Oracle Fusion Cloud Transportation and Global Trade Management

Administration Guide

Release 23B

Oracle Fusion Cloud Transportation and Global Trade Management
Administration Guide

Release 23B

F76485-03

Author: Paul Hamill

Contents

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*.

Thanks for helping us improve our user assistance!

2 Introduction

Basic Configuration

The purpose of this document is to help you get started with implementing and using the Transportation and Global Trade Management Cloud Services. More detailed documentation on particular topics is available in the form of online help and documents. Refer to the *Oracle Fusion Cloud Transportation and Global Trade Management Getting Started Guide* for basic information on accessing your Cloud Service and managing users.

3 Gen2 Migration

Gen2 Migration Overview

The purpose of this chapter is to provide information to assist you during the migration of your Oracle Transportation and Global Trade Management to a new data center which is part of the Oracle Cloud Infrastructure (Gen2). There are minor, but very important, differences with this infrastructure. It is important that you review these impacts and follow the necessary action items to ensure there is no disruption of your services. There is a Production Readiness Checklist section in this document to assist you with reviewing your readiness.

> **Note:** Some configuration changes (i.e. Email Configuration, IP Whitelisting, SSL Certificates) may require you to engage your Network Operations and/or Security teams.

Oracle began provisioning new customers in Gen2 starting in April 2020. If your service was provisioned after that date, you are already in Gen2 and this migration is not applicable to you.

Determining Your Tenancy

Once your instances are provisioned, you can determine if you are on an Oracle Public Cloud or Gen2 tenancy by logging into the instance and reviewing the Settings and Action pop-up. The Cloud Infrastructure field will either be “OCI-C” or “Gen2”.

Key Concepts and Terminology

- **Oracle Cloud Infrastructure (OCI)**: Oracle Cloud Infrastructure is a set of complementary cloud services that enable you to build and run a wide range of applications and services in a highly available hosted environment. Oracle Cloud Infrastructure offers high-performance compute capabilities (as physical hardware instances) and storage capacity in a flexible overlay virtual network that is securely accessible from your on-premises network.
- **Identity and Access Management**: Identity and Access Management is the Identity Provider used by Oracle Transportation and Global Trade Management Cloud Services in Gen2.
- **Cloud Account/Identity Domain**: Customer-specific name of a group of users. Users specify their Identity Domain on the login page prior to entering User Credentials.
- **Shared Identity Management (SIM)**: Shared Identity Management is the Identity Provider used by Oracle Transportation and Global Trade Management in Gen1.
- **Identity Domain**: Customer specific name of a group of users in Shared Identity Management. Users specify their Identity Domain on the login page prior to entering User Credentials.
- **TLS**: Transport Layer Security (TSL) is the successor protocol to SSL, which uses encryption to protect the transfer of data during transmission. TLS is used for securing inbound and outbound integration from Oracle Transportation and Global Trade Management Cloud Service.

Key Differences Between Gen1 and Gen2

The following represent changes between Gen1 and Gen2.

My Services Cloud Portal

The My Services Cloud Portal is the user interface where Service Administrators administrate users and manage their service instances. There is a different version of the My Services Cloud Portal for Gen2. During the migration process, the Service Administrator will receive a welcome email with the subject "Action Required: Please Activate Your Services." This email contains the URL for the new My Services Cloud Portal. Please refer to the User Sign-On/Identity Management section for more details on how to manage users within the new My Services Cloud Portal. Refer to the "*Designate New Service Administrator for Migration*" section of this document for details on how to change the Service Administrator prior to the Migration. There are two URLs that can be used to access the new Cloud Portal. One is based on your Identity Domain Name, the other is based on your Cloud Account ID.

- https://myservices-<my_identity_domain>.console.oraclecloud.com/mycloud/cloudportal/cloudHome
- https://myservices-<my_cloud_account_id>.console.oraclecloud.com/mycloud/cloudportal/dashboard

Note: Oracle Transportation and Global Trade Management users do not need access to the Cloud Portal. Instead the existing URL should re-direct users to the new instances in Gen2.

User Sign-On/Identity Management

The Single Sign-On Identity Provider in Gen2 is Oracle Identity Cloud Service (IDCS). As it is with Gen1, users need to be provisioned both within the Single Sign-On and within Oracle Transportation and Global Trade Management. User Authentication is enforced by the SSO, whereas User Authorization (Roles) are enforced within Oracle Transportation and Global Trade Management. Managing users within IDCS is similar to the legacy Shared Identity Management (SIM) service used in Gen1. Please refer to Users section of the Oracle Transportation and Global Trade Management Security Guide for more details on this subject.

Customers that have Additional Test Environments, aka "Dev" Environments, need to be aware of a significant difference in Gen2. In Gen1, the Production/Test Environments shared the same Identity Domain, but each Dev Environment had its own Identity Domain. In Gen2, all Environments share the same Identity Domain. Access to particular Environments should be controlled by whether or not a given user has been created in a given Environment using the Oracle Transportation Management and Global Trade Management User Manager.

Users will be migrated automatically from the legacy Identity Management prior to the cutover to the Gen2 instance. However, customers will be responsible for dual maintenance of users added/deleted between the user migration and the actual cutover date. It is also possible that some user's password will expire in legacy Identity Management between those two events. If that happens the password change will not be propagated to the Gen Identity Management. The source of the User Migration is the Identity Domain in Gen1 associated with Production/Test. The users in the Identity Domains associated with "Dev" Environments will not be migrated.

By default, all migrated users can perform self-service capabilities in Oracle Identity Cloud Service, such as updating their profiles, resetting their passwords, and changing their email preferences. The Identity Domain Administrator role will not be migrated from Gen1. You will need to assign this Role to users after the user migration is complete. To assign Roles to users, access "**Security > Administrators**" on the IDCS menu. 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.

The Identity Cloud Service can be access via the new My Services Cloud Portal. Please refer to the My Services Cloud Portal section above for instructions on how to access the Cloud Portal in Gen2. You access Identity Cloud Services by clicking on the menu in the top left of the Cloud Portal. Select "**Users**" and then "**Identity (Primary)**." Then click on the "**Identity Console**" button on the top right side of the page. You should bookmark this IDCS URL for future access.

An important difference with Gen2, is that the Password Policy in Gen2 is configurable. It is no longer necessary to use Security Questions for users to recover a forgotten or expired password. Users can click on the **Need Help Signing In** link on the login page to reset their password. To change the default Password Policy in Identity and Access Management, select **Settings > Password Policy** on the menu in the upper left section of the page.

Identity and Access Management provides some advanced capabilities. 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 Identity and Access Management documentation for more details on these features.

Federated Single Sign-On

The configuration for Federated Single Sign-On is similar between Gen1 and Gen2. It is important to understand that the Migration will not handle migrating the customer specific configuration of Federated Single Sign-On. It is your responsibility to sign into your Gen 2 Cloud Portal and configure Federated SSO prior to the migration cutover dates. Refer to the Federated Single Sign-On section in the Security Guide for more details on this subject. The following My Oracle Support Note will also be helpful: *How to Set Up Federated SSO for OTM on GEN2 (Doc ID 2932400.1)*.

> **Note:** Some customers instruct their users to log into the Oracle Transportation and Global Trade Management instance via the Cloud Portal. This will no longer work after the migration process starts, because the OTM instances are moved to a different Cloud Portal. Users should be instructed to bookmark the URL and access the instance using the bookmarked URL instead of accessing via the Cloud Portal. If some users login without the Federated Sign-On, it will be necessary to enable the hybrid login page. The hybrid login page is enabled with the option "Enable Sign In to Oracle Cloud Services with Identity Domain Credentials" in the SSO Configuration section of the existing Cloud Portal.

Business Metrics

The business metrics which were available in the Cloud Portal as part of Gen1 have been moved within the Oracle Transportation and Global Trade Management user interface. These metrics are now available by running a report.

IP Allow List

Some customers have firewall rules to restrict the source/destination IP Addresses for integration data sent from/to Oracle Public Cloud. In Gen1, all outbound integration from the Oracle Public Cloud is routed through a proxy server. In Gen2, all outbound integration is instead routed through a NAT Gateway. If you have a firewall with IP restrictions on inbound or outbound integration to/from your data center, refer to the *IP Allow List* section in this document for further instructions.

