

# Oracle Fusion Cloud Transportation and Global Trade Management

---

## **Security Guide**

Release 24A



Oracle Fusion Cloud Transportation and Global Trade Management  
Security Guide

Release 24A

F83469-02

Copyright © 2022, 2023, Oracle and/or its affiliates.

Author: Matt Cook

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

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

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

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

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

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

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

# Contents


<b>Get Help</b>	<b>i</b>
<hr/>	
<b>2 Overview</b>	<b>3</b>
<hr/>	
Preface	3
Shared Security Responsibility	3
Security Evaluation or Penetration Test	3
General Security Principles	4
<b>3 Service Security Features</b>	<b>7</b>
<hr/>	
Security Model Overview	7
Domains	7
<b>4 User Management</b>	<b>9</b>
<hr/>	
Oracle Transportation Management Users	9
Authentication	15
Authorization/Access Control	17
Oracle Identity Cloud Service	29
Data Access Control	38
Auditing	41
Password Storage	43
<b>5 Secure Configuration</b>	<b>45</b>
<hr/>	
Secure Configuration Overview	45
<b>6 Break Glass Support for Environments</b>	<b>49</b>
<hr/>	
Break Glass for Oracle Applications	49
Oracle Managed Access (Break Glass)	49
Customer Managed Keys for Oracle Break Glass	50
<b>7 Security Considerations</b>	<b>53</b>
<hr/>	
Security Evaluation or Penetration Test	53

Modifying Service Security Data	53
Integrating Security Data	54
Troubleshooting User Sign in Problems	55
Content Links Embedded by Email	55
Content Virus Checking	55
Content Use Cases	56
File Content Analysis	57
Further Secure the Inbound HTTP Request External Integration URLs	60
Additional Configuration	61
Oracle Transportation Mobile Web Application	64
Integrating with Other Components	64
Automation Agents	65
<b>8 Appendix: Generic Secure Configuration Checklist</b>	<b>67</b>
Security Checklist	67
<b>9 Appendix: General Properties</b>	<b>69</b>
General Properties	69

# Get Help

There are a number of ways to learn more about your product and interact with Oracle and other users.

## Get Help in the Applications

Use help icons  to access help in the application.

## Get Support

You can get support at [My Oracle Support](#). For accessible support, visit [Oracle Accessibility Learning and Support](#).

## 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, and watch events.

## Learn About Accessibility

For information about Oracle's commitment to accessibility, visit the [Oracle Accessibility Program](#). (if videos) Videos included in this guide are provided as a media alternative for text-based topics also available in this guide.

## 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 [otm-doc\\_us@oracle.com](mailto:otm-doc_us@oracle.com).

Thanks for helping us improve our user assistance!



# 2 Overview

## Preface

This document contains recommendations on how to make your software installation more secure. All of these recommendations should be evaluated carefully and implemented based on your own unique needs and the dictates of your own internal security procedures and guidelines. This guide applies generally to Oracle Transportation Management, Global Trade Management, and Transportation Intelligence/Global Trade Intelligence.

## Terminology

### Terminology

Term	Definition
Machine	The physical (or virtual) server.
Web Tier	The web server (Only Oracle HTTP Server)
Application Tier	The application server (Oracle WebLogic)
Web Tier Instance/Application Tier Instance	A specific instance in the Web or Application Tier
Service	The applications covered by this Guide – Oracle Transportation Management, Global Trade Management, Transportation Intelligence, and Global Trade Intelligence.
Properties	Configurable settings that require modification to the data-driven property set.

## Shared Security Responsibility

The Oracle Transportation 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.

## Security Evaluation or Penetration Test

Do not perform a Security Evaluation or Penetration Test on the Oracle Fusion Transportation 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 actually lead to an outage of your service.

**Note:** Penetration and vulnerability testing is not permitted for Oracle Software as a Service (SaaS) offerings.

- [Oracle Cloud Security Testing Policy](#)
- [Frequently Asked Questions About Cloud Security Testing](#)

## General Security Principles

### Overall Goals of Security

There are two main thrusts to securing your systems: preventing unauthorized access, and keeping the system up and running. Both are important aspects to consider, and both can be compromised by both deliberate acts and accidental failures.

Preventing unauthorized access consists of the following broad pieces:

- **Authentication:** is the person or process that is attempting to access the system who or what they say they are?
- **Authorization:** is the person or process allowed to be doing what they are attempting to do?
- **Data Access:** is the person or process restricted in what data it/they can access?
- **Auditing:** is there a way to tell that some aspect of security has been compromised?

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 as well.

### General Principals

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 Fusion Transportation Management Cloud Service will be updated to include any relevant Oracle Critical Patch Updates (CPUs). Oracle releases these Critical Patch Updates four times a year. The Oracle Fusion Transportation Management Cloud Service has three updates a year. These CPUs will be applied to your instances to keep the service as secure as possible. There is nothing a cloud client needs to do to request these CPU patches. However, a cloud client needs to make sure these scheduled updates happen on-time by preparing to thoroughly 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 Fusion Transportation Management Cloud Service patched and up-to-date with any relevant security patches as well.



## Follow the Principle 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, grants, etc., especially early on in an organization or during an implementation's life cycle when there are few people and work needs to be done quickly; 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: good security protocols, proper system configuration, and system monitoring. Oracle addresses the good security protocols and the proper system configuration pillars in the Oracle Fusion Transportation Management Cloud Service. However, when interfacing to the service with custom applications and external systems, it is the responsibility of the client to use good security protocols and the proper system configuration. Also, auditing and reviewing audit records address this third requirement and is the responsibility of the client. The Oracle Transportation Management service has some degree of monitoring capability. Follow audit advice in this document and regularly monitor audit records.

## 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 the Oracle SaaS Security (<https://www.oracle.com/security/saas-security/>).

## Service Components

The Oracle Fusion Transportation Management 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 your company, while others could be external. Data can be exchanged between the applications both internally and to your 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.

*Whatever you do, make sure to document it, and make sure to keep the document up-to-date!* This really 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 Environments

Test and Development 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.



# 3 Service Security Features

## Security Model Overview

The Oracle Transportation Management service provides security on components through the configuration of Domains, Users, User Authentication, Authorization/Access Control, and Auditing functionality. The service supports several authentication mechanisms such as Federated Single Sign-On Support, Single Sign-On (SSO), HTTP basic authentication, and OAuth2 and depending on the type of service request and type of user. Authorization/Access Control can be configured on individual components and end points based on required access. Further data visibility or record access control can be provided by configuring Oracle Virtual Private Database (VPD) capabilities through the Oracle Transportation Management service. A custom service audit capability is also available for auditing particular activity from within the service.

## Domains

One of the first steps in configuring the Transportation and Global Trade Management Cloud Service is to create a domain. Creating separate Domains allows you to keep data separate and secure in a shared web-based environment. The Domain manager enables administrators to organize and manage the domain structure of their provisioned instances.

There is considerable flexibility in the domain structure; you can configure the service to the particular needs of many types of organizations. Stand alone top-level domains with or without sub-domains, along with a variety of different access grants, can be created depending on the required needs. Deleting Domains requires a service request so carefully plan domains and names prior to actual creation.

You can use domains for many different purposes, e.g. modeling business units within a company. However, at a minimum, a single domain must be created to contain all customer specific data. Data should not be created in the PUBLIC domain unless explicitly instructed to do so by Oracle product documentation.

Domains are created via **Configuration and Administration > Domain Management > Add Domain**. For more details, see the "Add Domain" and "Domain Name Rules" help topics.

All provisioned instances of Oracle Transportation and Global Trade Management Cloud include several included domains that are intended to facilitate different implementations. Each of these domains includes a Domain Administrator user. See the Business Domain ADMIN User section for more information about Business Domain ADMIN users. See the Oracle Transportation Management Service Default Users section about default Domain Admin Users. Remember that every new domain created also creates a Domain ADMIN user which is disabled from login and these users should never be removed from the system.

### Default Domains

Domain	Description	Required	Can Be Deleted
SERVPROV	Domain for service provider users	Yes	No
PUBLIC	Global Data Domain	Yes	No

Domain	Description	Required	Can Be Deleted
DBA	Domain for super user and configuration users	Yes	No
GUEST	Sample Domain	Yes	No
EBS	Domain for sample E-Business Suite (EBS) integration.	No	Yes
E1	Domain for sample JD Edwards Enterprise 1 (E1) integration.	No	Yes
GLOG	Not used.	Yes	No
STAGE	Internal Global Data Domain template	Yes	No
FA	Domain for sample Fusion Application integration.	No	Yes

# 4 User Management

## Oracle Transportation Management Users

New Oracle Transportation and Global Trade Management Cloud user accounts must be provisioned within Oracle Transportation and Global Trade Management Cloud User Manager as well as in the Single Sign-On solution. The Oracle Transportation Management service requires a user record to be defined within the service for a user to be able to perform anything within the service. Every Oracle Transportation Management user also requires a password within the service even though this password may never be used by the end user. When provisioning service users, it is recommended to provide a strong password for this user regardless. This password is required internally within the service but also for possible Inbound Integration use.

**Note: Application User Passwords Restrictions:** Note that there are now longer forbidden characters that cannot be used for any service users' passwords by default. All characters can now be used in passwords for any service users. The ALLOW RESTRICTED PASSWORD CHARACTERS Optional Feature has been promoted and is no longer available.

The Oracle Transportation Management service user record contains numerous attribute fields for the defining and controlling the user. There are attributes which control authentication capability like Effective Date and Expiration Date. Some of these fields like First Name, Last Name and Email Address are purely informational. There are fields that are set internally from the application after successful login like the Last Login Data. And there are specific business use fields like Document Use Profile and Approval Rule Profile. The Account Policy field controls the account Policy assigned to the user.

In order to successfully login to the Oracle Transportation Management Cloud Service through Federated Single Sign-On, Single Sign-On (SSO) or OAuth2, you must provide a Nickname on the user record in the Oracle Transportation Management service. The Nickname is the key field which links a user to the Single Sign-On solution. In the case of an interactive end user, this Nickname field must be mapped to the end user's email address that you will define in the Single Sign-On solution. While for an OAuth 2 user, this Nickname field will be mapped to the Client ID of a configured Confidential Application. These nicknames must be unique per cloud service instance, and this is enforced by a check that is performed during user creation and modification. These nicknames are also case-insensitive so there is no way for two different Oracle Transportation Management service users to have different case nicknames.

**Note:** Every Oracle Transportation Management user requires a password within the service even though this password may never be used by the end user. It is recommended to provide a strong password for every user.

When provisioning users, it is necessary to specify the correct domain. By default, users created in one domain will only have access to PUBLIC data and data defined in their domain.

The User manager is accessed via **Configuration and Administration > User Management > User Manager**. For more details see the "Manage User" help topic.

## Oracle Transportation Management User Manager User Interface

To create or update an Oracle Transportation and Global Trade Management Cloud user via the User Manager screens, perform the following steps:

1. Log in as a **DBA.ADMIN** user as another Admin user of the user's domain.
2. Navigate to **Configuration and Administration > User Management > User Manager**.

3. Using the finders, search for the user needing updating.
4. Click on the user link to edit the user record.
5. Modify what is required.
6. Click on **Finished** to save the user change.

## Oracle Transportation Management Service Default Users

The Oracle Transportation Management service has and requires different default users that are utilized within the application.

### Oracle Transportation Management Service Default Users

User ID	Description	Required	Reserved	Can Be Deleted	Notes
otmSystem	A special user that is used internally by the application.	Yes	Yes	No	Do not change the password, delete or modify this user.
guest	A special user that is used internally by the application.	Yes	Yes	No	Do not change the password, delete or modify this user.
DBA.ADMIN	A super user and the Admin user of the DBA domain.	Yes	Yes	No	Do not delete or modify this user.
SERVPROV.ADMIN	The Admin user of the Service Provider domain.	Yes	Yes	No	Do not delete or modify this user.
GUEST.ADMIN	The Admin user of the Guest domain.	Yes	Yes	No	Do not delete or modify this user.
EBS.ADMIN	The Admin user of the EBS domain.	Yes if EBS domain is required.	Yes		
E1.ADMIN	The Admin user of the E1 domain.	Yes if E1 domain is required.	Yes		
FA.ADMIN	The Admin user of the FA domain.	Yes if FA domain is required.	Yes		

### Reserved Users

The Oracle Transportation Management service protects a set of users from modification or deletion. These users are referred to as **reserved users**. These are protected from changes that would destabilize the service.

**Note:** While the DBA.ADMIN user is given to a client to use since it is the true super user, the service internally does still need the DBA.ADMIN user.

# Oracle Transportation Management Service Automatic User Creation

In the Oracle Transportation Management service there are two post-provisioning automatic user creations that can occur during different circumstances. One of these user creations will occur when a new business domain is created and the other one can be configured to occur when a new service provider is created.

## Business Domain ADMIN User

A new user is created during a new business domain creation and there is no way to disable this user from being created automatically in the service. This ADMIN user is required and will be reserved. This user will have a user ID in the format of `<NEW_DOMAIN_NAME>.ADMIN`. This user will have the ADMIN user role, and this user will be used internally for automation agents and integration transaction processing in that business domain. There are also other assumptions in the service that there is an `<DOMAIN_NAME>.ADMIN` user, which makes this user required. The password for this Business Domain ADMIN user is prompted for during the business Domain creation and it is a required field on the UI. Make sure to use a strong password for this Business Domain ADMIN user during initial Business Domain creation. It is strongly recommended to review any of your existing Business Domain ADMIN users' password(s) immediately and ensure recently updated passwords that are not generally known.

**Note:** The new business domain ADMIN user, by default, is reserved to limit modification. It is not recommended to use this Business Domain ADMIN user for an end user that logs into the service.

## Service Provider User

By default in the Oracle Transportation Management Cloud service, a new Service Provider user is NOT created when a new service provider is created. However, it can be configured to have this user be automatically created when a new service provider is created through the service. If configured, this user ID would be created in the format of `SERVPROV.<CURRENT_DOMAIN>-<NEW_SERVPROV_XID>` and this new service provider user will have the limited SERVPROV user role. This new service provider user will NOT have a default password. In order for this new service provider user to use the service, another user administrator user will need to give this service provider user a password within the Oracle Transportation Management service. It is strongly recommended to immediately review all existing SERVPROV users and ensure strong and recently updated passwords that are not generally known.

This automatic service provider user creation during a new service provider creation can be enabled via the following property :

- `glog.servprov.autoCreateUser=[true|false] (defaults to false)`

**Note:** During this automatic creation, if a user already exists with this user ID that matches the Service Provider user format, then an exception could be raised because there is a potential for an incorrect user association record to be created which would tie the existing user to the service provider.

## Disabling Service Users

Instead of actually deleting Oracle Transportation Management service users, users can be set to become effective and expired on specific dates. This is the preferred recommendation for disabling user accounts. The effective and expiration dates can be set on the User Manager for individual users or via the Manage User Expiration Date Action by a user that has the correct service administration access to do so. Please also note that the actual date of the effective

date is the beginning of the date in the service server time. The actual date of the expiration date is the end of the date in the service server time. If the user log-in is not effective or expired the user will not be able to log into the service. It is also recommended to remember to check that the user that is set to expire is not a contact required in the service and also does not have any scheduled recurring process to run. Any recurring processes with an expired user will fail to run until it is assigned to another user.

Service users can be deleted from the service when the user account is no longer valid. However, before deleting any user, remember that any existing Recurring Processes for that user needs to be assigned to another user. Any recurring processes with a missing user will fail to run if these are not assign to another user. The recurring process will actually be deleted. All records which have a Foreign Key relationship to that user will also have to be reassigned or deleted.

