty Testing*

Oracle Warehouse Mobile RF Application

Oracle Warehouse Management Cloud supports a handheld RF (Radio Frequency) device interface to access the Mobile RF terminal-based application.

The Oracle Warehouse Mobile RF Application is an application that is written specifically for handheld devices. The mobile application communicates to the Oracle Warehouse Management Cloud service via the secure SSH protocol.

Best Security Recommended Practices for Mobile RF Devices

This is a general list of recommendations for security practices regarding mobile RF devices that may use the Oracle Warehouse Management Mobile RF Application. It is recommended and it may be very beneficial to determine your own mobile device policy and security recommendations, and ultimately enforce them.

- Require a passcode to unlock the mobile RF device before use with the use of a strongalphanumeric passcode is recommended.
- Mobile RF devices should be configured to lock the screen after the device has been inactive for a set period oftime.
- The mobile RF device being used should not have been jail broken or rooted.
- Be careful of other free mobile applications that may have been downloaded that could be malicious or unsafe.
- In order to avoid frequent session timeouts on Mobile RF application Keep-alive settings on the mobile RF device can

  be changed. It is recommended not to use a large number for Keep-alive sessions that can leave the session alive for hours.

5 Appendix

Group Permissions

Note: Please refer to the Group Permissions document for details. To find the latest Group Permissions document, from the *Info Center*, click the Documentation tab -> then **Current Documentation**. .