URL/SSL Certificates

The URL and SSL Certificates used with environments in the Gen1 data center should still work with your instances in Gen2. However, it is still very important that you test Inbound and Outbound integrations once your Test instance is migrated. It is not expected, but possible, that you will need to import the Certificates into your upstream Integration systems.

At some point in the future, you will be asked to switch to using the new URL and SSL Certificates. The URL of the new instances are displayed in the new My Services Cloud Portal. You are encouraged to start using the new URL as soon as possible. Advanced notification will be provided when the Gen 1 URLs and Certificates will no longer be supported. Switching to the new URLs may require downloading and importing the new Intermediate SSL Certificate into your upstream integration systems.

TLSv1.2

TLS is a transport security protocol used for securing inbound and outbound integration from Oracle Transportation and Global Trade Management. Gen2 only supports TLSv1.2 for both inbound and outbound integration, whereas Gen1 allow TLSv1.1 for Outbound integration. It is important that you validate your outbound integration on your Gen2 Test instance to ensure your integration is working prior to the cutover of your production instance.

GoldenGate Data Replication Service

Oracle GoldenGate Data Replication is an optional paid service to replicate the Oracle Transportation and Global Trade Management Cloud Service database to another Oracle Cloud Database service. It will be necessary to rebuild the GoldenGate server after the migration to Gen2 is complete. If you own this service, please open a Service Request to get more details on how to rebuild your GoldenGate server after the migration is complete.

Email Service

The email solution in Gen2 has changed and enforces practices to ensure better email deliverability. It is necessary for all customers to review and potentially change the Email From address when their instances are migrated to Gen2. Refer to the *Configuring the Email From Address* section for more details on this subject. The Email Services in Gen2 do not permit using From Addresses like *.oraclecloud.com, *.oracle.com, or *.glog.com. Please change your From Address in "glog.workflow.notify.advisor.email" glog.property to the data center specific Common Approved Sender until you have time to start using an email address with a proper domain name.

Email receiving systems use a variety of techniques to identify potential spam. In order to ensure the highest level of deliverability of email originating from Oracle Transportation and Global Trade Management instances, it is necessary to create a From Email Address that uses a custom domain that is configured to protect the email from spam detection. Refer to the *Configuring a Custom Domain* for more details on this subject.

Oracle understands that it may take some time for you to implement an Email From Address that uses a properly configured custom domain. In the interim, Common Email From Addresses are available in every Gen2 data center. It is important to understand that there are significant limitations when using this approach and it is highly discouraged from being used in production.

Note: You may need to change the value of multiple properties after the OCI migration if you are changing the Email From Address. You may also need to change the address defined in the "LOGISTICS" Involved Party on your Order Releases.

Refer to the *Using a Common Approved Sender Email Address* section for more details on this subject.

IPP Printing

In Gen2, it was required to configure your IPP Print Server in BIPublisher to use the Oracle proxy server. There is no proxy server in Gen2, so this configuration must be removed. You will need to login to BIPublisher and edit any IPP Print Servers. You will need to blank out the proxy host and port and save your changes. You also may need to adjust the ip addresses of any firewall rules protecting to the IPP Print Server. Refer to the *IPP Allow List chapter* for more details on this topic.

Migration Process

Customer Service Administrators will receive several notifications in regards to this migration. The initial notification will provide high level instructions on preparing for the migration. Test and Production instances will be migrated separately two weeks apart. Dev instances will be migrated at the same time as Test or Production, depending on the patching cadence you requested for these instances. A few weeks prior to the Test instance migration, customers will receive a notification that the migration process is about to start.

Designate New Service Administrator for Migration

There is a new property in the "CUSTOM" Property Set that allows you to designate the email address for the Gen2 welcome email. The default value for this property is the email address associated with the "DBA.ADMIN" user in OTM. Review this property and change the email address if necessary. Log into the OTM Production instance, select **Configuration and Administration > Property Management > Property Sets**, search for the "CUSTOM" Property Set ID, click on "CUSTOM", and look for the property named "glog.gen2migration.serviceadmin". If you would like to change the value, click on the pencil icon for the corresponding row and change the value and save the results.

Cloud Account Creation

The first step in the process is to generate a new Cloud Account. The migration process will automatically generate a Cloud Account with the same name as your existing Identity Domain Name in Gen1. Note: Some customers will already have a Cloud Account, in which case your Oracle Transportation and Global Trade Management Service will be automatically associated with that Cloud Account.

The welcome email for new Cloud Accounts will be sent to the current Service Administrator for your Cloud Service (see above). This email will contain the URL and default credentials for your accessing the Oracle Cloud Portal, which allows you to administrate the Oracle Cloud Services and Users. Note the rest of the users will automatically be migrated prior to the Test Instance Migration.

User Migration

A few days prior to the migration of your Test instance, users will automatically be migrated from Gen 1 Shared Identity Management to your new Cloud Account. At the time of the user migration, every user's password will be the same as it is in Gen1. However, if the user's password subsequently expires in Gen1, the password in Gen2 will no longer by in-sync. It is also important that any changes to users in SIM will need to be manually made in Gen2 Identity Management. Once

the production environment is migrated, it will no longer be necessary to maintain users in the legacy SIM instance and eventually it will be taken offline.

Test Instance Migration

The migration of your instance will take several hours to complete. You will receive a standard maintenance notification once the migration is complete. It is important that you prepare to validate this environment once it is available and complete the necessary configuration changes detailed in this document prior to the migration of your production instance.

Production Instance Migration

The migration of your Production instance will be scheduled two weeks after your Test instance. A Production Readiness Checklist has been provided to assist you in ensuring that you have done all the necessary configuration and testing to prepare for the Production Migration.

Reconfigure VPN

If you have a VPN configured for your instances in Gen1, it will be necessary to set up a new VPN in Gen2. Refer to the following MOS Note for details.

- *How to Setup VPN/FastConnect to Access OTM Over VPN/FastConnect on Oracle Cloud Infrastructure (OCI) (Doc ID 2831859.1)*

Step-by-Step Summary of Customer Responsibilities

The following list is a summary of the Customer Responsibilities to ensure a successful migration.

1. Confirm Correct Gen2 Cloud Account Welcome Email Recipient
2. Assess P2T and Weekly Patch Needs and Submit Requests
3. Confirm All End Users Login Using Direct Environment URL
4. Review Available Documentation
5. Assess Migration Impact on Integrations
6. Assess Work to Comply with New Gen2 Email From Address
7. Confirm Access to New Gen2 My Services Cloud Account
8. Begin Federated SSO, VPN, and GoldenGate Set Up, As Necessary
9. Manage My Services Cloud Account SSO Users
10. Complete Migration and Quarterly Update Validation Testing

Refer to the following My Oracle Support Notes for the latest information on the Migration process.

- *Overview of OTM/GTM Migration to OCI Gen2 (Doc ID 2918678.1)*
- *Gen2 Oracle Cloud Infrastructure Migrations Frequently Asked Questions (FAQ) (Doc ID 2918384.1)*

4 Configuring the Application

Customer-Defined Properties

Much of the configuration of Oracle Transportation and Global Trade Management involves managing properties used by the application. Properties are divided between their use in the web-tier (i.e. screen-related properties) and in the application-tier (i.e. business properties). You can view the current value of a property using the App-Tier Properties and Web-Tier Properties accessed via **Configuration and Administration > Technical Support > Diagnostics and Tools > Configuration**. Type the beginning of a property name in the Filter field and click Refresh button to see a list of matching properties and their corresponding values.

Note: Only users with an **ADMIN** User Role have access to this menu option.

Note: Changes made to properties on this page are lost when the server is restarted.

Property Sets

In the Oracle Public Cloud, you can make permanent property changes using the Property Set manager. A property set is a collection of ordered property instructions stored in the database. This page is accessed via **Configuration and Administration > Property Management > Property Sets**.