## Manage User Expiration Date Action

The Oracle Transportation Management User Manager's Manage User Expiration Date UI Action can be used to 'Manage the Users' expiration dates' en masse. This action supports multiple User IDs at once. Note that leaving the data field blank will actually null out the database column value.

## User Account Policies

The Oracle Transportation Management service provides the ability to set up different account policies for each individual user. Most of these Account Policy settings are only checked and enforced during an interactive end user login or a REST http Basic Authentication user login. The Account Policy settings are not checked during the other Integration User Authentications. Some of the others Account Policy settings are checked when the user themselves is conducting an Oracle Transportation Management service password change, or during an administration user maintenance update though the UI.

For proper security, users should be defined with an account policy.

Account policies are accessed via **Configuration and Administration > User Management > Account Policy**. For more details, see the "Account Policy" help topic.

The Account Policies provide control over password definition, password renewal rules and login behavior. Account policies allow configurability of 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

The account policy allows you to configure the following login behavior:

- Maximum number of failed login attempts before locking the account
- Lockout Attempts and Duration for Entering Incorrect Passwords
- Login History for auditing purposes
- Dormant Account Locking

Some of the available account policy settings, while they can be configured really no longer make sense in the Oracle Transportation Management cloud service since the service user's password is never actually entered by the end user. For example you can certainly set the Expiration Duration and Number of Passwords for History as desired and during the interactive end user login the user will be prompted to change their Oracle Transportation Management service password and it will be checked against previous passwords. However, this may confuse end users when they have remember a password they never use and have to periodically change it.



However, it is strongly recommended to assign users an account policy that contains basic password rules.

**Note:** With Oracle Single Sign-on, most users do not use the password in Transportation and Global Trade Management Cloud for authentication. The exception to this is Integration users and users that need to create/modify Reports or Analytic Dashboards. Integration and the Oracle Analytics Server and Publisher console applications still use Transportation and Global Trade Management Cloud authentication.

The service currently stages only one Account Policies during service provisioning for your use that's recommended for use. This is the BASIC POLICY account policy. The other account polices that are staged aren't recommended, are deprecated and will be removed in a future version. These are the BASIC PASSWORD RULES, STANDARD, NO DORMANCY, and NO RESTRICTIONS account policies. These staged account policy data records aren't assigned to any reserved user that Oracle Transportation Management service is provisioned with. The account policy field is defaulted to the BASIC POLICY account policy in the User Manager User interface for any user that's being newly created or an existing user is being edited and it doesn't contain an account policy.

### Staged Account Policies

Account Policy	Description
BASIC POLICY	A default account policy that contains updated basic password rules along with the lockout.
BASIC PASSWORD RULES	An account policy that contains only basic password rules that's deprecated and will be removed in a future release.
STANDARD	A standard account policy that contains example settings that is not recommend; is deprecated and will be removed in a future release.
NO DORMANCY	Not recommended for use and is deprecated and will be removed in a future release.
NO RESTRICTIONS	Not recommended for use and is deprecated and will be removed in a future release.

### Account Policy Password Rules

When creating an account policy, password rules should be created to ensure the strength of passwords chosen by user administrators or potentially end users. Every Oracle Transportation Management user requires a password within the service even though this password is not ever used and entered by an interactive end user. It is strongly recommended to ensure a strong password is provided for every user by the use of the Password Rules.

These password rules are defined using a regular expression, thus supporting standard rules (i.e. alphanumeric required) as well as providing the ability to create more complex customer-defined rules which adhere to your corporate standards.

The regular expression is based on standards for the Java Development Kit. Details on the expression patterns can be found at [Java Pattern Regular Expressions](#).

The BASIC POLICY and the BASIC PASSWORD RULES Account Policies contain Account Policy Password Rules that are staged with the service. These password rules are described in the table.

### Staged Account Policy Password Rules

Account Policy	Password Rules	Description
BASIC POLICY	{12,}	Password must have at least 12 characters.

Account Policy	Password Rules	Description
	<p>\p{Alpha}</p> <p>\p{Digit}</p> <p>\p{Lower}</p> <p>\p{Upper}</p> <p>\p{Punct}</p>	<p>Password must contain at least one alphabetic character.</p> <p>Password must contain at least one numeric character.</p> <p>Password must contain at least one lower case character.</p> <p>Password must contain at least one upper case character.</p> <p>Password must contain at least one special character.</p>
BASIC PASSWORD RULES	<p>.{8,}</p> <p>\p{Alpha}</p> <p>\p{Digit}</p> <p>\p{Lower}</p> <p>\p{Upper}</p>	<p>Password must have at least 8 characters.</p> <p>Password must contain at least one alphabetic character.</p> <p>Password must contain at least one numeric character.</p> <p>Password must contain at least one lower case character.</p> <p>Password must contain at least one upper case character.</p>

## Oracle Transportation Management User Login History

All failed attempts to login to the Transportation and Global Trade Management Cloud service are automatically logged as exceptions. While the Keep Login History flag can be enabled on any custom Account Policy, the Transportation and Global Trade Management Cloud service will record all end user interactive login attempts (successful or failed) regardless of the setting. The history can be viewed from within the service using the Login History user interface. These successful or failed Login History records should be visible to any user with the DBA.ADMIN user role.

## Oracle Transportation Management Service User Recommendations

- It is strongly not recommended to use the <Business Domain>.ADMIN user record for any actual end user.
- It is strongly recommended to create a dedicated user that does not typically log into the service to run recurring processes.
- Every Oracle Transportation Management user requires a password within the service even though this password is not ever entered or used by the end user. 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.
- User names cannot end with "ADMIN." Do not give .ADMIN user names a Nickname.

# Authentication

## Interactive End User Authentication

All interactive end user authentication is done through an Oracle Cloud Identity Management service. A valid user record is required in both the Oracle Cloud Identity Management cloud service and the Oracle Transportation Management service. If Federated Single Sign-On is also configured, a valid user record must exist in the external Identity Provider.

### Single Sign-On Authentication

See the User Provisioning section of the Oracle Transportation and Global Trade Management Cloud Getting Started Guide.

### Staying Logged into the Service: End User Session Timeout

The Oracle Transportation and Global Trade Management Cloud service has http session timeouts of 8 hours for invalidating inactive user sessions.

This means that any user after 8 hours must re-authenticate when the session gets timed out, and then they try to use a service resource.

The Oracle Cloud Identity Management cloud service also has a Session Settings capability where the Session Duration is also configured to be 8 hours by default.

## Integration User Authentication

The service has numerous mechanisms for inbound data integrations. These include Web Services, REST, and basic HTTP requests. These integration mechanisms vary on which underlying authentication mechanisms are required or supported.

### Web Service

There are inbound web services capabilities for the Oracle Transportation and Global Trade Management Cloud service. Please see the Oracle Transportation and Global Trade Management Cloud Integration Guide for more details on the configuring web service capabilities.

The web service capabilities adhere to the Web Service Security Specification. This specification is an OASIS standard for defining security related information as part of a SOAP message. See <http://www.oasis-open.org/>. The Username Token Profile is, as the name suggests, a standard way of specifying user credentials i.e. username and password. For inbound web services capabilities, user credentials must be specified in a Username Token when calling Oracle Transportation Management web services and must be transported using HTTPS.

The WS-Security token is passed in the SOAP envelope header. Following is an example of a username token with plain text.