The **CUSTOM** property set, provided during installation, should be used for simple property changes. This property set will override staged properties in both the web and application tiers. More complex property set hierarchies can be created. For more details, see the “Property Sets” help topic.

Property Sets contain important settings, which affect the system. For example, the following property can be used to configure automated emails: glog.properties.email.recipients.

Please refer to the “glog.properties Properties” help topic for more details.

Password Properties

Passwords are not stored in property files or property sets. Instead, password values are stored in secure wallets.

Any change to a password property in the Property Set manager is stored in the wallet. Note that all password values are masked on the manager for security reasons.

Units of Measure

Oracle Transportation and Global Trade Management stores all amounts in two units of measure: the actual unit of measure and a storage default unit of measure. The storage default amount is stored in the database “BASE” columns and is used to support querying amounts (i.e. Shipment Total Weight) which have different actual units of measure.

The storage default is designated by an indicator on the unit of measure for each unit of measure type (weight, volume, distance, etc.). The default for storage default uses U.S. standard units of measure.

In most cases, the unit of measure displayed on the user interface is controlled by a user preference. If a user does not have a user preference defined, the unit of measure is controlled by the Display Default indicator on the unit of measure for each unit of measure type. The default for Display Default uses U.S. standard units of measure.

The Display Default and Storage Default settings can be modified by running an action on the corresponding unit of measure. In addition, new units of measure and corresponding conversions can be created. The Unit of Measure page is located at **Configuration and Administration > Power Data > General > Unit of Measure**. This page is only available when you are logged in as DBA.ADMIN. For more information, see the help topic “Unit of Measure”.

Currency

By default, Oracle Transportation and Global Trade Management uses US Dollars when saving costs to the database. Also by default, Oracle Transportation and Global Trade Management triangulates all currency conversions through US Dollars.

> **Note:** The CSV records in the CURRENCY_EXCHANGE_RATE.csv are provided as samples and must not be used for currency conversions. You must load your own exchange rates using the CSV or Exchange Rate Inbound transmissions.

Example

This example illustrates how Oracle Transportation and Global Trade Management stores a shipment cost record with the currency storage default set to two different currencies.

Total actual cost of the shipment is 1000 JPY. If Oracle Transportation and Global Trade Management’s currency storage default is USD (current default in all Oracle Transportation and Global Trade Management installations), Oracle Transportation and Global Trade Management stores this cost as follows:

- Total_actual-cost: 1000
- Total-actual-cost_currency_GID: JPY
- Total_Actual_cost_base: 7.76

If instead Oracle Transportation and Global Trade Management’s currency storage default is GBP:

- Total_actual-cost: 1000
- Total-actual-cost_currency_GID: JPY
- Total_Actual_cost_base: 5.31

In the first instance, the rate of 7.76 represents the USD value of 1000 JPY converted at the current rate in Oracle Transportation and Global Trade Management (128.77) while in the second instance the rate of 5.31 represents the GBP value of 1000 JPY converted at the current JPY/GBP rate in the system (188.08).

When to Change Currency Storage Default

There are two scenarios where you would like to change your currency storage default: either you only use one currency other than USD or you use multiple currencies but not USD.

Rates in One Single Currency

If you only have one currency other than USD, you only need to set your currency storage default to the currency you use. For example, Oracle Transportation and Global Trade Management stores a 100 GBP shipment cost as 100 in both the total cost and the total cost base fields so no currency conversion is needed. In the case of multiple currencies, you need to decide what the currency storage default is for your Oracle Transportation and Global Trade Management installation before setting it.

The Storage Default Unit of Measure can be set by running an action on the "Currency" Unit of Measure. The Unit of Measure page is accessed via **Configuration and Administration > Power Data > General > Unit of Measure**. This page is only available when you are logged in as DBA.ADMIN. For more information, see the help topic "Unit of Measure".

Oracle Transportation and Global Trade Management still needs currency rates to convert between the currencies you use. You can download rates from the IMF website. (This populates the DEFAULT rate in the CURRENCY_EXCHANGE_RATE table.) Note: All exchange rates from the IMF are against USD. The following instructions are for using a base currency other than USD or to use a source other than the IMF:

- Update the rates you need manually or use a XML or CSV process while again entering your needed rates against your preferred currency. You can do this nightly, monthly, or at any other frequency.
- In the `glog.properties` property file or the `CUSTOM` property set, set `glog.currency.base` to your currency storage default (e.g. EUR). This makes Oracle Transportation and Global Trade Management triangulate through the currency of your choice.

This means that Oracle Transportation and Global Trade Management will have all DEFAULT rates stated against your base currency and triangulate using your base currency.

Country Codes

Oracle Transportation and Global Trade Management can be configured to use 2 or 3 character Country Codes. Both sets of Country Codes are loaded into the Country Code table. However, the user interface needs to be configured to display values from only one of these data sets. It is important to decide which data set will be used up front since there is no facility to change this data on related entities once the data has been used. Configuring the Country Code data set is accomplished using the Database Property Management page accessed via **Configuration and Administration > Property Management > Database Property Management**.

Business Number Generator

The Business Number Generator (BNG) is a Transportation and Global Trade Management mechanism for creating IDs based on a complex set of business rules. Since the IDs are based on a sequence, it is necessary to generate the

IDs one at a time in order to prevent duplicate IDs. For this reason, a process may have to wait for another process to finish generating an ID. This waiting can manifest itself as a performance issue. The impact is even more significant in a scalability environment since the synchronization must be coordinated across application servers. Transportation and Global Trade Management disables unnecessary BNG by default. In unusual circumstances it may be necessary to change this.

The Bill of Lading 'BM' Shipment reference number can be enabled with the following property:

```
glog.shipment.createBMRefnum=true
```

The Oracle Database sequence number generator has less overhead than the BNG and should be used instead of the BNG when possible. The following database sequences can be changed to use BNG by removing the following Properties:

```
glog.server.bngenerator.oracleSequence.xid.S_SHIP_UNIT_XID.DEFAULT=S_SHIP_UNIT_SEQUENCE
glog.server.bngenerator.oracleSequence.xid.SHIPMENT_XID.DEFAULT=SHIPMENT_SEQUENCE
glog.server.bngenerator.oracleSequence.xid.ORDER_MOVEMENT_XID.DEFAULT=ORDER_MOVEMENT_SEQUENCE
glog.server.bngenerator.oracleSequence.xid.SHIP_UNIT_XID.DEFAULT=SHIP_UNIT_GID_SEQUENCE
glog.server.bngenerator.oracleSequence.xid.ORDER_RELEASE_LINE_XID.DEFAULT=ORDER_RELEASE_LINE_GID_SEQ
glog.server.bngenerator.oracleSequence.xid.MONITOR_AGENT_XID.DEFAULT=MONITOR_AGENT_SEQUENCE
```

Refer to the Property Set section for more details on how to remove a Property.

User Interface

The Oracle Transportation and Global Trade Management user interface provides many capabilities for configuring the user experience. The following section describes some of these capabilities and potential pitfalls when using them.

Branding

As it relates to Oracle Transportation and Global Trade Management, the term “branding” refers to the process of changing the look and feel of the application to reflect the you or your client’s brand. Oracle Transportation and Global Trade Management is shipped with configurable images and web interface themes, which gives you the ability to easily change colors and logos viewed on Oracle Transportation and Global Trade Management web pages. For example, you can use your own logos to replace the default Oracle and Oracle Transportation and Global Trade Management logos throughout the application. The Oracle Transportation and Global Trade Management Cloud service supports two forms of branding:

- Themes
- User-defined Images

Themes

An Oracle Transportation and Global Trade Management “theme” is a specific color scheme for the application. A theme also provides the ability to reference user-defined images or logos. The following page allows you to create and modify themes: **Configuration and Administration > Branding > Theme Management**. This page can only be accessed by someone with DBA access.

There are several color schemes available by default:

- Redwood (Default): this is the default color scheme automatically used by OTM/GTM.
- Autumn Red
- Crisp Green

- Dark Blue: This theme does not include a springboard background image.
- Dark Grey
- Midnight Blue
- Sky Blue

Configurable images include:

Login

Variables in this section apply to the **Transportation and Global Trade Management log-in** page.