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
```

```
<wsse:Security xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wsswssecurity-secext-1.0.xsd">
<wsse:UsernameToken>
<wsse:Username>[you username]</wsse:Username>
<wsse:Password Type="#PasswordText">[your password]</wsse:Password>
</wsse:UsernameToken>
</wsse:Security>
</env:Header>
<env:Body>
...etc..
</env:Body>
</env:Envelope>"*****"
```

## REST

The Oracle Transportation and Global Trade Management Cloud service has the ability to receive data integrations utilizing REST requests. The URLs used do differ depending on the type of authentication being used. See the Oracle REST API for Transportation and Global Trade Management Cloud and the Oracle Transportation and Global Trade Management Cloud Integration Guide for more details on this capability. Oracle Transportation and Global Trade Management Cloud supports the following authentication options:

- **Single Sign-On:** Any attempt to use an Oracle Transportation and Global Trade Management service REST /logisticsRestApi/resources URI end point will use Single Sign-On Authentication.
- **HTTP Basic Authentication:** Any attempt to use an Oracle Transportation and Global Trade Management service REST /logisticsRestApi/resources-int URI end point will require a HTTP basic authentication authorization header.
- **OAuth2 Authentication:** Using Oracle Transportation and Global Trade Management service REST /logisticsRestApi/resources URI end points with OAuth2.

## HTTP Request with Integration URLs

The Oracle Transportation and Global Trade Management service has the ability to receive data integrations utilizing different HTTP URL requests. Please note that these URLs do differ depending on your cloud deployment generation and the type of authentication being used.

For more specific information about the usage and details about this please refer to the Oracle Transportation and Global Trade Management Cloud Integration Guide.

HTTP Basic Authentication is supported for the following Integration URLs.

### URLs Used for External Inbound Integration

Relative URL	Description
/GC3/glog.integration.servlet.WMServlet	WMServlet is the default URL to be used when sending the Transmission or Message XML.
/GC3/glog.integration.servlet.TransformerServlet	TransformerServlet is used to apply an XSL transformation to an XML to convert it into a valid Transmission XML. Refer to the Transform Inbound XML with XSL section in the Oracle Transportation and Global Trade Management Cloud Integration Guide for additional details.
/GC3/glog.integration.servlet.DirLoadServlet	DirLoad provides a faster option for loading data into the service by bypassing the application server. Refer to the DirLoad Section of the Oracle Transportation and Global Trade Management Cloud Integration Guide for additional details.
/GC3/glog.integration.servlet.DBXMLServlet	Provides the ability to export and import DB XML data.

Relative URL	Description
/GC3/ gtm.integration.itm.servlet.ITMIntegrationS	Receives XML from Oracle Enterprise Business Suite in its format, and converts these into proper Global Transportation Management format using XSL configured for processing.
/GC3/ gtm.integration.aes.servlet.AESFilingRespo	Global Transportation Management files EDI report to Customs via Descartes (External vendor). In return, Customs processes the EDI and prepare an EDI response which is send to this servlet by Descartes. This servlet converts the EDI to proper XML format for processing.
/GC3/ glog.integration.servlet.ExternalSystemServ	Provides testing ability to see data sent to an external system.
/GC3/ glog.integration.servlet.BatchCSVUtilServle	Used for exporting CSV data to a remote host.

OAuth2 Authentication is supported for the following Integration URLs when your deployment is in Gen 2.

### URLs for External Inbound Integration using OAuth2

Relative URL	Description
logisticsXmlApi/Transmission	Transmission should be used when sending a Transmission XML.
logisticsXmlApi/DeviceMessage	DeviceMessage should be used when sending a Device Message XML. Refer to the Mobile Device Communications Chapter of the Oracle Transportation and Global Trade Management Cloud Integration Guide for additional details.
logisticsXmlApi/Transformer	Transformer is used to apply an XSL transformation to an XML to convert it into a valid Transmission XML. Refer to the Transform Inbound XML with XSL section in the Oracle Transportation and Global Trade Management Cloud Integration Guide for additional details.
logisticsXmlApi/DirLoad	DirLoad provides a faster option for loading data into the service by bypassing the application server. Refer to the DirLoad Section of the Oracle Transportation and Global Trade Management Cloud Integration Guide for additional details.
logisticsXmlApi/DBXMLServlet	Provides the ability to export and import DB XML data.
logisticsXmlApi/ITMIntegration	Receives XML from Oracle Enterprise Business Suite in its format, and converts these into proper Global Transportation Management format using XSL configured.
logisticsXmlApi/AESFilingResponse	Global Transportation Management files EDI report to Customs via Descartes (External vendor). In return, Customs processes the EDI and prepare an EDI response which is send to this servlet by Descartes. This servlet converts the EDI to proper XML format for processing.

## Authorization/Access Control

### Authorization Overview

The Oracle Transportation Management service has a custom authorization and access control mechanism for user Role Based Access Control (RBAC) capabilities. The Access Control functionality allows a service administrator to configure and maintain service functionality privileges. These service privileges can then be assigned at a user group level, at an individual user level or both. This user grouping or User Role functionality allows the ability to control different service feature accesses at a higher group level as opposed to just an individual user level.

By configuring Users, User Roles with Access Control Lists (Functional Security), and then configuring User Access capabilities by user and user role will provide the complete authorization for the individual users.

## User Roles

The Oracle Transportation Management service has a User Role concept which allows for a way to configure and group similar users with similar characteristics together. Every user must have a default user role. Being able to define similar user characteristics at a group level instead of at an individual level provides easier security configuration and easier maintenance. These user roles within the service are where most data visibility via a virtual private database (VPD) and authorization capabilities known as functional security are defined and configured for users.

The user roles in the service are non-hierarchical, meaning they cannot build on top of each other and cannot inherit attributes from each other. User roles cannot union attributes from one user role into another. However, individual user roles can be configured so that they are granted to a specific user and other user roles, which then allow users to switch to another role within the service. Again, this switching does not allow the union of user role attributes from one user role into another but allows the user to morph into another role to have different data visibility or service privileges.

User role definitions can be changed while the service is running and these changes should be reflected immediately. However, there is some overhead associated with this and performance issues could occur. It is not recommended to change the user role definitions in production during peak volumes.

User roles allow for the configuration of VPD, User Access Level, grants to other user role and users, and Access Control Lists. User roles allow for the configuration of the data visibility by use of the Oracle Virtual Private Database (VPD) functionality with settings that include the VPD Context ID, the VPD Profile ID, and the VPD Domain Name that would apply to the users with this user role assigned. These VPD settings will be discussed in the section *Virtual Private Database Overview*. The user roles also provide a capability to configure the Security Level that is applicable to the user access concepts that will be discussed in the *User Access* section. The user roles also provide a capability to specify the user role grants and the user grants. The Grantee user role specifies other user roles that will have the ability to use the current user role. The Grantee user specifies individual users that will have the ability to use the current user role. In addition, user roles provide the capability of specifying Access Control Lists (ACL) that will apply to all of the users that are assigned the user role. The following menu item provides the ability to create, view, and modify user roles.

This page is accessed via **Configuration and Administration > User Management > User Role**. For more details see, the "User Role" help topic.

After a user role is added to the system, you can assign it directly to a user as their default user role or assign it to another role as a grant. If you assign multiple roles via grants, a user can switch between each role without logging out and logging back into the system. For example, you may configure many user roles that provide domain level visibility into different sets of data for different companies. Then, you can assign one or more of these roles to a user and the user could switch between the roles as needed without logging in and out. You can also assign multiple roles to a master role and then assign the master role to a user thereby providing that user with visibility in multiple domains of select data. See the Change User Role section for more information.

Service administrators can set the default user role for any individual user during creation or modification of the user. In addition, there is a way to have the default user role for new users specified on the domain itself. This allows any user that is created in that domain to have the default user role specified for that domain automatically. This can be configured through the following Add Domain and Manage Domain menu items.

- **Configuration and Administration > Domain Management > Add Domain**
- **Configuration and Administration > Domain Management > Manage Domain**

## Oracle Transportation Management Default User Roles

The Oracle Transportation Management service stages several user roles by default. Please see the below table for the information and details about these default roles.

### Default Transportation Management User Roles

User Role ID	Description	Required	Reserved	Can Be Deleted	Notes
DBA.ADMIN	Intended for use by service super administrator(s), for full access to data and functionality	Yes	Yes	No	Assigned to user DBA.ADMIN. Data access crosses domains.
SERVPROV.ADMIN	Intended for the administrator(s) of the Service Provider domain to provide Access to service provider users	Yes	Yes	No	Assigned to user SERVPROV.ADMIN. Data access crosses domains.
ADMIN	Intended for use by a service Domain administrator for access to data and functionality.	Yes	Yes	No	Data is limited to the user's domain. Functionality typically includes Domain administration and diagnostics.
INTEGRATION	Intended for use by only an external integration user for limited access to external integration	No	Yes	No	Not assigned to any user by default
DEFAULT	A default User Role not really intended for normal end user for user access to data and functionality	Yes	Yes	No	Not recommended for direct use for end users.
SERVPROV	Intended for Service Provider users for limited access to data and functionality.	Yes	No	No	Data and functionality are limited to those needed by a service provider using Oracle Transportation Management.
OTM-SYSTEM	Special user role intended only for the internal otmSystem user, which has very limited service level privileges.	Yes	Yes	No	Designed only for 'otmSystem' user.
OTM-GUEST	Special user role intended only for internal guest user, which has very limited service level privileges and no data privileges.	Yes	Yes	No	Designed only for 'guest' user.  No data privileges.

User Role ID	Description	Required	Reserved	Can Be Deleted	Notes
USER-ADMINISTRATION	Intended only for users who provide user account provisioning.	No	Yes	No	Will allow user administration related modifications with specific exceptions.
DATAENTRY	Limited access to data	No	Yes	No	Data is limited to the data entered by the current user.  Not assigned to any user by default
EXTERNAL		No	Yes	No	Not assigned to any user by default. May be removed in a future version.

The DBA.ADMIN and SERVPROV.ADMIN user roles are special roles in that they are primarily intended for the DBA.ADMIN and SERVPROV.ADMIN users respectively. The ADMIN user role is intended for the Domain Admin user. The ADMIN user role will automatically be assigned to the Business Domain ADMIN user that is created when creating a new domain in the service. The DEFAULT user role is a default user role that is not really intended for normal end users, but serves more as an example of what could be configured. The SERVPROV user role is intended for use with service provider users. The OTM-SYSTEM user role is intended for use with only the 'otmSystem' user. The OTM-GUEST user role is intended for use only with the 'guest' user. The DATAENTRY and EXTERNAL user roles are not needed by default, but are provided as example user roles that could be modified and used in an implementation. The INTEGRATION user role is not needed and is not assigned to any user by default, but is provided to easily assign external integration user(s) the access control entry points required for inbound external integration.

The USER-ADMINISTRATION user role is intended for use for users who only want user administration capabilities. A user with this user role will have full access through the User Manager, User Role, Account Policy and LoginHistory User Interfaces. This includes any field or grids on these screens. Note that VPD and other data restrictions still will apply. For example, since you have access to the Login History User interface, you will not see all login history records. You will be able to grant this new user role to your user roles or users as you see fit.

Note the following caveats:

- The USER-ADMINISTRATION user role is Reserved. You will only be able to modify the new user role to add User Role Grants and add User Grants.
- The DBA.ADMIN user role and ADMIN user role will still NOT be able to be assigned or granted by this new User Role.
- Any DBA.ADMIN or ADMIN user role user will still not be able to be modified by this new User Role.
- This USER-ADMINISTRATION user role does not have its own limited menu. Therefore, you will need to create and assign a menu through User Access.

**Note:** Do not ever change the DBA.ADMIN user's user role. This will cause issues.

## Reserved User Roles

The service protects a set of user roles from modification or deletion. These roles are referred to as *reserved user roles*. Most of the Oracle Transportation Management service default user roles listed above are reserved user roles.



## Change User Role

The Oracle Transportation Management service has the ability to allow individual end users to temporarily change their current User Role to another one, after logging into the service. These user role options do need to be granted appropriately to the user through the User Role user and role grants. The Oracle Transportation Management service only supports 1 current user role per user at a time. Changing a user role can be done via the “Settings and Action” popup section in the upper right Header section of the application shell of the service which is seen after successful login.

In order to allow users to switch to another role, another user role needs to be configured so that it is granted to specific user(s) and/or to other user role(s). Just note that this switching does not allow the union of user role attributes from one user role into another. Changing the user’s User Role after login is only valid for the duration of that session or until it is manually reset or changed back.

The end user will have the ability to Change their User Role to their default user role, any additional user role(s) that has been granted to their default user role, and any additional user role(s) that have been granted specifically to their user. The end user can only have 1 current user role at a time.

The ability to Switch User Roles adds a layer of complexity and should be avoided unless absolutely necessary. There are some considerations that should be reviewed prior to implement thousands of user roles.

First, if an end user has the ability to switch to a different user role in order to do a business or management application operation don't they have the ability to do this operation regardless? Forcing end users to have 3 additional mouse clicks to perform their work tasks just to gain access to something they have access to, is just overhead on the end user and the application. Instead of very complex switch user role types of workflows, when an end user has the access to do it; just let them do it instead of constantly switching user roles to do it. Plus, the user will have 3 additional clicks to switch their user role back to the default to be able to do their other work. And that is if they remember to switch the user role back prior to getting errors and having to redo what they just did after fixing their user role.

Next, the required setup is more complex and requires more maintenance and testing. When allowing a user to switch to another user role you potentially have to have a different set of ACLs, VPD related settings, menus per user role and other User Access items per user role. You will now have more than 1 user role that you have to maintain for that user or users that you may need to periodically need to review to ensure it is correct. You can also change the Data visibility / business domain of the user by changing user roles by use of the VPD Domain Name which adds even more complexity. Remember, if the user has the ability to switch to a different user role in order to do a business operation they have the ability to do it already.

Consideration needs to be given since a user can only have 1 current user role at a time within the Oracle Transportation Management service. So if there is a Recurring Process or Agents that run as a particular user, then you do not want that user running these processes switching user roles.

While there are no real consequences of frequently switching user roles, please be aware that there is a waste of CPU cycles to process the user role change, increased network traffic for the requests, and annoyance from end users. With 3 mouse clicks to get permissions for end users to do something they are allowed to do will definitely get annoying after a while if frequently switching roles.

Oracle cannot dictate to clients as to what is necessary or unnecessary in regards to requirements on whether or not to use user role switching capabilities. Oracle can only recommend. Every client should use the switching user role functionality for difference reasons and how they see fit. In reality, there are only 4 valid reasons to switch user roles. These are for VPD Data Visibility reasons, testing of another role that is other user default user role, demonstration purposes and the occasional case where the end user really does need those special permissions to go override or change something they don't normally need to. The number one reason for changing user roles though, is for VPD Data Visibility either across Business Domains or across specific business regions or locations. For example, I have a planner who only does Northeast corridor order and shipments. The order and shipments are restrained to regions or locations.

However a bunch of southwest planner called in sick and help is needed there. So temporarily, a client could have the Northeast planner users help by switching their user roles to see those orders and shipments.

**Note:** Instruct End Users to be very careful before and after switching user roles. Plus, instruct them to save all current data changes before changing the user role.

**Note: Warning!** Any user who switches user roles can not be used in a Recurring Process or be used in an Agent. There is only one current user role per user at a time within the Oracle Transportation Management service. Allowing a user who is configured for a Recurring Process or an agent to change their user role can cause unknown issues while in the execution of the process or agent. Instead, you should create these recurring processes/agents to run as a user who does not normally log in or does not change user roles.

## Access Control Lists/Functional Security

Access control is a general security term for grouping application permissions together for the purpose of being granted or denied to a user. This capability is referred to as Authorization, which is the definition of what business functions the user is permitted to perform, after they have been authenticated. The Oracle Transportation Management service has a concept of Access Control Lists (ACL) for authorization. This functionality is also referred to as Functional Security. Within the service, an ACL is a grouping of service specific entry points. These specific entry points include servlets, user interface actions, user interface queries, workflow topics, session beans and the session bean's public methods, Mbeans and Mbean methods, Log IDs, and a miscellaneous group of Other. Please note that the Other is a catch all list which is used by the service for web service, REST, and specific Power Data entry points.