- **Login Logo**: The image that appears in the lower right-hand corner of the Sign In To Oracle Transportation and Global Trade Management screen. Only used for a global theme.

  > **Note:** By default this variable is hidden. To show this variable set the property `glog.webserver.branding.showLoginOptions` to true.

  > **Note:** When using a single-sign on server (SSO) such as Transportation and Global Trade Management in the Cloud, this image is not used.

Home

Variables in this section only apply to the **Transportation and Global Trade Management** home page and Unified Global Header.

- **Header Logo**: The image that appears next to the Navigator icon in the Unified Global Header.
- **Springboard Background Image**: The image that appears behind the springboard.
- **Branding URL**: The URL used when you click the Header Logo.
- **Springboard Background Color**: The color used as the background color for the application shell. Enter a valid HTML color code or use the browser's color selection tools.
- **Main Font Color**: The font color used for the top level springboard menu items. This color is also used for third level springboard menu items.
- **Springboard Submenu Font Color**: The font color used for the second level springboard menu items.
- **Springboard Submenu Background Color**: The background color used for the second level springboard menu items. The default is white.
- **Header Icon Color**: The color used for the Unified Global Header icons.
- **Header Background Color**: The color used as the background color for the Unified Global Header.
- **Title**: The text displayed next to the Header Logo.

Logout

Variables in this section apply to the Transportation and Global Trade Management log-out page.

- **Logout Logo**: The image that appears after you click the **Sign Out** link to log out of Transportation and Global Trade Management. Only used for a global theme.

  > **Note:** When using a single-sign on server (SSO) such as Transportation and Global Trade Management in the Cloud, this image is not used.

For more details, see the “Theme Management: Create Theme” help topic.

User-Defined Images

User-defined images can be any graphic in .gif or .jpg format. They can be used in email messages, themes, as design elements for a workspace, or be assigned to user-defined fields that get associated with business objects (for example, orders, shipments, etc.). The Set Image action is used to set the image on the corresponding business object. The following page allows you to upload user defined images: **Configuration and Administration > Branding > Upload Mail and User Defined Images**. For more details, see the “Upload Mail and User Defined Images” help topic.

Finder Page Size

A Finder Page is the Oracle Transportation and Global Trade Management terminology for the standard result page which is returned when running an Oracle Transportation and Global Trade Management finder query. The number of records returned per page is configurable via the “Finder Page Size” user preference. Increasing this from the default value of 25 has a direct impact on the performance of loading this page due to the increased amount of data that needs to be processed and displayed. Values greater than 100 are likely to make the performance unacceptable.

User Favorites

Favorites allow you to limit initial `Find ()` results so that your favorite results are displayed first. For example, you can create a favorite for locations. In that favorite, you specify the top 10 locations which you use on a regular basis. Then, whenever you use the `Find ()` button the system first displays those 10 locations. If you want to find a different location, you are given the option to search for more locations.

Adding Search Fields to Finders (Grid-Flattening)

Grid flattening enables administrators to present "pseudo fields" for search, result, and other manager pages that are configured to the needs of their users. Pseudo fields "flatten" a grid by presenting field labels that are more specific than the default fields. For example, a PO Number field could be added to the order base search page, so users can search for purchase orders directly by their numbers. Grid flattening is used to make it appear as if data from a child database table is on a parent database table. Using grid flattening on search and result pages should be done with caution since the resulting query is more complex and therefore susceptible to slower performance.

Manager Layout Producer Configuration

Manager layout allows you to configure a page by adding or removing fields. The XML document for an object is created by a series of "producers". These producers are associated with objects within Oracle Transportation and Global Trade Management. Each manager in Oracle Transportation and Global Trade Management has an XML document associated with it. When you create a customer-defined manager layout, you can create or remove fields from that manager. The system creates an XML document containing relevant data that is displayed in that manager. However, the XML document may contain data that is no longer needed in a customer-defined manager that has had a lot of

fields removed. By deleting the associated producers from the customer-defined manager the XML document will be smaller, allowing the page to load more quickly. For more details, see the "Manager Layout: Producers" help topic.

Customizing Visibility of PUBLIC Data

Oracle Transportation and Global Trade Management includes various data by default such as currency codes, country codes, and reference number qualifiers. It may be desirable at times to remove some of this data from drop downs and pick lists, for example, if you only work in a small number of currencies or do not use the PUBLIC qualifiers. This can be accomplished by attaching a VPD predicate to the table for that data. For example, if you want to restrict currencies to only USD and EUR, create or edit the VPD profile for the users who should only see those currencies to include the following:

Table Name: CURRENCY, Predicate: currency_gid in ('USD','EUR')

(Be sure the "Use External Predicate Rule" box is checked.)

Diagnostic Tools

Oracle Transportation and Global Trade Management provides several utilities to help while configuring the system and while the system is running. The following sections describe these utilities.

Application Logging

Oracle Transportation and Global Trade Management provides an embedded logging utility. Application logging is configured on the page **Configuration and Administration > Power Data > General > Log Files**. Application logging provides detailed information about the processes running in the system. The output of the logging is viewed on the following page, which is accessible from all parent menu groups,**Process Management > Logs > System**. For more details, see the “Logs: System and Integration Files” help topic.

Although logging is a vital function in Oracle Transportation and Global Trade Management, excessive logging is a very common cause of poor performance. This is particularly true of bulk planning processes. You can review what logging is currently enabled in the system using the page **Configuration and Administration > System Administration > Logging Overview**. You can also temporarily disable all logging by setting the following property:`glog.log.suppressAll=true`

Setting this property can be a quick method of determining whether logging is the cause of a performance issue.

> **Note:** The **Logging Overview** screen cannot be used to display summary information or suppress logging in Log Files of type WEB.

LogIDs with a suffix of “Debug” or “Details” have the potential to log significant amounts of data and should be avoided unless directed to be by Oracle Technical Support. Ad-hoc logs are the most dangerous because they generate logging regardless of the user logged in. On the other hand, User logs only write to the log file when that particular user is logged in and using Oracle Transportation and Global Trade Management. In some scenarios user logs can still have a significant impact on performance, even if that particular user is not logged in. This logging happens because there is a certain amount of overhead in generating a log message. The overhead occurs before Oracle Transportation and Global

Trade Management determines, based on the logged in user that it does not need to write the message to the log file. For this reason, having many user logs with detailed logging enabled can have a significant impact on performance.

Note: In the Oracle Public Cloud, log files are limited to a maximum size of 10MB and 20 Backups.

Performance Monitoring

Oracle Transportation and Global Trade Management provides embedded tools which should be used for investigating performance issues. The following tools are located on the menu at **Configuration and Administration > Technical Support**:

- Diagnostics and Tools
- Configuration Collection
- Performance Collection

These tools provide insight into the current transactions in the system, as well as, historical statistics based on previous transactions. They capture data on technical components of the application such as data caches, workflow threads, object locks, and more. Diagnostics and Tools are a set of user interfaces, whereas Configuration Collection and Performance Collection are utilities which capture data in an XML format. Should performance issues occur in the system you may be requested by Oracle Technical Support to monitor and/or capture data from one of these utilities.

Historical Metrics and Notifications

The Oracle Transportation and Global Trade Management Cloud Service captures a broad set of performance metrics. These performance metrics are persisted to the database on an hourly basis and are aggregated by day and week and are referred to as Historical Metrics. The Historical Metrics cover many technical components within the service including User Interface, Integration, Agents, Email and Logging. They also cover Infrastructure Health components including caches, connections, object locks, and memory. These metrics should be used to help identify, diagnose, and resolve application performance issues. Refer to the **Historical Metrics** topic in the online help for more details.

Metric Collections provide a configurable mechanism for comparing Historical Metrics to a baseline. Email Notifications can be generated based on user defined thresholds. It is also possible to initiate a Diagnostic Logs capture, QDLogs, based on a defined threshold. This will provide additional diagnostic data for analysis by Support and Development. Please refer to the **How to Configure Metric Collections** topic in the online help for more details.