The most important entry points to be concerned about are both of the types of web services, servlets, user interface actions, user interface queries and the log IDs. The Mbeans and Mbean methods entry points are generated, but not currently checked within the service so they should be ignored. Due to the nature of any web application it is necessary to manage access to functionality at a more granular level than what a user sees on a menu, otherwise users would be able to access functions by entering the corresponding URL directly into the web browser. All of the access control entry points for the service are staged with the Oracle Transportation Management service and are grouped by default into numerous ACLs to help clients use these default ACLs to build up their own custom ACLs.

The Access Control Lists within the service are a very configurable way to control security. The Access Control Lists (ACLs) are hierarchical so an ACL can contain specific entry points and/or other ACLs.

**Note:** An ACL cannot contain itself, and the same ACL cannot be added more than once to the same ACL hierarchy.

**Note:** The same ACL can be added more than once through the User / User Role ACL hierarchy. This is redundant, strongly discouraged, and can cause performance overhead.

Within the service, the access control lists are generally user role based, meaning that they are granted or denied at the user role level. This means the permissions that are established or taken away by the ACL would apply to all users that have been assigned the user role. However, individual users can additionally have other ACL granted or denied at the User level. For example, a user with the DEFAULT user role that has the DEFAULT ACL assigned to it could get an additional ACL assigned to them for access to a custom UI action that the rest of the users with the same user role would not have. In addition, the same user with the same user role and ACL could also be denied access to a certain user interface action for shipment manipulation.

Listed below are some important ACLs that need to be understood.

## Important Access Control Lists

Access Control List ID	Description
COMMON	List common entry points that every user will need. This should be a child ACL of another ACL that would be assigned to a user.
everyone	List that contains basic entry points that are required for all users. Do not assign this ACL.
Administration	List of administrator-like entry points
Diagnostics	List of *most application diagnostic entry points
ADMIN	Top Level Parent ACL for all DBA.ADMIN and ADMIN user roles
DEFAULT	Top Level Parent ACL for DEFAULT user role. This is the default list of all ACLs.
OTM_SYSTEM	ACL for only the otmSystem user and OTM-SYSTEM user role.
OTM_GUEST	ACL for only the guest user and OTM-GUEST user role.
Power Data - Update	Child ACL for all generic Power Data entry points for record updating
INTEGRATION	Top Level Parent ACL that contains all the child External Integration ACL for the external Integration entry points. This ACL is intended for use only for the INTEGRATION user role.
External Integration	Child ACL that contains all external Integration entry points. This ACL is intended for use for users and/or user roles other than the INTEGRATION user role that require the ability for external Integration entry points.
StackTrace - View	ACL that controls visibility to see application Stack Traces.
Mobile Application REST	Parent ACL for the Mobile Application RESTful web services
Common Interface Layer	ACL for the Common Interface Layer RESTful web services schema metadata.
USER_ADMINISTRATION	Top Level Parent ACL for only the USER-ADMINISTRATION user role.

The COMMON ACL is the default grouping of entry points. Most of the entry points that exist in the COMMON ACL are needed for just the basic navigation capabilities of the application. When creating a new custom ACL, make sure to include the COMMON ACL as a child ACL if it is not already included in a child ACL of another ACL you have included. For example, if I created a new custom ACL that was called MY\_CUSTOM\_ACL and it included the ADMIN ACL, then COMMON is not required to be included. Yet if MY\_CUSTOM\_ACL only included Shipment – View then COMMON is required.

The ‘everyone’ ACL is another special ACL that needs to be explained. The ‘everyone’ ACL is the ACL which contains specific entry points that every user has and needs access to. The ‘everyone’ ACL does not need to be included as a child ACL in any customer-defined ACL that is created, and may cause exceptions if it is.

The Diagnostics ACL is a grouping of diagnostic and performance monitoring related entry points. For example, the Diagnostics ACL entry points include the Cache and Event Diagnostic servlets. This ACL should only be given to users who need to do diagnostic and performance monitoring.

The Administration ACL contains administration user interfaces and actions. For example, the Administration ACL includes entry points for the properties, scalability topology, and account-related user interfaces. This Administration ACL by default is granted to the ADMIN ACL. The ADMIN ACL is a top level parent ACL that is staged by the service and by default is granted to the DBA.ADMIN and ADMIN user roles that are installed with the service. Care should be given in who is given access to this ACL.

The ADMIN ACL is top level parent ACL and has all of the child ACLs, except for the child ACLs for REST. The ADMIN ACL is granted to the DBA.ADMIN and ADMIN user role that is staged with the product. The ADMIN ACL basically contains access to everything in the service, should only be given to ADMIN type users and never given to individual end service users.

The DEFAULT ACL is another top level parent ACL and has the same child ACLs as the ADMIN ACL, except for the child ACLs of Administration and Diagnostics. The DEFAULT ACL is granted to the DEFAULT user role that is staged with the service. Both the ADMIN and DEFAULT ACLs contain numerous other child ACLs that are groupings of similar functional areas of the service.

The OTM\_SYSTEM ACL is only for the otmSystem user and OTM-SYSTEM user role.

The OTM\_GUEST ACL is only for the guest user and OTM-GUEST user role.

The StackTrace – View ACL is an ACL that should be used as a child ACL. No default user, user role, or top level parent ACL is granted the StackTrace – View ACL by default.

## Oracle Transportation Management Service Entry Points

There are all kinds of different Oracle Transportation Management Service entry points. It is important to understand how to determine what the underlying entry point is for a particular part of service functionality. The next sections will try to describe the format and / or what entry points are available.

### Oracle Transportation Management Service User Interface Action Control

The Oracle Transportation Management Service provides a security entry point for each individual Oracle Transportation Management user interface action. The action entry points is based on their ACTION\_GID of the underlying action.

The User Interface Action Entry Point will be in this format:

- `glog.webservlet.util.QueryResponseServlet.action.<lower case ACTION_GID>`

### Oracle Transportation Management Service Web Service Control

The Oracle Transportation Management Service provides a security entry point for each individual Oracle Transportation Management inbound Integration web service. The web service entry points is based on their web service name.

Oracle Transportation Management Service Web Service Access Control Entry Points:

- CommandService
- AgentService
- DriverService
- GtmRestrictedPartyService
- OrderMovementService
- OrderReleaseService
- SellSideShipmentService
- ShipmentService
- GtmSanctionedTerritoryService
- IntXmlService

- MessageService
- IntGtmXmlService

All of the Oracle Transportation Management Service Web Service Access Control Entry Points are grouped into the child "External Integration" Access Control List by default.

## Oracle Transportation Management Service REST Control

The Oracle Transportation Management Service provides a security entry point for each individual REST API URI in combination with the individual Oracle Transportation Management Service Business Entity. The RESTful Web Service Entry Points are based on their URI path and HTTP Request Method, instead of being based on underlying code classes and classname; as is done with most of the other resources.

Please see the Resource Paths and the All REST Endpoints sections of the REST API for Transportation and Global Trade Management Cloud Guide for more information about determining relative REST API URIs.

The version 2 REST Entry Points will be in this format:

- `/resources/{version}/(Resource URI Path) (SPACE) (DASH) (SPACE) (HTTP Request Method)`

Examples of Version 2 of the Oracle Transportation Management Service Business Entity REST Access Control Entry Points:

- `/resources/{version}/shipments - GET`
- `/resources/{version}/shipments - POST`
- `/resources/{version}/shipments - PATCH`
- `/resources/{version}/shipments - DELETE`

Examples of Oracle Transportation Management Mobile Service REST Access Control Entry Points:

- `/api/shipment/add_event - POST`
- `/api/shipment/tender - POST`
- `/api/shipment - GET`

The version 1 of the REST Entry Points will be in this format:

- `/api/sdo/(Resource URI Path) (SPACE) (DASH) (SPACE) (HTTP Request Method)`

Examples of Deprecated Version 1 of the Oracle Transportation Management Service Business Entity REST Access Control Entry Points:

- `/api/sdo/Shipment - GET`
- `/api/sdo/Shipment - PUT`
- `/api/sdo/Shipment - POST`
- `/api/sdo/Shipment - DELETE`

All of the Mobile Oracle Transportation Management Service REST Access Control Entry Points are grouped into child ACLs of the "Mobile Application REST" Access Control List. The "Common Interface Layer" Access Control List only contains the Oracle Transportation Management Service Business Entity REST API Schema Metadata retrieval related entry points. While each individual REST Oracle Transportation Management Service Business Entity supported, has its own corresponding Access Control List. These REST Oracle Transportation Management Service Business Entity Access Control Lists are not granted to any user role or user by default.

Examples of Oracle Transportation Management Service Business Entity REST Access Control Lists:

- REST - Shipment – View
- REST - Shipment – Update
- REST - Item – View
- REST - Item – Update

### Important Warning!

There are Access Control Lists that must be granted to User, User Roles, or Access Control Lists for any end user to gain access to use these Oracle Transportation Management REST APIs. These Access Control Lists are "Mobile Application REST" and "Common Interface Layer" and numerous other Oracle Transportation Management Business Entity specific ACL ("REST - <BUSINESS ENTITY> – View"). The "Mobile Application REST" ACL is for all of the Mobile related APIs, while the "Common Interface Layer" ACL only contains the Oracle Transportation Management Business Entity REST API Schema Metadata retrieval related entry points. The "REST - <BUSINESS ENTITY> - View" or "REST - <BUSINESS ENTITY> - Update" Access Control Lists will contain the entry points needed for the HTTP Method operations on that specific Oracle Transportation Management Service Business Entity.

Access Control Lists will need to be granted to whatever end users that needs to use these RESTful web services for both Mobile and the Oracle Transportation Management Service Business Entity REST APIs. See below for details.

Regarding the "Mobile Application" ACL APIs:

For any user, user role, or ACL that requires use of the Mobile REST APIs, you will have to add the new 'Mobile Application REST' Access Control List to your user, user role, or ACL hierarchy.

Regarding REST Oracle Transportation Management Service Business Entity Access Control Lists:

For any user, user role, or ACL that requires use of the Oracle Transportation Management Service Business Entity REST APIs, you will have to add the correct "REST - <BUSINESS ENTITY> - View" or "REST - <BUSINESS ENTITY> - Update" Access Control List to your user, user role, or ACL hierarchy.

**Note:** <BUSINESS ENTITY> should be replaced with the actual business entity.

Regarding the "Common Interface Layer" ACL APIs:

Most users will not need the "Common Interface Layer" ACL. If you use a user that uses the default "ADMIN" user role or "ADMIN" ACL and you want to Oracle Transportation Management Service Business Entity REST API Schema, you will be fine for the Common Interface Layer web service APIs. There is nothing for you to do. If you have a customer-defined user role or customer-defined ACL, you will need to add the new "Common Interface Layer" Access Control List to your user role or ACL hierarchy.

### Customer-Defined User Interface Action Control

Customers can control access for customer-defined User Interface actions. The customer-defined actions capabilities include a customer-defined action for a report, a custom action that runs an agent action, a customer-defined action that is set up for a customer-defined RIQ screen and any other configurable action. There is a UI action called "Secure Action" is available from the Action Manager UI. This action should be used to create the required security entry point and to ensure proper Access Control List Role assignment. The required entry point records are created when the "Secure Action" action is ran.

**Note:** This "Secure Action" action can only be run once per customer-defined action created. Any subsequence Access Control List Role assignments will need to be done using the Access Control List Manager.

The new Custom Action Entry Point created will be in this format:

- `glog.webserver.util.QueryResponseServlet.action.<custom_action_gid>`

## Individual Generic Power Data User Interface Control

The Oracle Transportation Management Service provides a security entry point for each individual generic power data edit screen. Currently, there are two access control lists that control all of access to the generic power data screens. These are "Power Data – View" and "Power Data – Update". These ACLs control use of all of the generic power data at a very high level and provide access to all power data screens or no power data screens. This high level is at a generic servlet level that provides the generic capability of power data screens. These generic servlets used for power data are the `glog.webserver.powerdata.GenericManagementServlet` and `glog.webserver.powerdata.GenericSaveServlet`. In addition to the all or nothing option, you could also restrict generic power data via the corresponding UI query security entry point to prevent new records and editing of records. However, there is certain data that end users need to be able to query from the UI in a picklist or dropList and denying access to the query would not have allowed this. This is why there is functional security for each individual generic Power data screen to provide extra granularity of control.

The Generic Power Data Entry Points will be in this format:

- `glog.webserver.powerdata.GenericSaveServlet.powerdata.<(typically) lower_case_table_name>`

List of a few examples:

- `glog.webserver.powerdata.GenericSaveServlet.powerdata.equipment_refnum_qual`
- `glog.webserver.powerdata.GenericSaveServlet.powerdata.s_ship_unit_refnum_qual`
- `glog.webserver.powerdata.GenericSaveServlet.powerdata.sku_cost_type`

All of the individual related generic Power Data entry points are grouped into the "Power Data – Update" access control list.

**Note:** Not every menu item under the default power data menus is a true generic power data UI. True generic power data UIs use `glog.webserver.powerdata.GenericManagementServlet` `glog.webserver.powerdata.GenericSaveServlet`.

## Individual Process Control Topic Control

The Oracle Transportation Management Service provides a security entry point for each individual process control topic screen menu. Access is checked using the entry point format below when actually rendering the process control menu. These menus have the URL format of:

- `glog.webserver.processcontrol.ProcessServlet?[application=<a>]&[userLevel=<u1>]`

There are access entry points records that will have a similar format of `processcontrol.level.<u1>[.<a>]` to match these URLs. If the `<u1>` is missing, then "default" will be assumed.

For each of these new entry points, an access entry point record is added as follows:

1. If the `<a>` is missing, the entry point is assigned to Administration.
2. If `<u1>` is "default", the entry point is assigned to COMMON.
3. Otherwise, the entry point is assigned to Administration.

**Note:** There are also entry points for `processcontrol.level.qa`, `processcontrol.level.devl` and `processcontrol.level.default`.

This Topic access check will occur during the rendering of the topic parameters and not during topic submission. The user will get an access violation (if any), when they click on a process control topic they do not access to.

## User Access

With a web application, it is important to understand that user menu options are NOT a form of security. Users can access particular web pages by directly changing the URL, not just by clicking on the menu. Therefore, in order to truly restrict access it is necessary to define what the service defines as user access.

The Oracle Fusion Cloud Transportation Management and Global Trade Management Service have another security feature referred to as user access. This functionality allows different access configurations of user interface components for end users. The user interface components which can be controlled with this functionality consists of action checks, action executions, action reasons, the Ask Oracle Transportation Management saved query, field screen sets, power actions, report workspaces, saved queries, screen sets, status type filters, user menus, and user preferences.

This page is accessed via **Configuration and Administration > User Configuration > User Access**. For more details see the "User Access" help topic.

The user access security mechanism can be assigned at the domain, user role and user levels. When defining the user access at the user role level, the user access security will affect all individuals that have that user role assigned. When defining the user access at the user level, the user access security will only affect the individual user.

User access and access control lists are separate functionality but are complementary to each other. While the Functional Security manages access to code entry points, access control manages access to the user interface components that are directly exposed to the end user.

The user access configurations inherit access to objects based on a hierarchy. The hierarchy is ranked from the more general setting of domain down to a specific setting of an individual user, level, role, and domain. The following list is the hierarchy from general to most specific:

- Domain
- User Role + Domain
- User Level + Domain
- User Level + User Role + Domain
- User + User Level + User Role + Domain

If there are access conflicts because of different configurations between the hierarchy levels, then the user access specified in the lowest and most specific hierarchy level is used. For example, if user access configurations are made at the User Role level and Domain level, then the user access defined at the user role level takes precedence.

There are also Include and Exclude options for certain user access configuration capabilities. The Include and Exclude functionality provides the ability to grant or deny access. The Include and Exclude functionality are only available for the Ask Oracle Transportation Management saved query, saved query, screen set, and user menu user access configuration types.

The user access configuration changes take effect on next login. So any currently active users that would be affected by the changes would need to log out of the service or have their HTTP session timeout and then log back in for the changes to take effect.

The user access functionality provides the additional capability to prevent user access changes. The administrator could set up user access at a determined level, mark it as final, and then prevent other users from changing it. By enabling the



Prevent Access Changes check box as part of defining the user access records, the administrator prevents other users from having the ability to alter the user access configuration.

## Oracle Identity Cloud Service

Oracle Identity Cloud Service provides the user sign-on for Oracle Cloud Services, including Oracle Transportation and Global Trade Management. Oracle is merging the capabilities of Oracle Identity Cloud Service (IDCS) into the native Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) service. This will enable Oracle Cloud customers with a rich, enterprise-class set of identity and access management (IAM) features for use with OCI, Oracle Cloud applications, and third-party applications. You access the Identity Management Cloud Service using the Oracle Cloud Console, aka Cloud Portal. Refer to the "*Introducing OCI IAM Identity Domains: What customers need to know*" and "*OCI IAM Identity Domains: What OCI IAM customers need to know*" to know document for more details on the forthcoming changes to Oracle Cloud Identity Management.

## Oracle Cloud Console

The Oracle Console, also known as Cloud Portal, is the user interface for managing Oracle Cloud Services. In the past Oracle software and infrastructure services had distinct consoles for managing service instances. Oracle is in the process of transitioning to a single Cloud Console for managing all Oracle Cloud Services. The cloud portal management functionality for Oracle Transportation and Global Trade Management largely remains the same regardless of the version of the console. However, the menu and user interface for the console varies. You can determine which version of the Cloud Portal your service is using by the URL you use to access it.

- Oracle Cloud Classic: <https://myservices-cacct...>

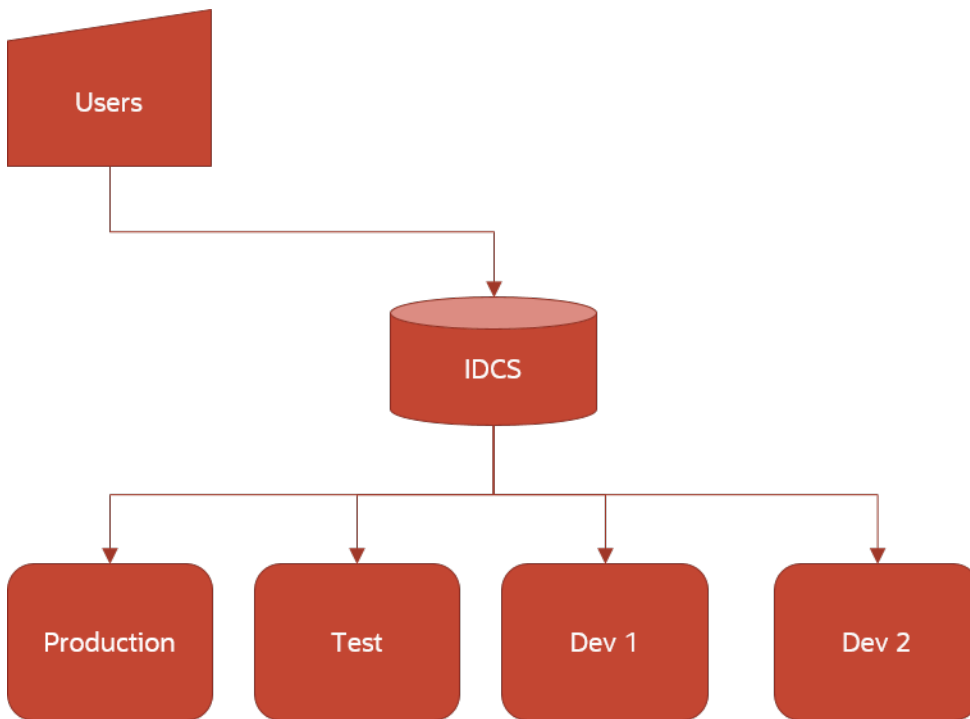
This version of the Cloud Portal is applicable to customers provisioned prior to May 2023.

- Oracle Cloud Console: <https://cloud.oracle.com>

This version of the Cloud Portal is the unified console for all Oracle Cloud Services. Each Oracle Cloud Service is migrated to the new Oracle Cloud Console independently. As of May 2023, new Oracle Transportation and Global Trade Management customers will be provisioned with the new Oracle Cloud console. Migration of existing customers will start shortly thereafter. The version of the Cloud Portal impacts how you manage your users in the Identity Cloud Service.

It is important to understand how the Identity Management service is associated with the Transportation and Global Trade Management Cloud environments. All instances (Production, Test, Dev) are associated with a single Identity Domain (a.k.a Cloud Account). The following diagrams illustrates this configuration.

Default Configuration



## Creating Users in Oracle Single Sign-On

### Creating Users in Single Sign-On: Oracle Cloud Classic

#### Creating Application Administrator Users in Single Sign-On

It is strongly recommended that you provision at least one Application Administrator User in addition to the default one created during service provisioning. In addition to provisioning the new user in the Transportation and Global Trade Management user interface, the user also needs to be provisioned in the Cloud Single Sign-On.

Log into the Oracle My Services Cloud Portal using the URL, Identity Domain and User Credentials provided in your Welcome email.

1. Click on the menu icon in the top left of the screen and select **Users > Identity (Primary)**.
2. Click the **Add** button.
3. Enter the **First Name**, **Last Name**, and **Email Address** for the new user.

**Note:** The email address must match the **Nickname** field on the corresponding Transportation and Global Trade Management User account.

4. Click **Next**.
5. Click the **Add My Roles** button. This will create a user with the same roles that you currently have. These roles provide access to the My Service Cloud Portal and the ability to manage users in the Single Sign-On. The only required roles are listed under Identity Cloud and Transportation Management.
6. Click the **Finish** button. The new user will receive an email containing their default password. They will be prompted to change the password on first login.

## Creating Application Users in Single Sign-On

The following instructions provide the steps needed to provision a new Application User in the Single Sign-On Identity Management Service.

Sign in to the Oracle Cloud Classic using the URL, Identity Domain and User Credentials provided in your Welcome email.

1. Click the menu icon in the top left of the screen and select **Users > Identity (Primary)**.
2. Click the **Identity Console** button on the far right side of the page. This will navigate you to the Identity Cloud Service user interface. You can bookmark this page for future use.
3. Click the **Add** button.
4. Enter the **First Name**, **Last Name**, and **Email Address** for the new user.

**Note:** The email address must match the **Nickname** field on the corresponding Transportation and Global Trade Management Cloud User account.

5. Click the **Finish** button.

**Note:** You don't want to add Application users to any Groups in the Identity Cloud Service other than OTMBI\* named groups.

6. The new user will receive an email containing their default password. They will be prompted to change the password on first sign in.

## Creating Users in Single Sign-On: Oracle Cloud Console

Oracle is in the process of unifying all Oracle Cloud Services into a common management experience. This change does not impact the Transportation and Global Trade Management Cloud service, but it does impact Service Administration and User Administration in the cloud portal. Single Sign-On is still provided by Identity Cloud Service, but the menu has changed. The User Management menu is accessed via the Cloud Portal menu, select **Identity & Security > Identity > Domains**. Select the **"root" Compartment**. Click on the **Default Domain**. Select the Users menu option to add or remove users. To add or revoke a role to/from a user, select **Security > Administrators** on the **Identity Domain** menu. It is important to understand that the Roles and Groups in Identity Management are not relevant for end users of the Oracle Transportation Management and Global Trade Management Cloud Service. Roles for Application Users are administrated with the Oracle Transportation Management and Global Trade Management user interface. Within the Cloud Portal, you can assign User Roles such as Identity Domain Administrator, Security Administrator, or Application Administrator. Refer to the context sensitive online help for the Cloud Portal for more details on these roles and how to assign them. The Identity Administrator can do much more than manage users in the Gen2 Identity Cloud Service. Users that only need to manage other users, should only be assigned the "User Administrator" role.

Outside of the menu navigation changes and the differences mentioned above, the instructions for *"Creating Users in Single Sign-On – Oracle Cloud Classic (OCI Gen2)"* are still applicable.

## Oracle Transportation Management User Synchronization to Oracle Identity Management

The Transportation and Global Trade Management service supports the ability to synchronize users and some user attributes with the users in the Oracle Cloud Identity Management service by defining an External System for the Oracle Cloud Identity and Access Management cloud service. The user data synchronization is only one-way from the Transportation and Global Trade Management service to Oracle Identity and Access Management cloud services. The user synchronization works by matching up the Transportation and Global Trade Management Nickname field to the Oracle Identity and Access Management cloud Service User Name field. The extra user attributes supported for synchronization include first name, last name, and email address. These extra user attributes fields are actually required by Oracle Identity and Access Management cloud service for a user, while these are purely informational in the

Oracle Transportation and Global Trade Management service. There's also an ability to synchronize the users Business Intelligence Roles from Transportation and Global Trade Management Cloud to Oracle Identity Cloud Service groups.

See the [Configuring Oracle Identity Cloud Service User Synchronization](#) topic in the online help for instructions on configuring user synchronization.

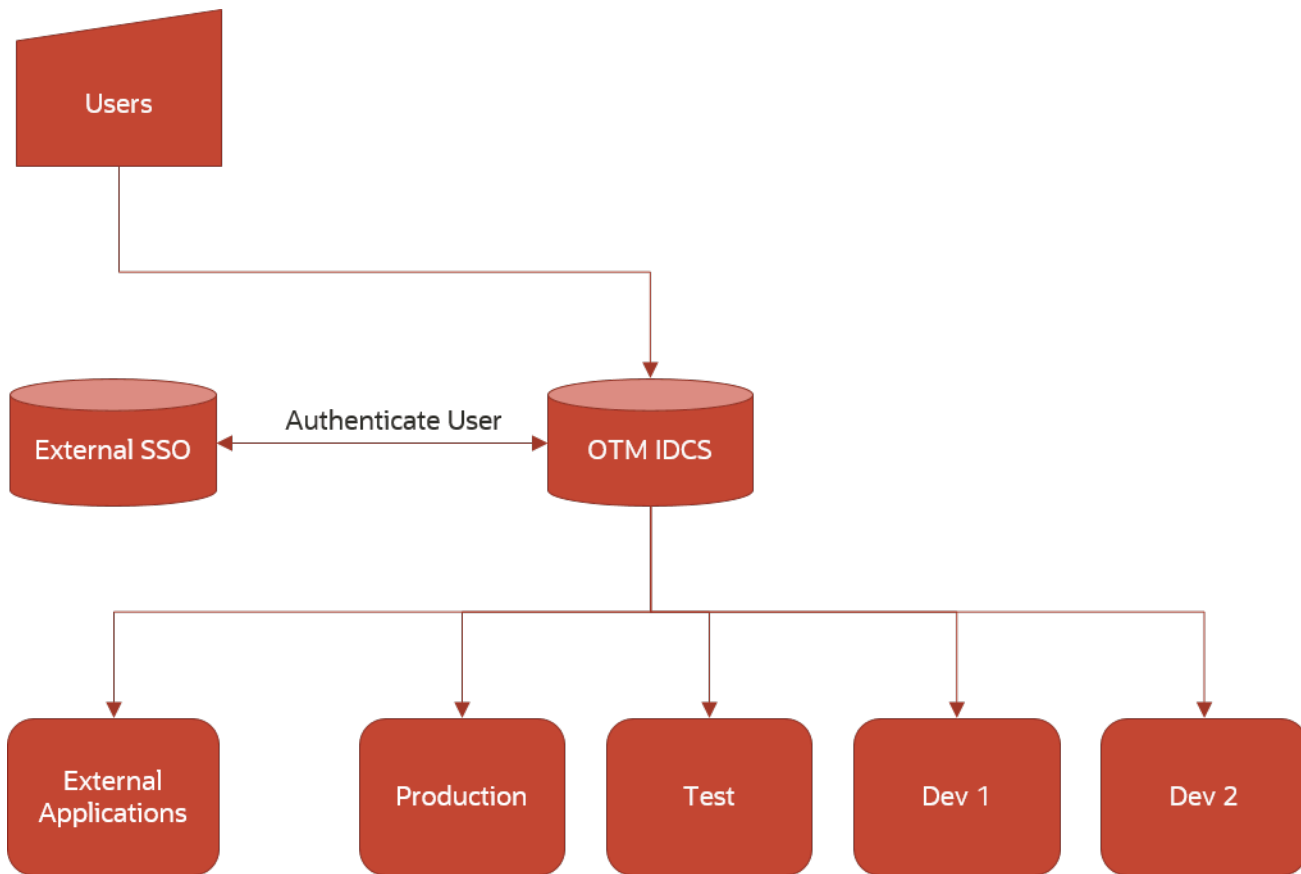
## Federated Single Sign-On

A Federated Single Sign-on (SSO) is a system where your sign-on information is stored in separate identity management systems (IDMs). Identity Federation allows Oracle Identity Management to refer the user authentication to an external Identity Provider.

### Important Identity Cloud Service Terminology

- **Identity Provider:** An identity provider, also known as an "authentication authority", provides external authentication for users who want to sign into Identity Cloud Service using their external provider's credentials.
- **Identity Provider Policy:** An identity provider policy allows identity domain administrators, security administrators, and application administrators to define which identity providers are visible in the Sign In page.
- **Sign-On Policy:** A sign-on policy allows identity domain administrators, security administrators, and application administrators to define criteria that is used to determine whether to allow a user to sign in.

Transportation and Global Trade Management has multiple instances grouped under a single "Cloud Account". Configuration for enabling Federated SSO is done with Identity and Access Management within the Cloud Portal. When the setup is complete, User Authentication will be re-directed from Oracle Identity Management to the External Identity Provider. The following diagram depicts a typical configuration with Federated SSO enabled.



The high level steps to configure the Federated SSO are:

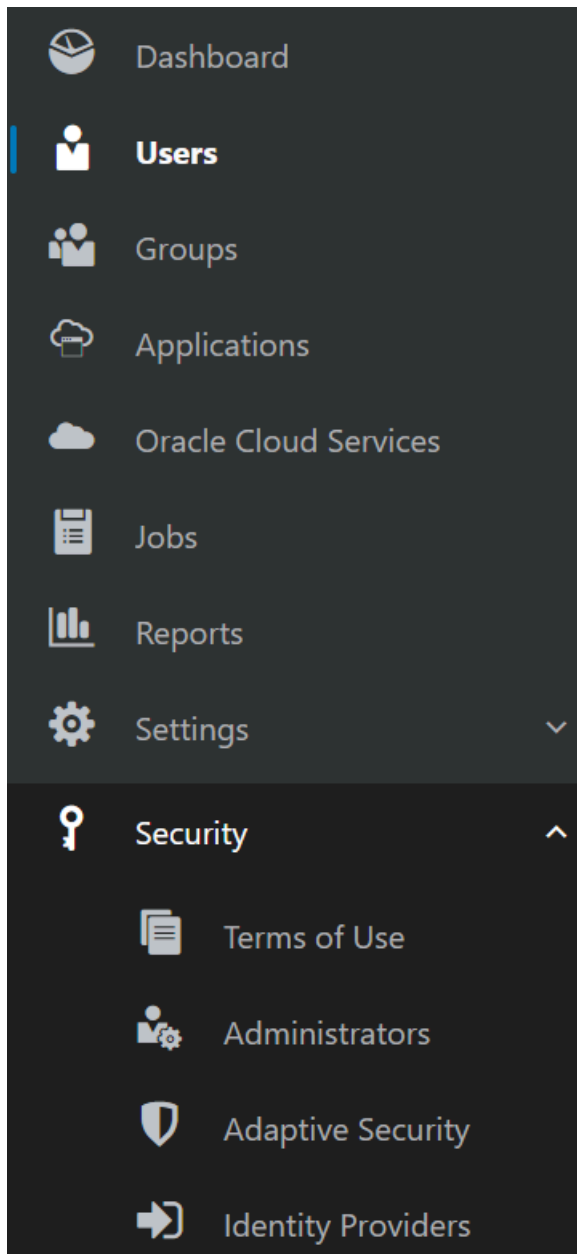
1. Download the Identity Provider (IDP) metadata XML file from your External SSO system.
2. Create an Identity Provider using the metadata XML file.
3. Assign the new Identity Provider to the Default Identity Provider Policy.
4. Assign the new Identity Provider to the Default Sign-On Policy.

The following My Oracle Support Note will help guide you through the process of configuring Federated SSO: "[How to Set Up Federated SSO for OTM on GEN2 \(Doc ID 2932400.1\)](#)".

Federated SSO is configured within the Oracle Cloud Portal. The menu navigation varies depending on the version of the Cloud Portal Associated with your service. Please refer to the "[Oracle Cloud Console](#)" section for more details on how to determine the version of the Cloud Portal.

## Oracle Cloud Classic (OCI)

1. Click on the menu icon in the top left of the screen and select **Users > Identity (Primary)**.
2. Click on the "**Identity Console**" button on the far right side of the screen.
3. Click on the hamburger menu on the top left and you should see a menu like the following. Expanding the "Security" sub-menu will reveal menu options for configuring Identity Providers and Sign-On Policies as shown below.



## Oracle Cloud Console (OCI)

With the new Oracle Cloud Console, Identity Management for Oracle Cloud Services is on the menu option **Identity & Security > Identity > Domains**. Select the "root" Compartment. Click on the "Default" Domain. Clicking on the

“Security” menu option will review menu options for “Identity Providers” and “Sign-On Policies” as shown below.

The screenshot shows the Oracle Cloud interface. At the top, there is a navigation bar with the Oracle Cloud logo and a search bar. Below the navigation bar, the breadcrumb trail reads: Identity > Domains > Default domain > Security > Identity providers. The main heading is "Identity providers (IdP) in Default Domain". On the left, there is a sidebar menu with options: Terms of use, Administrators, Adaptive security, Identity providers (highlighted), IdP policies, Sign-on policies, Network perimeters, App gateways, and Account recovery. The main content area features a dark blue box with the heading "What is an identity provider (IdP)?" and a sub-heading "Set up federated login between an identity domain and external identity provider. The passwords managed by the identity provider. [Learn more](#)". Below this is an information icon (i) in a blue circle, followed by the text "When you configure a SAML IdP, you also must send the identity domain's S". At the bottom of the main content area, there is a button labeled "Add IdP" with a dropdown arrow. Below the button is a table with two columns: "Name" and "Type".

Refer to the [Oracle Identity and Access Management documentation](#) for more details on Identity Providers and Sign-On Policies.

## Customer Identity Provider Policy

ORACLE Identity Cloud Service

# Add Identity Provider Policy

Cancel



Details



Identity Provider Rules



Apps

## Apps

Select All

**+** Assign

**×** Remove



No apps are assigned to this policy.

Assign Apps



## Custom Sign-On Policy

ORACLE Identity Cloud Service

# Add Sign-On Policy

Cancel <

Details Sign-On Rules Apps 3

## Apps

Select All + Assign x Remove

No apps are assigned to this policy.

Assign Apps

## Configuring Custom Identity Providers and Sign-On Policies for Environments

The preferred approach for Oracle Transportation and Global Trade Management is to use the default Provider and Policy as documented in the previous section, which applies to all environments. However, it's possible to configure custom Identity Provider Policies and Sign-On Policies for each environment. This is done by creating new Identity Provider Policies and/or Sign-On Policies and by assigning the corresponding Application on the last step of configuring the policies. There's an Application corresponding to each environment. The name of the application is "OTMGTM\_" followed by the environment name that was specified when creating the environment. A separate Disaster Recovery Application is created for the production environment in the Disaster Recovery region. Customers must also associate this Applications with their custom Identity Provider/Sign-On Policy to ensure business continuity.

**Note:** A new Application is also created for each Environment during Quarterly Updates. It is necessary for the customer to associate this new Application immediately following the Quarterly Update.

## 3-Legged OAuth for Oracle Identity Cloud Service

Oracle Identity Management supports a 3-Legged OAuth flow for web applications. This allows single sign on for web applications integrated with Oracle Transportation and Global Trade Management. Additionally, the application can retrieve an access token on behalf of a user, which can be used to invoke the Oracle Transportation and Global Trade Management Rest API. Since the access tokens are user specific, Oracle Transportation and Global Trade Management data security will apply when invoking the Rest API. For an example of configuring an application with 3-Legged OAuth see the guide for configuring the Logistics Digital Assistant.

## Advanced Configuration

### Identity Domain Management Service

The Identity Domain Management Service provides some advanced capabilities. To access these features, click the **Identity & Security > Domains** menu option in the Cloud Portal. Clicking on the menu icon on the top left corner of the screen and expanding the Security menu option provides access to the following features:

- Identity Providers: also known as Federated Single Sign-On
- Sign-On Policies
- Account Recovery
- MFA: Multi-Factor Authentication

Clicking on the top left corner of the screen and expanding the Settings menu options provides access to the following features:

- Notifications
- Branding

Refer to the Oracle Identity and Access Management documentation for more details on these features.

## Data Access Control

### Virtual Private Database Overview

The Oracle Transportation and Global Trade Management Service utilize the Oracle database functionality of Virtual Private Database or VPD. VPD allows for fine grained row level data security at the database tier layer. In brief, VPD works by dynamically adding a SQL WHERE clause to the SQL statement to provide data security. The dynamic SQL WHERE can be different for all of the different types of SQL statements like SELECT, INSERT, UPDATE, and DELETE.

Within the Oracle database there are different VPD Policy Types which control how the Oracle database actually caches the Policy Predicates. The service rely on all of the VPD Policy Types to be set to SHARED\_CONTEXT\_SENSITIVE in the Oracle database.

The relevant policy type is described here:

## Used VPD Policy Type

VPD Policy Types	Description
SHARED_CONTEXT_SENSITIVE	Executes policy function when the table is first referenced in a database session or whenever local context changes.

The service utilize VPD policies to provide two distinct data visibility capabilities called Domain Grants and External Predicates.

The domain grants capability allows the ability to give access to data in a different business domain. These can be managed through the Domain Grants user interface. By default, the service attach domain grant predicates to every table in a query. Since this domain criteria can have an adverse effect on query performance, the service utilize a capability referred to as “Active Table”. Active table provides the ability to specify which child table policies to use for a given SQL statement.

External predicates provide the ability to attach customer-defined predicates to individual tables. The predicates will automatically be appended to any SQL statement, in addition to domain grant predicates. External predicates are defined in a VPD Profile, which is assigned to a user role. External predicates provide the ability to create customer-defined data security rules (i.e. users can only see orders with a source location associated with them).

A VPD Profile is basically a set of VPD rules. A VPD rule provides the configuration capability to specific fine-grained data access control to a group of users or individual users. This data access control can be across or within Domains. The VPD Profile is then assigned to a user role. The VPD Profile allows for the use of external predicate rules, the use of the insert user rule, and the use of the service provider rule. The Use External Predicate rule enables and disables the external predicates specified in the rules. The Use Insert User rule limits the data access to only the data that the current user entered. This is ideal for a data entry employee who enters data across different domains, and should only be able to view and modify data that was entered by them. The Use of the Service Provider rule limits the data access to only the data where the user is associated to the service provider.

Please be aware that there are service performance implications when utilizing the VPD capabilities of the Oracle database. There is slight overhead in the service when setting up the user context when using a database connection. The dynamic SQL WHERE clauses that gets appended to the SQL statement could also cause additional overhead, and could completely change the execution plan used by the database. Also, depending on the customer-defined predicates and domain grants that are configured within the service there could be additional performance concerns.

## Default VPD Context Variables Attributes

The service define an application context and provide the ability to allow use of context variables to be embedded within external predicates. The default application context that is used in the VPD functionality is `gl_user_ctx`. The default application context of `gl_user_ctx` has attributes that are used to build the standard VPD predicates within the service. A few examples of these attributes are `DOMAIN_NAME`, `FROM_DOMAIN`, `GL_USER_GID`, and `VPD_DOMAIN_NAME`.

There are pre-existing and default VPD Context Variables that are staged with the service for use when configuring external predicates.

### VPD Context Variable Attributes

- `domain_name`
- `gl_user_gid`
- `user_role_gid`

## Default VPD Profiles

There are pre-existing and default VPD Profiles that are staged with the service.

### Default VPD Profiles

Default VPD Profiles	Description
DATAENTRY	Limits data access to only those records in which a user has entered the data. Thus, in effect, users create personalized databases limited to the records they have created.
DBA	Provides data access for the DBA.ADMIN user. All data is visible with this profile, so it should not be used with any other user role other than a DBA user role.
DEFAULT	Provides data access to the entire domain, PUBLIC data, and any other data to which they have been granted access.
OTM-GUEST	Limits data access entirely and is only intended for OTM-GUEST user role.
INVOLVED_PARTY_DOMAIN_VIS	Limits data access to only records for business objects like order base, order release, and shipments in a particular domain in which the user is an involved party in that domain.
INVOLVED_PARTY_USER_VIS	Limits data access to only records for business objects like order base, order release, and shipments in which the user is an involved party.
SERVPROV	This VPD profile should be set for all users who are service providers. It contains the applicable Oracle TI specific external predicates for HD tables that limits data access to only those shipments, rates and capacity usages in which the user is associated with the Service Provider.
FTI_DEFAULT	<p>This VPD Profile is applicable for all Oracle TI users who are not service providers in Oracle Transportation Management. This includes all the external predicates available in the existing DEFAULT Oracle Transportation Management VPD profile and the new external predicates specific to the Oracle TI solution's historical database tables.</p> <p>There are some standard external predicates (specific to TI) applied to each TI table/materialized views that are associated to this VPD profile. Every TI user should be associated to either the FTI_DEFAULT or SERVPROV VPD profile.</p>
GTI_DEFAULT	<p>This includes all the external predicates available in the existing DEFAULT and FTI_DEFAULT Oracle Transportation Management VPD profiles and the new external predicates specific to the Oracle Global Trade Intelligence solution's Historical Database tables.</p> <p>There are some standard external predicates (specific to GTI) applied to each GTI table that are associated to this VPD profile. Every GTI user should be associated to either the GTI_DEFAULT profile.</p>