Business Object Caches

The Transportation and Global Trade Management Business Object caches are maintained by Transportation and Global Trade Management. The majority of Transportation and Global Trade Management Business Objects caches use a Least Recently Used (LRU) strategy to maintain the cache. When an LRU cache reaches its maximum, a one-for-one exchange is made for the new object and the least recently used object in the cache. Most static data used by Transportation and Global Trade Management business logic is maintained in one of these caches. The App-tier Caches utility page, located on the menu under Technical Support – Diagnostics and Tools – Caches, can be used to review statistics on these caches.

The size of a Business Object Cache can have a significant impact on performance. The efficiency of a cache is measured by its hit ratio. A low hit ratio is a possible indication of an undersized cache. If a cache has reached its capacity and the hit ratio is low (less than 0.80), performance may be impacted. Increasing the maximum size of this cache may increase system performance. Temporary changes can be made to the cache using the diagnostic screen, but the changes will revert to the default upon restart. To permanently change the size of a cache the appropriate glog.property must be set in a Property Set. For example, the size of the Rate Offering cache is set by the following property:`glog.cache.TRateOfferingCache.capacity=2000`

It is important to note that increasing the size of the cache has the adverse effect of increasing memory usage, so changes should be done incrementally and with thorough testing. Please refer to the Property Sets section of this document for more details on changing property value.

Timeouts

In order to maintain stability of the application, timeouts have been configured. It is important to be aware of these timeouts, however they cannot be modified.

Thread Tuning

Transportation and Global Trade Management workflow is based on a set of business topics and thread groups. A Topic is the Transportation and Global Trade Management terminology for a particular workflow process. For example, AutoMatchInvoice is a topic. Each Topic is associated with a thread group by a glog.property.

A Thread Group is a set of threads dedicated to processing a set of topics. Each thread group is given a number of threads that can be used to simultaneously process topics. When all threads in a group are busy processing a topic, all additional topics are placed in a queue until a thread becomes available. Transportation and Global Trade Management computes statistics for the amount of time a topic spends waiting to be processed and the amount of time spent processing the topic. These statistics can be reviewed with the Event Diagnostics page available on the DBA Technical Support menu.

A long average wait time and/or a backlog of queued events, accompanied by a short average time to process the topic, may indicate a need to increase the number of threads in a thread group. These thread settings may be maintained in the Property Set Manager in either the "`APP_WORKFLOW_THREADING`" or "`CUSTOM`" Property Set. Thread settings in "`APP_WORKFLOW_THREADING`" take precedence. Each thread group has a corresponding property to control the number of threads

- `glog.workflow.queueThreads.<queuename>`

"`<queuename>`" should be replaced by the name of the queue (i.e. "planningBuild", "transport – Services") and specified in Property Set's "Key" field. The number of threads should be specified in the Property Set "Value" field. Data Queue threads such as INTEGRATION IN are managed differently. See *Integration Data Queues* for more information.

In addition to configuring the number of threads, particular parts of the planning process support multi-threading. The behavior of multi-threading is configurable based on a Batch Size. By default, Cloud is configured with the following Batch Sizes.

- CommitShipmentGraphs - 25
- CommitShipmentGraphsForOrderMovements - 25

- BuildShipmentGraphCollections - 25
- BuildShipmentGraphs - 25
- BuildShipments - 25
- BuildShipmentGraphsForOrderMovements - 25
- FleetAssignment - 25

For details on this topic, please refer to the “glog.workflow Properties” section of Online Help.

Business Object Metrics

The Transportation and Global Trade Management application captures metrics to track the total number of business objects and as well as counts of the individual key business objects used across the application. A business process called *Collect Business Metrics* is scheduled to run once every day to count the business objects and store these counts. The business process can also be manually invoked via the user interface.

The business object counts are stored in the table OTM_BUSINESS_OBJECT_COUNT, for a period of 3 years. The table has read-only access for users; the counts records cannot be modified or deleted. The counts can be retrieved by querying the table, or viewed in a report. The *Business Object Metrics Report*, displays the total business object counts and the individual business object counts for each of the last 7 days. The *Business Object Metrics Report* can be accessed via the Report Manager and is listed under the Metrics section.

Recurring Processes and Automation Agents

The Recurring Processes and Automation Agents are a Transportation and Global Trade Management mechanism for creating recurring or application event driven processes within the application.

Note: Any user who switches their user role cannot be used in a Recurring Process or be used in an Agent. There is only one current user role per user at a time. Allowing a user who is configured to 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 process or agents to run as a user who does not normally log in or does not change user roles.

Note: Do not change the DBA.ADMIN user’s user role. This could cause unknown issues.

5 Configuring Email Notifications

Email Configuration Overview

The Oracle Transportation and Global Trade Management service is capable of sending out a variety of email notifications to users and business partners. For some customers, these notifications are critical business transactions such as Tender Offers. In order to ensure a high level of deliverability, it is important to configure your email From Address using a valid Internet Domain. Oracle Transportation and Global Trade Management supports three methods for sending email. There are advantages and disadvantages with each approach.

- **Common Approved Sender**: This approach uses a From Email Address that is shared among all customers in a given region.
- **External SMTP Host**: This approach routes all email to your own SMTP Host which is external to Oracle Cloud Infrastructure.
- **Custom Email Domain**: This approach uses a From Address that contains your company's domain. When done correctly, this is the most reliable method.

Refer to the corresponding section of this document for details on each approach. Regardless of the method, it is necessary to set the Email From Address, so refer to that section after you have implemented your preferred method.

Configuring the Email From Address

Before sending any email from the Oracle Transportation and Global Trade Management service, it is necessary to configure the Email From Address. It is strongly recommended to us a single Email Address as the From Address. Once you have determined the address that you will use, you configure that within the service by setting the `glog.workflow.notify.advisor.email=OTMAdvisor@example.com` glog.property in the CUSTOM property set. It is possible to add a more friendly label along with the email address, i.e. `"OTMAdvisor@example.com='Example Company Transportation Administrator'"`. You will also need to set the email address on the contact associated with the LOGISTICS involved party if using Shipment Tenders.

Note: The following properties that control Email From Addresses automatically default to the same value as "glog.workflow.notify.advisor.email". It is not necessary to set these properties unless you want to use a different Email From Address.

- glog.properties.log.email.from
- glog.procurement.fromMailAddress
- glog.mail.from
- glog.mail.quota.email
- glog.integration.servlet.TransmissionStageError.errorEmailFrom
- glog.odi.email.from.address

Configuring the Email From Address for BIPublisher

It is possible to email reports directly from BIPublisher. In order to do this, you must specify the Email From Address. After connecting to the BIPublisher Administration URL, click on the menu in the top right and select "Administration". Click on Delivery Configuration under Delivery. Set the **Email From Address** and **Delivery Notification Email From Address** fields to your chosen Email From Address. Click the **Apply** button.

Using a Common Approved Sender Email Address

Using a Custom Domain is strongly encouraged for high deliverability, however a data center specific common from address can be used in the interim. Although SPF and DKIM are configured for the domain of this common address, Oracle cannot guarantee the reliability of email deliverability when using this address. Email reputation of that From Address is shared across all customers using that address. It is also important to understand that Blocked Recipients are common to all customers using the common address. It is also not possible to receive replies to emails sent with these addresses since it is not a legitimate email address with a corresponding inbox. Oracle strongly recommends that this approach only be used as a temporary solution until a Custom Email Domain is configured.

To use this Common Approved Sender, select the Approved Sender from the list below depending on the region where your service is deployed. Refer to the *Configuring the Email From Address* section of this document on how to use this address.