## Additional Data Access Constraints

For security purposes, there are additional security data access constraints for the following:

- Only users with the "DBA.ADMIN","ADMIN" or "SERVPROV.ADMIN" user roles have rights to create/update/delete on these tables
  - DOMAIN
  - DOMAIN\_GRANTS\_MADE
  - EXTERNAL\_PREDICATE
  - USER\_ROLE
  - USER\_ROLE\_GRANT
  - VPD\_CONTEXT
  - VPD\_CONTEXT\_VARIABLE
  - VPD\_PROFILE
  - ROLE\_ROLE\_GRANT
- Only users with the "DBA.ADMIN","ADMIN" or "SERVPROV.ADMIN" user roles user role have rights to create/update user role grants
- Only users with the "DBA.ADMIN","ADMIN" or "SERVPROV.ADMIN" user role have rights to create/update users to have the "ADMIN" user role.
- Only users with the "DBA.ADMIN" user role as the default user role have rights to create/update users to have the "DBA.ADMIN" user role.
- Users only have rights to modify their own user record, unless the logged in user has the "DBA.ADMIN","ADMIN", "SERVPROV.ADMIN", or the "USER-ADMINISTRATION" user role.
- Only the "ADMIN" user role is allowed for each individual "DOMAIN.ADMIN" user.
- The "SERVPROV.ADMIN" user can have only "SERVPROV.ADMIN" user role.
- Users are blocked from assigning "DBA.ADMIN" role to themselves or others, unless the logged in user already has the "DBA.ADMIN" user role. Non "DBA.ADMIN" users who already have the "DBA.ADMIN" user role are grandfathered in.

## Auditing

### Login

The Oracle Fusion Cloud Transportation Management and Global Trade Management service have the user login auditing functionality enabled by default. This means that every interactive user login will have a record of the login. A login history record to be created and if the user was successfully authenticated, the Last Login Date on the User record will be updated as well.

When you configure a custom account policy for individual users you can also specify to Keep Login history. When this option is enabled, it will also create a login history record and will update the Last Login Date of the user.

The Login History user interface can be used to audit user login attempts. This user interface will be able to show an administrator a user's login attempt, login status, and login time.

- **Configuration and Administration > User Management > Login History**

## Data Auditing

The Oracle Fusion Cloud Transportation Management and Global Trade Management service have a data auditing capability. Many of the service functions can be audited. Ultimately, all business functions act upon business objects that store data in a database table. Within the service you can audit user interface business actions, agent actions, events related to data change, and get actual data change information. The data change information is available for all database columns within the tables that make up a business object. The business object is referred to as a data query type. All of the major entities are data query types. A client can configure by a domain or globally what data query types need to have the audit trail capability. A client can also enforce their users to provide event reasons for running particular user interface actions, which would give the audit information context as to why to the data needed to be changed. There is also the capability to capture the pre-changed and post-change data information.

There is a lot of information that is recorded in an audit record. This information includes the user interface action or agent action, the event reason and associated comments, the time the data modification took place, the business object ID, the table name, the database action taken, and the pre and post data changes. There is minimal service performance overhead associated with utilizing the data auditing capabilities.

You can also control what users have access to audit log data. Typically a service Administrator or domain level Administrator should be responsible for reviewing and/or purging the audit logs. Some audit data is available with just the DEFAULT user role and Audit ACL, but in order to see all audit details, a user would need to also have the Administration ACL. You can review the audit trail records by using the Audit Trail Management user interfaces. These include the Audit Trail Manager, the Audit Trail By User, Audit Trail By Event, and the Audit Trail By Notification managers. There are also application SmartLink user interfaces available on the business entities managers for the Data Query Types that support the audit capability. These SmartLinks are links to the Audit Trail Data just for that particular business object.

The service provide a capability for purging audit trail records. The purging can be done by the data query type or business object. The purging of the audit trail records is not tied to the actually business object's purge. This means that when there is a purge of the business objects, it will not automatically purge the audit trail records. In order to purge the audit trail records an additional purge will need to be scheduled to clean up these related records.

The following property enables additional behavior to compare the before and after values.

- `glog.audit.beforeafter=[on|off]`

## Service Change Control Auditing

The service do not provide any capability for auditing service level changes that are made within the service. Access to Property Servlets, Property Set, Optional Feature and Logic Configuration User Interfaces should be restricted by user role and access control list assignments. In addition it is recommended to have a formal change control process implemented for your organization so that you know when and why something was changed.

# Password Storage

## Third Party Authentication

To interact with third party tools and downstream applications the Oracle Transportation Management service stores passwords in a wallet.

### Oracle Wallet

To securely store third party passwords, Oracle Transportation Management uses Oracle Wallet Manager. This wallet is a container used to store authentication, signing credentials and other secure information. It sits as a flat file outside of the database and service property files, holding encrypted information.

Oracle Transportation and Global Trade Management use a wallet to store passwords for holding customer specified passwords that are used to communicate with external third party tools and systems. These passwords may be modified by users as they only impact communication with one external system.

### Screen Support

The following user interface fields contain third-party passwords:

- Password field on External System
- Password field on Report System
- Password field on Printer
- Password column in Web Service Endpoint list on Web Service
- Password column on Content Management System

When a user enters or modifies one of these passwords, the password value is written to the Oracle Transportation Management Wallet. The database field holds a reference to the wallet key of the form:

`{w<table name>:<primary key>`

where the `{w` prefix denotes an indirect reference to a wallet key. E.g., the password for external system `MYDOMAIN.TEST` would be placed in the Oracle Transportation Management Wallet under key `external_system:MYDOMAIN.TEST`. The corresponding **PASSWORD** column in **EXTERNAL SYSTEM** would hold `{wexternal_system|MYDOMAIN.TEST`.

### Property Support

A number of Oracle Transportation Management properties represent passwords. If a user has rights to edit properties in a property set, he can type them into the Value column of the Property Set screen. This screen knows which properties are passwords, to which wallet each password property belongs, and the corresponding wallet key for that wallet. The password entered by the user is stored in the proper wallet under the proper wallet key. The value stored in the database is a reference to the wallet key.

The following lists properties declared as password. Only users who have the DBA.ADMIN user role can modify these properties.

- `glog.RatingEngine.*.Password`
- `glog.RatingEngine.*.License`

- glog.RatingEngine.\*.Username
- glog.ExternalDistanceEngine.\*.Password
- glog.ExternalDistanceEngine.\*.Account
- glog.ExternalDistanceEngine.\*.Username
- glog.ExternalDistanceEngine.\*.AuthorizationKey
- intelliroute.password
- here.app\_id
- here.app\_code
- alk.api\_key

## Direct Wallet Access

There is no direct wallet access. All changes to the Oracle Transportation Management wallet must be performed via an Oracle Transportation Management screen.



# 5 Secure Configuration

## Secure Configuration Overview

As explained in the Service Security Features Chapter, the Oracle Fusion Transportation 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 of the Oracle Fusion Transportation Management Cloud Service clients however there are definitely general recommendations and general Dos and Do Nots 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

- Use caution in giving out the DBA.ADMIN user role ability to individual users. This is a super user role and has privileges to everything within the service.
- Use caution 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.
- It is not recommended to use the DEFAULT user role since this is a pretty broad service privileged user role.
- It is recommended to create custom user roles for every role within your organization so that you can easily control and maintain groups of users' service privileges and data visibility.
- Do not create a custom "DBA.ADMIN" or "ADMIN" user roles as this will just sidestep built in service constraints. Do this at your own risk.
- Do not modify the "DBA.ADMIN" or "ADMIN" user roles.
- Do not change the DBA.ADMIN user's user role.
- User names cannot end with "ADMIN." Do not give .ADMIN user names a Nickname.

### Users

#### Recommendations

- Do not use commonly known or previously known passwords for the Oracle Transportation Management Users. Use a strong and unique password by at least utilizing the default BASIC PASSWORD RULES Account Policy.
- Do not use commonly known or previously known passwords. Use a strong and unique password.
- Do not share the DBA.ADMIN user account. Instead give individual users the DBA.ADMIN user role as their default role or provide them ability to change to the DBA.ADMIN user role by granting it to their default user role.
- Do not change the DBA.ADMIN user's user role.

- Do not use the <DOMAIN\_NAME>.ADMIN user account(s).
- Expire or delete only unneeded Oracle Transportation Management Users.
- Do not expire or delete users who have recurring processes.
- Only enabled OBIEE Non-SSO User for users who require access to OAS.
- Only grant Business Intelligence Applications and Business Intelligence Roles to users who require it.
- Do not use the External User field as there is no such thing as an external user.

## Access Control Lists (ACL)

### Recommendations

- Do not use assign the same ACL at both the User Role and the User level. As a bad and not recommended example, a user has the DEFAULT user role and then the DEFAULT ACL assign to the individual user. This is redundant and cause performance overhead.
- Create custom ACLs that only contain the entry points required for a given set of business functionality access(es) required.
- Use caution in granting the "ADMIN" ACL since this almost contains every child ACL and allows privileges to everything within the service.
- Use caution in giving out the child "Administration" ACL since this only contains administration entry points.
- Do not create a custom "COMMON" ACL by copying "COMMON". By doing this, you will miss any new child ACLs granted or additional entry points grouped into "COMMON" in future releases. Do this at your own risk.
- Do not modify the "COMMON" ACL.
- Make sure that the "COMMON" ACL is in the hierarchy of child ACLs preferably assigned to the User role.
- Do not grant "ADMIN", "DEFAULT", and "COMMON" ACL directly to the user. This is not needed at all.
- Do not grant the "everyone" ACL.

## User Access

### Recommendations

- Create custom menus for users based on individual roles. These custom Menu should only contain what you want the user to see.
- Create custom Screen Sets for users based on roles. These custom Screen Sets should hide fields and available actions you don't want users to see.
- Create custom Manager Layouts for users based on roles. These custom Manager Layouts should hide fields you don't want users to see.
- When allowing users to change user role that change business domains by use of the VPD Domain, ensure to have equivalent user access records in the domain being changed to.

## VPD

### Recommendations

- Create custom VPD Profiles to be assigned to the custom user roles you defined.

- Use External Predicate Rules and create External Predicates to restrict data.
- It is recommended to block every table that is not required with a predicate that will never be true like (1=2).
- Do not modify the DBA and OTM-GUEST VPD Profiles.
- Take precaution in creating External Predicates to restrict data visibility when a certain join or condition may not exist prior to business actions completing.

## Account Policies

### Recommendations

- Use the default "BASIC PASSWORD RULES" Account Policy for users or create an even stronger custom account policy based on the default password rules. This will ensure a strong Oracle Transportation Management user password.
- Do not use the "NO RESTRICTIONS" Account Policy.
- It is strongly recommended not to use the "NO DORMANCY" Account Policy.
- Do not modify the default Account Policies.

## General

### Recommendations

- "Menu Security" is not security; it is obfuscation at best. While most interactive end users will not stray outside of URL menu links presented, users could potentially still gain access if they know the service resource URLs.
- Use caution when granting access to use SQL Execution Interface tool.
- Use caution when granting access to upload files into the service.
- Use caution when granting access to upload raw data via CSV or DB.XML.
- Use caution when granting access to use external integration functionality.
- Use caution when granting abilities to define External Systems
- Disable or delete obsolete and unused External Systems to prevent accidental usage.



# 6 Break Glass Support for Environments

## Break Glass for Oracle Applications

Break Glass for Oracle Applications 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.

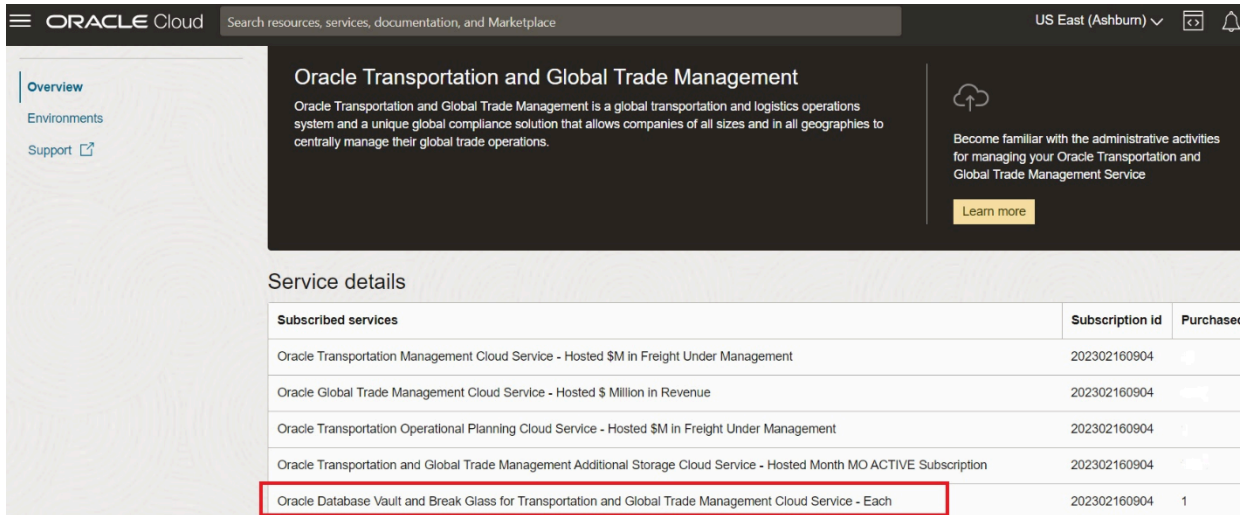
This feature allows customers to approve Oracle Administrator access to their cloud environment for analyzing and resolving environment issues.

Prerequisite:

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

You can verify that your subscription includes the Break Glass Entitlement on the Overview page for Oracle Transportation and Global Trade Management.

**Note:** The Break Glass feature is automatically enabled for environments provisioned in the Government regions.



Oracle Transportation and Global Trade Management

Oracle Transportation and Global Trade Management is a global transportation and logistics operations system and a unique global compliance solution that allows companies of all sizes and in all geographies to centrally manage their global trade operations.

Become familiar with the administrative activities for managing your Oracle Transportation and Global Trade Management Service

Learn more

Service details

Subscribed services	Subscription id	Purchased
Oracle Transportation Management Cloud Service - Hosted \$M in Freight Under Management	202302160904	
Oracle Global Trade Management Cloud Service - Hosted \$ Million in Revenue	202302160904	
Oracle Transportation Operational Planning Cloud Service - Hosted \$M in Freight Under Management	202302160904	
Oracle Transportation and Global Trade Management Additional Storage Cloud Service - Hosted Month MO ACTIVE Subscription	202302160904	
Oracle Database Vault and Break Glass for Transportation and Global Trade Management Cloud Service - Each	202302160904	1

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 [Break Glass Support for Environments](#) to setup the lockbox and approvals for your environments.

## Customer Managed Keys for Oracle Break Glass

By default, your Global Trade and Transportation 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.

Global Trade and Transportation 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.

### Adding the System Policy to Enable Customer-Managed Keys in Your Tenancy

See [Add the System Policy to Enable Customer-Managed Keys in Your Tenancy](#).

**Note:** You need to add a System Policy in your Tenancy before proceeding with enabling Customer Managed Keys. The contents of this System Policy are different for each Oracle application service. 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). The contents of this policy will be documented in the future.

Refer to the *Customer Managed Keys for Oracle Break Glass* documentation for more details on managing the Encryption Keys for your environments.





# 7 Security Considerations

## Security Evaluation or Penetration Test

Do not perform a Security Evaluation or Penetration Test on the Oracle Fusion Transportation 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 actually lead to an outage of your service.

**Note:** Penetration and vulnerability testing is not permitted for Oracle Software as a Service (SaaS) offerings.

- [Oracle Cloud Security Testing Policy](#)
- [Frequently Asked Questions About Cloud Security Testing](#)

## Modifying Service Security Data

Different companies and organizations have different service user and permission maintenance strategies. Some have a single service administrator for this user maintenance, and use the Oracle Transportation Management default user roles with high privileges. While others view this user maintenance as a help desk type of task and want to use a custom user role for just this access. Regardless of the strategy, it is good to know there are Oracle database triggers implemented, which place different constraints on which User Roles can insert, update, and delete records for specific security related tables. If the conditions of the User Role constraints are not met, these database triggers will raise different database exceptions based on the violation. Some of these below rules are very complicated.

Only users with the "DBA.ADMIN" user role can modify records in the following tables. If a user with a different user role other than "DBA.ADMIN" user role, then an "ORA-20201: User does not have privileges to modify this data" exception will be raised.

- ACR\_ROLE
- ACR\_ROLE\_ENTRY\_POINT
- ACR\_ROLE\_ROLE
- GL\_USER\_ACR\_ROLE
- GL\_USER\_BI\_APP
- GL\_USER\_BI\_ROLE
- PROP\_INSTRUCTION
- USER\_ROLE\_ACR\_ROLE
- VPD\_CONTEXT
- VPD\_CONTEXT\_VARIABLE
- VPD\_PROFILE

Only users with the "DBA.ADMIN", "ADMIN", or "SERVPROV.ADMIN" user roles can modify records in the following tables. If a user with a different user role other than these user roles, then an "ORA-20007: Transaction not permitted" exception will be raised.

- DOMAIN
- DOMAIN\_GRANTS\_MADE
- EXTERNAL\_PREDICATE
- USER\_ROLE
- USER\_ROLE\_GRANT
- VPD\_CONTEXT
- VPD\_CONTEXT\_VARIABLE
- VPD\_PROFILE
- ROLE\_ROLE\_GRANT

Only a user with the "DBA.ADMIN" user role can grant another user role the "DBA.ADMIN" user role. If a user with a different user role other than this, then an "ORA-20008: Transaction not permitted" exception will be raised.

Only a user with the "DBA.ADMIN" or "OTM-SYSTEM" user role can create or update another user to have the "DBA.ADMIN" user role. If a user with a different user role other than this, then an "ORA-20013: {User} not allowed to update gl\_user" exception will be raised.

Only a user with the logged in user role of "DBA.ADMIN" can create or update another user to have the "DBA.ADMIN" user role. If a user with a different user role other than this, then a "ORA-20020: Transaction not allowed, DBA.ADMIN role cannot be assigned by {User}" or an "ORA-20021, Transaction not allowed, DBA.ADMIN role cannot be assigned by {User}" exception will be raised.

Only a user with the "ADMIN", "DBA.ADMIN", "SERVPROV.ADMIN", or "OTM-SYSTEM" user role can create or update another user to have the "ADMIN" user role. If a user with a different user role other than this, then an "ORA-20014: {User} not allowed to update gl\_user" exception will be raised.

Only a user with the "ADMIN", "DBA.ADMIN", "SERVPROV.ADMIN", "USER-ADMINISTRATION " or "OTM-SYSTEM" user role can update or delete another user. If a user with a different user role other than this, then an "ORA-20015: {User} not allowed to update gl\_user" exception will be raised.

A user will and must be able to change their own individual Oracle Transportation Management password.

A Domain Admin user must have the "ADMIN" user role. If a different user role is used other than this, then an "ORA-20016: Transaction not allowed, Domain Admin user {User} must be assigned ADMIN user role." or an "ORA-20018: Transaction not allowed, Domain Admin user {User} must be assigned ADMIN user role." exception will be raised.

The SERVPROV.ADMIN user must have the "SERVPROV.ADMIN" user role. If a different user role is used other than this, then an "ORA-20017: Transaction not allowed, SERVPROV.ADMIN must be assign SERVPROV.ADMIN user role" or an "ORA-20019: Transaction not allowed, SERVPROV.ADMIN must be assign SERVPROV.ADMIN user role" exception will be raised.