Approved Sender Email Addresses by Region

OCI Region	Provided Common Approved Sender Email Address
ap-melbourne-1 Australia Southeast	`noreply@mail.otmgtm.ap-melbourne-1.ocs.oraclecloud.com`

OCI Region	Provided Common Approved Sender Email Address
ap-sydney-1 Australia East	noreply@mail.otmgtm.ap-sydney-1.ocs.oraclecloud.com
eu-amsterdam-1 Netherlands Northwest	noreply@mail.otmgtm.eu-amsterdam-1.ocs.oraclecloud.com
eu-frankfurt-1 Germany Central	noreply@mail.otmgtm.eu-frankfurt-1.ocs.oraclecloud.com
me-jeddah-1 Middle East	noreply@mail.otmgtm.me-jeddah-1.ocs.oraclecloud.com
uk-cardiff-1 UK West	noreply@mail.otmgtm.uk-cardiff-1.ocs.oraclecloud.com
uk-london-1 UK South	noreply@mail.otmgtm.uk-london-1.ocs.oraclecloud.com
us-ashburn-1 US East	noreply@mail.otmgtm.us-ashburn-1.ocs.oraclecloud.com
us-phoenix-1 US West	noreply@mail.otmgtm.us-phoenix-1.ocs.oraclecloud.com

In order for the Common Approved Sender to work, you must set the Email From address exactly as specified above. Email will not work if you try to use an email alias, i.e. `noreply@mail.otmgtm.us-phoenix-1.ocs.oraclecloud.com="noreply@mycompany.com".`

Note: If you choose to use the Common Approved Sender Email Address, you will not see the Approved Sender in the user interface and you should not attempt to register it because it is already registered.

It is now possible to register a custom Approved Sender using the region specific Oracle Transportation and Global Trade Management email domains listed above. For example, it is now possible to register an Approved Sender with the address `"noreply-mycompany@ mail.otmgtm.us-phoenix-1.ocs.oraclecloud.com"`. Using this approach alleviates the need to configure a custom Email Domain with SPF and DKIM. The custom Approved Sender must be registered via the following menu option: **Business Process Automation > Power Data > Mail Management > Mail Senders**.

Configuring a Custom Domain

Obtaining reliable email delivery requires the implementation of SPF, DKIM, and DMARC. The only way to achieve that in Oracle Transportation and Global Trade Management service is to use an email from address that uses a valid and properly configured Internet Domain. Customer's often use their company's domain. It is a best practice to create a mail specific sub-domain, perhaps even an OTM mail specific sub-domain, i.e. `OTMAdvisor@otm.mail.example.com`. Using a sub-domain will make the configuration of SPF, DKIM, and DMARC easier.

Sender Policy Framework (SPF) is an internet standard for email to reduce spamming and other fraudulent emails by specifically identifying which Internet hosts are allowed to originate email for email addresses within a specific domain name. Since spamming and phishing attacks primarily use forged sender email addresses to lure the victims into opening dangerous emails (since they appear to be from trusted friends, colleagues, or businesses), SPF prevents this by allowing receiving email servers to reject emails that come from hosts that should not be originating emails with certain sender email addresses, therefore preserving the trustworthiness of those email addresses' domains.

Terminology

- **Spoofing**: Method of forging another entity's identity (e.g., the "From" address) onto an email in order to get users to open a message.
- **Phishing**: Method of tricking recipients into giving out personal information, such as credit card numbers or account passwords, often by spoofing the origins of the email (e.g., a user's bank, credit card company, or familiar merchant).
- **Approved Sender**: The address used in the "From:" header of the emails you send must be managed as an approved sender via the Email Delivery Service (OCI SDK). The domain name used in the approved sender needs to be configured as a sending domain which requires DNS configuration; see sending domain definition below. An approved sender is a regional resource with an associated Oracle Cloud ID (*OCID*).
- **DomainKeys Identified Mail (DKIM)**: DomainKeys Identified Mail is a cryptographic signature-based type of email authentication. DKIM requires email senders' computers to generate "public/private key pairs" and then publish the public keys into their Domain Name System (DNS) records. The matching private keys are stored in a sender's outbound email servers, and when those servers send out email, the private keys generate message-specific "signatures" that are added into additional, embedded email headers. ISPs that authenticate using DKIM look up the public key in DNS and then can verify that the signature was generated by the matching private key. This ensures that an authorized sender actually sent the message, and that the message headers and content were not altered in any way during their trip from the original sender to the recipient.
- **DKIM Selector**: A DKIM selector is a short name for a DKIM private/public key pair within a given sending domain. It's also the first component of the DNS name used to publish the DKIM public key. The recommended naming convention is `<prefix>-<shortregioncode>-YYYYMMDD`. Each sending domain must have at least one unique DKIM selector per region used. Best practice advice is to rotate the DKIM key every 6 months by creating a new selector (see M3AAWG advice: *m3aawg-dkim-key-rotation-bp-2019-03.pdf*). We have future plans to automate DKIM key creation and rotation.
- **Domain-based Message Authentication, Reporting & Conformance (DMARC)**: DMARC standardizes how email receivers perform email authentication using both of the well-known SPF and DKIM mechanisms. It allows a sender to indicate within its DNS record that its email is protected by SPF and/or DKIM. If neither of those authentication methods pass, the sender can specify the actions a receiver should take (i.e. quarantine or reject the message). DMARC helps senders experience consistent authentication results for their messages at AOL, Gmail, Hotmail, Yahoo! and any other email receiver implementing DMARC.

- **Return Path**: The return path is an SMTP email source address used to process the bounces that occur with your emails. The return path is where mailbox providers send the bounces. The default Email Delivery return path domain is `<region-short-code>1.rp.oracleemaildelivery.com`. Customizing the return path can improve: Deliverability & Reputation, Addressbook addition & other allow-listing mechanisms, DMARC alignment (SPF), consistent branding.
- **Sender Policy Framework (SPF)**: SPF is an IP-based process that enables the verification of a sender's IP address by cross-checking the domain in the email address listed in the visible "Mail From" line of an email against the published record a sender has registered in the Domain Name System (DNS). An SPF record consists of a list of computer servers or IP addresses that senders indicate are "authorized" to send email for that domain. By publishing an SPF record for a domain, that domain is declaring which IP addresses are authorized to send out email claiming to be from that domain .
- **Sending Domain**: the DNS domain name used in the From header when sending email. This domain should have an MX or A record (a CNAME can be used but is not as good) and should accept mail for `postmaster@domain` and `abuse@domain` without bouncing. For more details, see *MAAWG best practices* for sending domains document.
- **Suppressions**: If you send to an email address that fails (due to a hard bounce, repeated soft-bounce, or spam/abuse complaint), we'll automatically process the bounce message and create a suppression. Subsequent attempts to send to that address will be accepted (counting against your limits) and dropped. See Managing Suppressions for more details on this topic. See *Managing Suppressions* for more details on this topic.

Configuring Approved Senders

In Gen2 Cloud Infrastructure, it is mandatory to register your Email From Address as an "Approved Sender". Within the Oracle Transportation and Global Trade Management service, the Approved Sender is added via the following menu option.

Business Process Automation > Power Data > Mail Management > Mail Senders

As of the 23A January 27 weekly, it is now possible to register a “Wildcard Approved Sender”. Instead of registering every Email From Address individually, you can now register a special Approved Sender of the format “@mydomain.com”, where mydomain is your Custom Email Domain that has been properly configured with SPF and DKIM for Oracle mail. Do not attempt to register the Wildcard Approved Sender until you have correctly configured SPF and DKIM. Once SPF, DKIM and the Wildcard Approved Sender are configured, you will be able to send email from any email address that matches the format of “@mydomain.com”. This is a very useful feature if you are using multiple Email From Addresses where you are expecting responses to the emails.

Configuring SPF

Sender Policy Framework (SPF) is an internet standard for email to reduce spamming and other fraudulent emails by specifically identifying which Internet hosts are allowed to originate email for email addresses within a specific domain name. Since spamming and phishing attacks primarily use forged sender email addresses to lure the victims into opening dangerous emails (since they appear to be from trusted friends, colleagues, or businesses), SPF prevents this by allowing receiving email servers to reject emails that come from hosts that should not be originating emails with certain sender email addresses, therefore preserving the trustworthiness of those email addresses' domains.

SPF works by having the owner of the domain name specifically identify which public Internet hosts are allowed to originate email for addresses in that domain. For example, if the `example.com` domain owner only wanted the host mx.example.com to be able to publicly send emails from anyone with a `user@example.com` email address, they could

specify that with SPF, so any other computer that attempted to send example.com emails would have their email discarded when the SPF-compliant receiving email server received the forged email.