## Integrating Security Data

Take extreme care when bulk loading or moving security related data across instances through the various Integration methods. There are slight differences depending on the integration mechanism being used. All of these integration

mechanisms do not enforce strong passwords based on account policies. Also moving bulk security data between instances may cause user expiration date related authentication issues.

## Troubleshooting User Sign in Problems

At times, there can be Oracle Transportation Management service user sign in issues that arise due to various reasons. Most of these sign in issues are a result of bad data due to security data integration and service cache inconsistency.

- Check that the Oracle Transportation Management Nickname matches the user name of the user defined within the Oracle Identity Management service.
- Check that the Oracle Transportation Management user record for that particular instance isn't expired.
- Check that the Oracle Transportation Management user record for that particular instance isn't set to be effective in the future.
- Check that there are no special characters or whitespaces prepended or appended to the Nickname field in Oracle Transportation Management.
- Not likely, but check that there aren't multiple users configured with the same Nickname.
- Not likely, but check that the domain of the user actually exists in the particular instance.
- User names can't end with "ADMIN." Don't give .ADMIN user names a Nickname.

## Content Links Embedded by Email

When sending out large emails, typically from a large report attachment, it's possible to exceed the maximum mail size on the SMTP server. Oracle Transportation Management has the following options for handling these emails:

- For large reports, the normal security level of 2 (send report via attachment) can be replaced with a security level of 1 or 3. In each of these cases, Oracle Transportation Management writes the report to a temporary file on the application server. The email recipient receives a link to a page to retrieve the report contents via HTTP. With a security level of 1, the recipient must have a valid login to view the report. Security level 3 is deprecated.
- For other large emails, Oracle Transportation Management checks the email size against a maximum, if the email is too large, Oracle Transportation Management creates a temporary file on the server and provides a link to the file in the email. When a user receives the e-mail, they are redirected to a page that retrieves the file from the server. This page requires a valid user login.

## Content Virus Checking

There are many use cases in the Oracle Transportation Management service for a user to upload arbitrary data content into the service, e.g., scanned images can be attached to shipments or structured data can be uploaded via CSV. In each of these cases, the service virus checks the content against a virus scanning server.

The virus scanning server is responsible for scanning the supplied content for viruses and responding:

- the content is clean

- the content is infected with details on the likely infection

It is unlikely but possible for the Oracle Transportation Management service to be unable to connect to the virus scanning server within a given time limit.

Since virus checking is enabled, the Oracle Transportation Management service only stores content (either locally in the Oracle Transportation Management service schema or a specified content management system), if the virus scanning server reports the content is clean. Any infection or failure to communicate with the virus scanning server forces the Oracle Transportation Management service to fail the content upload.

Difficulties communicating with a virus scanning server may critically impact business flow in the system by blocking document uploads and should be quickly resolved. Errors can occur due to:

- The virus scanning server is not responding.
- The virus scanning server host refuses a request for a virus check.
- The virus scanning server host times out during a virus check.
- The virus scanning server host returns an unexpected response that does not match the virus scanning server specification.

If you see any of these types of errors like "Virus detection connection failed", "The ICAP host is refusing requests", or "The ICAP request failed" occur during document uploads, please contact Oracle support to determine the status of the virus scanning server.

## Content Use Cases

There are a number of use cases in Oracle Transportation Management where content is brought into the service. To fully secure the cloud service, any external content is virus checked before being persisted, displayed or processed by Oracle Transportation Management. The following table describes the content use cases in Oracle Transportation Management.

### Content Use Cases

Use Case	Description	Enabled by Default
BrandingThemeUpdate	Updating a branding theme	yes
BrandingImagesUpload	Uploading branding images	yes
ContainerOptimization	A container optimization problem staged as XML	yes
CSVContent	CSV content sent in a <CSVDataLoad> or <CSVFileContent> integration transaction	yes
CSVTTargets	CSV content for TI targets	yes
DBXML	DB XML Integration	yes
DiagnosticsLog	Planning diagnostic load import	yes
DocumentIntegration	Binary or text content sent in a <Document> integration transaction	yes

Use Case	Description	Enabled by Default
DocumentStorage	Retrieving document content from a CMS (e.g. WCC or Sharepoint)	no
DocumentUpload	Uploading document content via the document finder or manager	yes
IntegrationPost	Uploading integration csv files.	yes
MessageIntegration	Mobilcomm message content sent in via a web service	no
MigrationProjectUpload	Uploading a migration project zip file	yes
OutXmlTemplate	Uploading an Out XML Template	yes
ProcurementAttachment	Attachments uploaded as part of procurement bidding	yes
ProcurementBid	Carrier response data for procurement	yes
ReportExternal	Retrieving report content from an external server other than BI Publisher	yes
ReportExternalBIPublisher	Retrieving report content from a BI Publisher server	no
StylesheetContent	Uploading stylesheet content for notification	yes
TransmissionIntegration	Transmission content sent in through the following integration methods:  HTTP POST (i.e. DirLoadServlet, WMServlet, TransmissionReceiver)  Web Service (i.e. IntXmlService, WMService)	no

## File Content Analysis

There are many use cases for a user to upload arbitrary file content to the Transportation and Global Trade Management service, e.g., scanned images can be attached to shipments or structured data can be uploaded via CSV. In each of these cases, the service does a file content analysis of the content uploaded to prevent accidental or malicious uploading of malware, attack vectors or other inappropriate files.

The uploaded file content is analyzed to ensure the uploaded file(s) are of a valid content for the intended usage (regardless of the file name extension). Using a simple file name extension alone is not sufficient in determining a true file content type. Simply renaming a file does not change the underlying file type and renaming a file to disguise its contents is a common tactic of malicious attackers. Also, using simple file detection alone is not sufficient in determining the true file content, as simply mimicking a loose file format type to disguise its true contents is another common tactic of malicious attackers.

The uploaded file content analysis includes a file detection check, a file parsing check, and a file extension check if applicable. Each one of these checks done must pass to allow the file content upload. The file upload will fail upon the first check failure. The uploaded file content is preliminary scanned to determine the type of file content being

uploaded. If it is permitted based on allowable MIME types, the uploaded file content is then parsed (if applicable) based on that detected type to ensure the uploaded file(s) have the same and correct file format structure that the detected file type should have. Finally after the file content is parsing to ensure integrity based on the file detected, the file content file name (if applicable) extension will then be checked to further ensure file and file name integrity.

There are a number of different File Content upload use cases in the Oracle Transportation Management service where file content is brought into the service. All of this external file content is analyzed before being persisted or processed by the Oracle Transportation Management service.

## File Content Analysis Use Cases

The following table describes the file content analysis use cases in Oracle Transportation Management and the permitted file content types allowed (identified using Internet-standard MIME types).

### File Content Analysis Use Cases

Use Case	Description	Default File MIME Types
BatchCSVUtil	Loading CSV files through Integration	text/plain, text/csv
BrandingThemeUpdate	Updating a branding theme	image/gif, image/png, image/jpeg, image/x-wap-wbmp, image/tiff
BrandingImagesUpload	Uploading branding images	image/gif, image/png, image/jpeg, image/x-wap-wbmp, image/tiff
ContainerOptimization	A container optimization problem staged as XML	application/xml, text/plain
CSVContent	CSV content sent in a <CSVDataLoad> or <CSVFileContent> integration transaction	text/plain,text/csv
CSVTargets	CSV content for TI targets	text/plain,text/csv
DBXML	DB XML Integration	application/xml, text/plain
DiagnosticLog	Planning diagnostic load import	text/plain
DocumentIntegration	Binary or text content sent in a <Document> integration transaction	application/msword,application/pdf,application/vnd.openxmlformats-officedocument.spreadsheetml.sheet, application/vnd.openxmlformats-officedocument.wordprocessingml.document, application/vnd.ms-excel,application/vnd.ms-word,application/x-tika-msoffice,application/x-tika-ooxml,application/xml, image/gif,image/png,image/jpeg,image/x-wap-wbmp,image/tiff,text/csv,text/html,text/plain,text/xml
DocumentStorage	Retrieving document content from a CMS (e.g. WCC or Sharepoint)	application/msword,application/pdf,application/vnd.openxmlformats-officedocument.spreadsheetml.sheet, application/vnd.openxmlformats-officedocument.wordprocessingml.document, application/vnd.ms-excel,application/vnd.ms-word,application/x-tika-msoffice,application/x-tika-ooxml,application/xml, image/gif,image/png,image/jpeg,image/x-wap-wbmp,image/tiff,text/csv,text/html,text/plain,text/xml

Use Case	Description	Default File MIME Types
DocumentUpload	Uploading document content via the document finder or manager	application/msword,application/pdf,application/vnd.openxmlformats-officedocument.spreadsheetml.sheet,application/vnd.openxmlformats-officedocument.wordprocessingml.document,application/vnd.ms-excel,application/vnd.ms-word,application/x-tika-msoffice,application/x-tika-ooxml,application/xml, image/gif,image/png,image/jpeg,image/x-wap-wbmp,image/tiff,text/csv,text/html,text/plain,text/xml
IntegrationManager	Uploading integration files.	application/xml, application/xslt+xml, text/csv, application/zip, text/plain
MigrationProjectUpload	Uploading a migration project zip file	application/zip, application/x-zip-compressed, application/x-zip, multipart/x-zip  (ZIP files can only contain text/plain and application/xml files)
MobileLogFile	Uploading log files from mobile app	text/plain (contained in application/zip)
OutXmlTemplate	Uploading an Out XML Template	application/xml, text/plain
ProcurementAttachment	Attachments uploaded as part of procurement bidding	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet,application/vnd.ms-excel, application/x-tika-msoffice, application/x-tika-ooxml, application/pdf
ProcurementBid	Carrier response data for procurement	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet,application/vnd.ms-excel, application/x-tika-msoffice
RateMaintenance	Uploading Rates	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet,application/vnd.ms-excel, application/x-tika-msoffice, application/x-tika-ooxml
ReportExternal	Retrieving report content from an external server other than BI Publisher	text/html,application/pdf,application/rtf,application/msword,application/vnd.ms-excel,application/vnd.openxmlformats-officedocument.spreadsheetml.sheet,text/csv,text/plain,text/xml,application/xml,application/x-tika-msoffice,application/x-tika-ooxml
ReportExternalBIPublisher	Retrieving report content from a BI Publisher server	text/html,application/pdf,application/rtf,application/msword,application/vnd.ms-excel,application/vnd.openxmlformats-officedocument.spreadsheetml.sheet,text/csv,text/plain,text/xml,application/xml,application/x-tika-msoffice,application/x-tika-ooxml
StylesheetContent	Uploading stylesheet content for notification	application/xslt+xml, application/xml, text/plain

Use Case	Description	Default File MIME Types
TransmissionIntegration	Transmission content sent in through the integration servlets (i.e. DirLoadServlet, WMServlet, etc.)	application/xml, text/plain
UploadCSVTargets	CSV content for TI targets	text/plain, text/csv

## Additional File Content Analysis Information

### Additional File Content Validation Information

Description	Default
Default not allowed "Dangerous" file content types blocked to prevent risky files from being uploaded.	application/ecmascript, application/javascript, application/vnd.debian.binary-package, application/x-executable, application/vnd.microsoft.portable-executable, application/vnd.ms-office.activeX+xml, application/x-msdownload, application/x-sh, application/x-perl, application/x-python, application/x-python2.7,application/x-python3, application/java, application/java-byte-code,application/x-java-class, application/java-archive, application/jar, text/ecmascript, text/javascript, text/x-jsp, text/x-python

- The MIME types are in standard `type/subtype` format (as shown in the defaults above) and only in lowercase.
- Note that Microsoft Office uses a common internal file structure for all Office document types (Word, Excel, PowerPoint, etc., because you could embed an Excel spreadsheet into a Word document or similar Microsoft Object Linking and Embedding), so the different document types cannot be told apart by the File Content Analysis code. The Apache Tika library used by File Content Analysis uses a metatype to generically identify Microsoft Office documents, which is the MIME type that will actually be matched. The specific Office document subtypes are only included in the default allowed MIME type lists for documentation purposes and possible future support from a newer version of Tika in a future release of Oracle Transportation and Global Trade Management Cloud.
- Conversely, Microsoft radically changed this common Office file structure for Office 2017 and later, so a different metatype identifies the newer files (`application/x-tika-ooxml` versus Office 2013 and earlier version's `application/x-tika-msoffice` MIME type).
- The several use cases which accept XML files are somewhat tolerant of "loose" compliance with the XML specification, but files that are not strictly compliant with the XML specification may not be identified correctly as the `application/xml` MIME type. The `text/plain` MIME type was included in these use cases so such non-strict files will still be accepted by Oracle Transportation and Global Trade Management Cloud while still rejecting files that are blatantly not XML.
- CSV (comma-separated values) files cannot be specifically identified, as any text file could have line breaks and commas in it. `text/plain` is used to identify such files and reject more complex file structures.

## Further Secure the Inbound HTTP Request External Integration URLs

External integration users require the correct permissions to use non-UI external integration http request URLs. If proper access entry points are not given to the user then failures will occur.



By default, all of the non-UI external integration http request URLs are grouped into a child access control list of "External Integration". There is a User Role of "INTEGRATION", a parent level access control list of "INTEGRATION" and a child level "External Integration" access control list which all have been created by default so you can easily assign or extend just the external integration related access control entry point to your external integration users depending on the access needs to other parts of the service.

Depending on your current user role and access control list assignment strategy and business needs, you need to determine if you should use the "INTEGRATION" user role, the parent level "INTEGRATION" access control list or the child level "External Integration" access control list. It is best to isolate the true external integration only users from other parts of the service by using one of these. You may even want to consider a custom ACL which only grants the specific integration http request URL(s) required.

List of non-UI HTTP Request External Integration URL entry points:

- `glog.integration.servlet.DBXMLServlet`
- `glog.integration.servlet.ExternalSystemServlet`
- `glog.integration.servlet.TransformerServlet`
- `glog.integration.servlet.WMServlet`
- `glog.integration.servlet.BatchCSVUtilServlet`
- `glog.integration.servlet.DirLoadServlet`
- `gtm.integration.itm.servlet.ITMIntegrationServlet`

## Additional Configuration

### General/Miscellaneous

#### Controlling Application Stack Traces

The ability to hide stack traces from end users is controlled via a property (`glog.security.stackTrace.hide=[true|false]`) and the "StackTrace – View" Access Control List (ACL). The property is already set correctly by default (true). Also by default, the "StackTrace – View" ACL is not a child Access Control List of any staged parent Access Control Lists like the "ADMIN" and "DEFAULT". This means that no user or user role even one that has the top level "ADMIN" or "DEFAULT" ACL will not have the ability to view full stack traces. If you do want to allow the ability to view stack traces, then you should just grant the "StackTrace – View" ACL on the individual user or the user role.

- `glog.security.stackTrace.hide`
  - defaults to "true"
  - determines whether or not stack traces are hidden
  - it is recommended not to change
- ACL: "StackTrace – View"
  - Provides additional configurability for individual users and user roles when `glog.security.stackTrace.hide` is true.
  - Is not a child Access Control List of any Access Control List like the ADMIN and DEFAULT Access Control Lists by default. Any user or user role with either of these top level Access Control Lists will not see a stack trace.

**Note:** The `glog.security.stackTrace.hide` property and "StackTrace – View" Access Control List control some Stack Traces for integration related activities.

**Note:** The "StackTrace – View" Access Control List is not granted to any user or user role by default.

**Note:** After a UI error, the "StackTrace" UI folder tab is not visible if "StackTrace – View" Access Control List is not granted. Also, the default label is "Details" instead of "Stack Trace".

## SSL/TLS Certificates

See the Inbound Integration and SSL Certificates and Outbound Integration and SSL Certificates sections of the Oracle Transportation and Global Trade Management Cloud Administration Guide for required information.

## Browser Cookies Used in Oracle Transportation and Global Trade Management Cloud

The following browser cookies are used in the Oracle Transportation Management service. There are only browser cookies used for the Oracle Transportation and Global Trade Management Cloud Service.

Table 2-2: Browser Cookies Used in Oracle Transportation and Global Trade Management Cloud

### *Browser Cookies Used in Oracle Transportation and Global Trade Management Cloud*

Cookie Name	Personally Identifiable Information	Retention Policy	Effect of Refusal	Usage
JSESSIONID	There is no personally identifiable information collected or stored in this cookie.	The cookie only lasts as long as the browser is open; once the browser closes the cookie is discarded.	Oracle Transportation Management will not work without this.	See notes below.

### **JSESSIONID**

The Oracle Fusion Cloud Transportation Management and Global Trade Management does not create any HTTP cookies for use in the service; however the web container creates and sets a cookie for http session tracking purpose. By default this cookie is called JSESSIONID and has a value set to random characters. Since HTTP is a stateless protocol the web container uses this cookie to maintain session state between requests.

## Trusted Hosts

The service can be configured with custom URLs to allow users to have links to other websites outside of the service. An example would be hyperlinks to a custom application or another package tracking page for a parcel carrier. However having end users click on any hyperlinks to external websites presents a potential security threat. Therefore the service has the concept of "Trusted Hosts". These hosts are defined via a multiple value property. If a configuration user enters a URL that is not defined in such a property the service will not display the URL as a link.

- Trusted Hosts can still be specified in `glog.web.security.trustedHost` for backward capability. However, you should transition and use the `glog.web.security.url.<protocol>.trustedDomain`

- Use `glog.web.security.url.<protocol>.trustedDomain` where `<protocol>` is either `http` or `https` and the value of the property is the host name or ip address of the trusted URL.
- An example for this property would be: `glog.web.security.url.https.trustedDomain=http://www.oracle.com`
- This property is a multiple value property.