SPF-compliant receiving email servers look up the sending email address's domain name, and see if an SPF record is specified. If so, the computer attempting to send the email is cross-checked against the list of authorized Internet addresses in the SPF record; if the sending computer is not authorized, the email can be rejected or classified as spam.

Note that SPF is not used within a corporate intranet; it is implemented at the firewall border between a company's intranet and the global Internet. This is why company-originated emails go to the Internet through a specific border public email server (or redundant cloud of servers), and are similarly received by a single publicly-exposed entry point into the company.

Emails supposedly from domains that do not use SPF probably will not be trusted, as the domain owners appear too careless to prevent forgeries in their name.

Transportation and Global Trade Management can send automated emails to many users for many different reasons, and such emails have to have a sender email address. If the sender email address is not left to the standard installation setting for an Oracle Cloud deployment, such emails will appear as forged to the recipients' email server because the email server associated with the Transportation and Global Trade Management application server may not be on the SPF-authorized list for the Internet domain name of the sender email address.

Hence, for every sender email address configured into a Transportation and Global Trade Management deployment, not only do they have to be registered with the Oracle email service (through the registration web page in the Transportation and Global Trade Management web UI), but the Oracle public outbound email servers have to be listed as authorized email originators in the SPF records for the email addresses' domains.

This requires contacting the parties within your organization responsible for maintaining your organization's domain name records, and asking them to add an SPF directive to your domain name's SPF record authorizing the Oracle public email servers to send email on behalf of the configured Transportation and Global Trade Management sender email addresses in that Internet domain.

Oracle has created publicly posted SPF sublists of the Oracle Cloud public outbound email servers that can be conveniently included by reference in your domain name's SPF record.

In order to continue, you must determine which type of cloud server your system is using. Transportation and Global Trade Management is currently delivered in two tenancies: Oracle Public Cloud and the newer Oracle Generation 2 Cloud Infrastructure (Gen2). With Gen2, only the email addresses registered with Gen2 through this interface are valid to be used as From addresses. This functionality is only available on Cloud installations running on a Gen2 tenancy. For more information on registering email addresses, see the Mail Senders topic in the online help.

One way to determine if you are on Oracle Public Cloud or on a Gen2 tenancy is to look at the URL of your instance.

If it is an Oracle Public Cloud, the URL of the instance ends in one of the following:

- `.otm.us6.oraclecloud.com`
- `.otm.us2.oraclecloud.com`
- `.otm.em2.oraclecloud.com`
- `.otm.em3.oraclecloud.com`

If it is a Gen2 instance, the URL ends in one of the following:

- `otmgtm.us-phoenix-1.ocs.oraclecloud.com`
- `otmgtm.us-ashburn-1.ocs.oraclecloud.com`
- `otmgtm.us-london-1.ocs.oraclecloud.com`
- `otmgtm.us-frankfurt-1.ocs.oraclecloud.com`

If you are using an Oracle Public Cloud system, add this directive (if not already there) to your SPF record:

```
+include:spf_c.oraclecloud.com
```

If you are using a Gen2 tenancy, you will need to add a different directive (if not already there) to your SPF record. The SPF for Gen2 is dependent on the geographic region where your service deployed. Refer to the following table to determine the correct SPF record corresponding to your region.

In your DNS setup, create a TXT record and paste the following information into the record based on the sending region:

Configuring SPF

Sending Region	SPF Record
Americas	`v=spf1 include:rp.oracleemaildelivery.com ~all`
Asia/Pacific	`v=spf1 include:ap.rp.oracleemaildelivery.com ~all`
Europe	`v=spf1 include:eu.rp.oracleemaildelivery.com ~all`
All Commercial Regions	`v=spf1 include:rp.oracleemaildelivery.com include:ap.rp.oracleemaildelivery.com include:eu.rp.oracleemaildelivery.com ~all`
Government Regions	• For US Government Cloud with FedRAMP Authorization, see *SPF Record Syntax*. • For US Federal Cloud with DISA Impact Level 5, see *SPF Record Syntax*. • For United Kingdom Government Cloud, see *SPF Record Syntax*.

Note: If your organization is already using the Oracle Cloud to service your email needs, this SPF update should already have been done.

Do not use only the directive above as your entire SPF record unless you are using the Oracle Cloud as your sole email service provider; otherwise, specifying only the Oracle Cloud SPF directive may block your other legitimate email servers. For example:

```
v=spf1 a:mx.example.com include:spf_c.oraclecloud.com -all
```

would specify for the example.com domain that their public email gateway (mx.example.com) and the Oracle Cloud email gateways are permitted to send emails for the example.com domain, and all other hosts should be rejected as probable spam forgers. Consult *Internet RFC 7208* for technical details about specifying the contents of your SPF record.

If your domain has a large quantity it may be necessary or even desirable to create a new domain or sub-domain that is specifically intended for Oracle Cloud email, i.e. "mail.example.com". You should use this domain for your Approved Sender, i.e. "`no-reply@mail.example.com`".

Note: All domains should have an SPF record specifying which servers are authorized to send email to the Internet on behalf of their domain. Oracle will be enforcing a policy of requiring customers sending email using the Oracle Cloud to properly list the Oracle Cloud email servers in your domain's SPF record. Failure to do so could cause the Oracle Cloud to be put in a Block List by other email systems, so Oracle will not accept sender email addresses which would be blocked; Oracle will instead check your SPF record and preemptively block emails using sender domains not authorizing the Oracle email gateways before the emails leave the Oracle Cloud.

The status of each sender email address used by the system can be monitored to ensure it has an associated SPF record in the customer's domain. A performance collector, MAIL COMMUNICATIONS, keeps track of every sender email, showing the status of each email address from the perspective of the domain.

You can review your SPF configuration with a public service like *dmarcian*.

Configuring DKIM

In addition to adding the proper SPF record to your email domain, it is necessary to enable DKIM (Domain Keys Identified Mail) in order to ensure reliable delivery of your mail via Oracle Cloud Infrastructure. Technically speaking, DKIM provides a method for validating a domain name identity that is associated with a mail message through cryptographic authentication. The identity is independent of other email identities, such as the Email's From Address.

DKIM requires creation of a private key for use by your approved sender and provisioning that key in DNS so that your email signature can be verified by recipients. There are two parts to enabling DKIM. Oracle creates the DKIM Keys and the customer creates a CNAME record in their domain. The first step is to create a DKIM Selector. The DKIM Selectors will be used by Oracle to generate the DKIM keys. Use the following best practices when naming your DKIM Selector:

- Use the form: `otmgtm-<prefix>-YYYYMMDD` for your DKIM Selector, where the prefix is a unique name for your service (i.e. the domain name of your Email From Address), and `YYYYMMDD` is a timestamp (i.e. 20210126).
- For example, for an Email From Address of firstname.lastname@example.com and the selector is created on January 27, 2021, the suggested selector is "otmgtm-example-20210127".
- Never reuse an already existing selector in a given sending domain; this will result in your request getting delayed. Instead create a new selector with a new date.
- Please use a recent or current date. Requests with a date older than 6 months will be rejected, unless you have a valid business reason.
- The selector must follow DNS hostname syntax (made up of alphanumeric characters, dash, internal non-repeating period).

Enabling DKIM is presently a manual process (automation is on the roadmap). You will need to open a Service Request with Oracle Transportation Management Support. Provide the following details in the request:

Please enable DKIM for my domain for sending mail from the Oracle Global Trade and Transportation Management Cloud Service.

- Sending Domain
- Approved From Email Address
- Your DKIM selector

It may take several days to process this request.

You will need to create a CNAME DNS record in your domain using the DKIM details provided in the Service Request. For example, if your selector is "otmgtm-example-20210127", you will create a CNAME record like:

```
otmgtm-example-20210127._domainkey.example.com IN CNAME otmgtm-
example-20210127.example.com.dkim.iad1.oraclemaildelivery.com
```

You can check your DKIM record using a web-based tool such as dmarcanalyzer. *https://www.dmarcanalyzer.com/dkim/dkim-check/*.