```
glog.web.security.url.https.trustedDomain=http://www.oracle.com
```

```
glog.web.security.url.https.trustedDomain=http://www.oracle.com
```

- A reserved domain, `<all>`, is used to trust all domains. This is actually the default setting which means everything is trusted by default for the `http` and `https` protocols. It is strongly recommend to change the default setting.

```
glog.web.security.url.http.trustedDomain=<all>
```

```
glog.web.security.url.https.trustedDomain=<all>
```

In certain instances, such as invalid redirect URLs, Oracle Transportation and Global Trade Management Cloud will throw a security exception.

Trusted URLs are used in:

- Text fields where the “displayAsLink” attribute is set to true.
- Remarks where the remark qualifier is set to “URL”.
- Protecting the URLs Oracle Transportation and Global Trade Management Cloud re-directs to after a user logs in.

## Logging

There are different logging capabilities throughout the service components. It is recommended to review the correct documentation for that specific component on their individual logging capabilities. Please see the Oracle Transportation and Global Trade Management Cloud Administration Guide for specifics on logging and for more details, see the “Logs: System and Integration Files” help topic.

### Oracle Transportation and Global Trade Management Cloud Service Log Files

The Oracle Transportation and Global Trade Management Cloud services have the ability to enable service specific debug logging. Most of this debug logging is helpful to enable during service request issue diagnosis. However, this logging is bad for performance and could expose important sensitive data to flat log files which end users could then download. In order to obtain optimal performance and prevent information leakage, it is highly recommended to keep all enabled log IDs to a minimum in a production environment.

## Default Log Files

### Default Log Files

Log	Filename	Description
SYSTEM	glog.app.log	An application server log file that contains all of the default enabled log IDs.

Log	Filename	Description
WEB	glog.web.log	The UI Component container log file that contains the enabled log IDs logging.
EXCEPTION	glog.exception.log	An application server log file that contains all of the exceptions and the full associated stack trace.

Specific log IDs that are enabled could be logging and exposing information about the data, actual system information like URLs, user names. These important log IDs and log files should be safe-guarded. However, there are occasions that these log IDs should be enabled.

## Oracle Transportation Mobile Web Application

This mobile application requires an Oracle Transportation and Global Trade Management Cloud service instance in order to function properly. The mobile application communicates to the Oracle Transportation and Global Trade Management Cloud service via the HTTPS protocol using mostly REST APIs calls along with a few additional HTTP URL requests.

### Best Security Recommended Practices for Mobile Devices

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

- Require a passcode to unlock the mobile device before use with the use of a strong alphanumeric passcode is recommended.
- Mobile devices should be configured to lock the screen after the device has been inactive for a set period of time.
- The mobile 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.

### External Service Provider considerations for the Oracle Transportation Management Mobile Application

Carefully consider which external service provides should use the Oracle Transportation Management Mobile Application to interface into the Oracle Transportation Management Service.

## Integrating with Other Components

### Oracle Components

#### Oracle eLocation Server (MapView & Spatial)

The Oracle Transportation Management service support the use of external geomapping services. Please see the Oracle Maps Cloud section under the Geo-coding and External Distance/Time section in the Oracle Transportation and Global Trade Management Cloud Administration Guide.

### **Oracle Analytics Publisher**

See the Oracle Transportation and Global Trade Management Cloud Report Designer's Guide.

### **Oracle Analytics Server for Transportation Intelligence and Global Trade Intelligence**

See the Configuring Oracle Analytics Server in the Oracle Transportation and Global Trade Management Cloud Administration Guide for more information.

## Third-Party Complementary Components

The service provides integration capabilities with third party components for rating and distance calculations. Most of these communications between the service and these third party components are web service capabilities based on URL and additional properties that are configured in property sets. There is typically authentication required for these third party components. These third party components are not required by the service. Oracle is not responsible if these capabilities are configured incorrectly or cause any issues.

See the Complementary Products section of the Oracle Transportation and Global Trade Management Cloud Administration Guide.

The service have the capability of utilizing external engines with which Oracle does not necessarily have a certified integration. The service have the ability to use external distance and rating engines by configuring the service and implementing an externally exposed java application program interface. Although this capability must be configured, it is important from a security perspective to be aware of its existence.

## Automation Agents

The service have a major important capability of running automated agents to perform business procedures on business objects, or perform various other tasks. The automated agent capability is a pseudo-application specific language that allows complete configurable functionality based on the needs of the client's business practices. These agents and the associated logic are automatically run on the application when configured to do so and are triggered via application generated lifetime events that are raised based on various actions that took place within the service. Consult Online Help for more details about automation agents and the specific options available for the different business entities that exist within the service. By default, these automation agent capabilities can be configured by any users that have the DEFAULT and ADMIN ACLs. However, agent activity can have a significant impact on performance and all agent creation/modification should be handled by a formal change control process.

### Agent Run As

By default, agent actions run as the Admin user for the domain of the business object. There is a capability of having the agent and its associated business object procedures and tasks run as a different user or a different user role than the user related to the business event that triggered the agent to run. The different user or different user role should be related to the business object itself.

In order to change this configuration, an administrator would first need to check the value on the automation agent itself on the main tab there is a Run As Type dropdown list field, as well as fields for either the user or user role to use when the agent runs.

## Direct SQL Update

Within an automation agent, there is a capability of being able to configure any number of business actions that will directly perform any SQL statement.

The service have no capability of being able to audit the data changes that are performed by this direct SQL. There can be logging enabled but this should not be used as an audit feature due to the significant performance impact.

The Direct SQL Update agent action, although powerful, can have a significant impact on performance.

# 8 Appendix: Generic Secure Configuration Checklist

## Security Checklist

The following security checklist includes guidelines that help securely configure the service.

1. Practice the principle of least privilege.
  - a. Grant only necessary service access.
  - b. Grant only required data privileges.
  - c. Revoke any unnecessary privileges.
2. Safe guard and securely store generic user account passwords.
3. Do not share user accounts.
4. Promptly remove unnecessary or terminated user accounts.
5. Enforce access controls effectively.
6. Review service and data privileges periodically.
7. Use strong passwords and not well known passwords.





# 9 Appendix: General Properties

## General Properties

See the "Configuring the Service: Customer-defined Properties" section in the Oracle Transportation and Global Trade Management Cloud Administration Guide for instructions on how to use Property Set properties.

### General Properties

Property	Description	Values
glog.audit.beforeafter	See Data Auditing	
glog.mobile.max_session_timeout	Please see Oracle Transportation Management Mobile Application Session Timeout	
glog.servprov.autoCreateUser	Please see Service Provider User section	[true (false)]
glog.userAccess.validate	Controls whether additional validation is done during User Access configuration.  Note: This property should not be changed.	[(true) false]
glog.userManager.debug	Enables UserManager object debug logging using the SecurityDetails LogId.	[true (false)]
glog.web.security.trustedHost	Please see Trusted Hosts	