For more information, see *How to Configure Email Senders in Oracle Generation 2 Cloud Infrastructure (Gen2) (Doc ID 2742815.1)* and *Enabling DKIM (Domainkeys Identified Mail) for Oracle Global Trade and Transportation Management (Doc ID 2746725.1)*.

Configuring DMARC

DMARC standardizes how email receivers perform email authentication using both of the well-known SPF and DKIM mechanisms. It is highly recommended to configure DMARC so that you have better control over the verification of emails originating from your domain. You can check the DMARC configuration of your domain using a service like dmarcian (*https://dmarcian.com/dmarc-inspector/*).

For more detail on DMARC, please refer to the DMARC specification or other publicly available documentation on the topic.

https://tools.ietf.org/html/rfc7489

Configuring a Custom Return Path

If you would like to have a **Custom Return Path** Oracle supports creation of a custom return path for an approved sender. This has to be approved by Oracle's deliverability team and is regional.

To get a Custom Return Path:

1. Create a subdomain in your main domain. For example, with a main domain of `example.com`, you will have to create a subdomain `<prefix>.example.com` such as `rp.example.com` or `bounce.example.com`.
2. Create a CNAME DNS record that looks like `<prefix>.example.com. IN CNAME <region-short-code>1.rp.oracleemaildelivery.com`. An example of a regional return path for Email Delivery is: `fra1.rp.oracleemaildelivery.com`
3. Create MX record as below and provide the same in the SR: `10 bmta.email.<REGION IDENTIFIER>.oci.oraclecloud.com`. The `<REGION_IDENTIFIER>` is based on the region of the instance, which can be obtained from the URL, i.e. `us-phoenix-1`. *All regions are documented here*.
4. Open a Customer Support ticket, provide the approved sender(s) email address you want to have a return path for and the CNAME you configured (screen shot or text version of the record).

Managing Suppressions

Outbound Email Delivery may be suppressed at various points in the delivery process and for various reasons:

- Mail recipients may reject email with hard or repetitively soft bounces.
- Email Delivery may reject emails due to complaints, manual entry or list-unsubscribe requests.
- Transportation and Global Trade Management may block outbound emails not properly registered with Email Delivery or passing Sender Policy Framework (SPF) checks.
- Transportation and Global Trade Management may block outbound e-mails due to various mail quotas.

If email recipients report they are not receiving emails, a number of monitoring and configuration screens in Transportation and Global Trade Management can aid in determining the underlying cause and correcting the issue.

Monitoring Email Delivery Suppressions

Emails suppressed by Email Delivery can be monitored via:

- **Logging**: The **MailError** log ID shows the From and To address of each suppressed email. By setting up an ad-hoc log that enables this logging, all such email can be tracked as they fail.
- **Real-time Diagnostics**: The **Mail Suppressions** screen shows summary information for suppressed emails. For each From/To address pairing that failed, you can monitor:
  - the number of emails suppressed by Email Delivery
  - the number of emails failing due to other address issues
  - whether Email Delivery is currently suppressing the sender
  - the SPF status of the sender. This requires opting in to the **APPLY SPF CHECKS TO OUTBOUND MAIL** optional feature or setting the **glog.mail.spfCheckMailOnSend** property to **true**.
- **Historical Diagnostics**: As part of Historical Metrics, the following metric types can be used to track mail suppression over the preceding hours, days and weeks:
  - **MAIL – FAILED** shows a count of general mail failures due to addressing issues
  - **MAIL – SUPPRESSED** shows a count of mail failures due explicitly to Email Delivery suppression

  Note that these metrics are collected for three subcomponents: Total, Common Addresses and User Addresses. Common Addresses refer to valid senders pre-authorized for use for all Transportation and Global Trade Management customers. User Addresses refer to senders configured on the Mail Sender screen for your installation and domains.

Resolving Email Delivery Suppression

Once the underlying cause of Email Delivery Suppression is determined and resolved, or if the cause is known to be an aberrant failure (e.g. hard bounce due to temporary communication issue), you can request Email Delivery remove the mail suppression by clicking **Unsuppress** on the Mail Suppression screen. Note that while this will remove the suppression, the removal may be temporary if the underlying cause is not resolved. Email Delivery may simply suppress the recipient address again. If this happens, Transportation and Global Trade Management needs to work with Oracle Cloud Email Operations to determine the cause.

Incorrect SPF configuration can often lead to Email Delivery suppression. It's important to correctly configure your SPF with respect to your e-mail domains and any downstream servers. If using the **APPLY SPF CHECKS TO OUTBOUND MAIL** optional feature, these SPF checks can be viewed and reapplied from the Mail Sender screen. This allows you to fix all SPF issues before sending faulty requests through Email Delivery.

Email Delivery suppression may also be due to excessive mail use. See the Mail Quota section below for guidelines on monitoring your overall, per content and per recipient email use.

Monitoring Transportation and Global Trade Management Email Blocking

Unless using a pre-authorized sender address for outbound emails, customers must register all from addresses to Email Delivery via the Mail Sender screen. The system will block sending of any email to a sender not successfully registered as a Mail Sender. These blocks can be monitored with **MailError** logging. In addition, the system can block outbound mail that fails SPF checks. This can avoid having Email Delivery suppress all recipients receiving email from an invalid sender and shift the responsibility for SPF validation to Transportation and Global Trade Management. If this feature is enabled, by opting in to the **APPLY SPF CHECKS TO OUTBOUND MAIL** optional feature, these blocks can be monitored via **MailError** logging.

Resolving Transportation and Global Trade Management Email Blocking

If emails are being blocked by Transportation and Global Trade Management, make sure you have successfully registered your From addresses as valid mail senders on the Mail Sender screen. If opting in to the **APPLY SPF CHECKS TO OUTBOUND MAIL**, make sure each mail sender has passed its SPF check.

Configuring an External SMTP Host

Oracle Transportation and Global Trade Management service supports customers configuring OTM to send email via their own SMTP server. Doing so alleviates the need to configure SPF/DKIM and the need to create an Approved Sender since the email. The disadvantage of this approach is that there is a greater change of instability because the email traffic is routed over the Public Internet. Transportation and Global Trade Management does not have an automatic retry capability with this approach, so intermittent connectivity issues with the external SMTP server will result in emails failing to deliver. Since this traffic traverses the Public Internet, only authenticated SMTP transport with TLS is supported on Port 587. This option is also only supported for the new Gen2 Oracle Cloud Infrastructure (OCI) environments.

In order to use this approach, you will first need to open a Service Request to request the outbound IP Address that will be the source of the mail traffic from the Transportation and Global Trade Management instance. You will need to whitelist the source IP address on your SMTP Server.

Once the whitelisting is complete, add the following properties to the CUSTOM Property Set.

- glog.mail.smtp.external.host
- glog.mail.smtp.external.port

For the "host" property, the value must use the following format:

```
[<user>][/{w<key>][@]<host>
```

where:

- `<user>` is the mail server user for authentication.
- `<key>` is a password wallet key that is used to store the mail server user's password in a wallet.
- `<host>` is the SMTP host name.

To set this property in the CUSTOM Property Set:

1. Choose a name for the password wallet key, i.e. "smtp.external".
2. Edit the CUSTOM Property Set and add a new property for the SMTP host using the password wallet key, i.e. "glog.mail.smtp.external.host=myuser/{wsmtp.external@host.<YOUR DOMAIN>.com".
3. Add a new property for the SMTP port, i.e. "glog.mail.smtp.external.port=587".
4. Save the property set.
5. Edit the CUSTOM Property Set again and add a new property where the key is your password wallet key and the value is your password, i.e. "smtp.external=PASSWORD".
6. Save the property set.

On the second save, the password will be properly stored in a wallet, and you should be able to start sending mail.

Note: It is very important that you follow the steps provided exactly. Make sure that you add the "glog.mail.smtp.external.host" property and save the property set before adding the "smtp.external" property. If you added both properties at the same time, it will not work correctly. If needed, delete these two properties and try again.

Managing Mail Quota

In order to prevent abhorrent behavior of one Cloud customer affecting the quality of service of other customers, it is necessary to limit the volume of email that can be sent by any Cloud instance. You can view the quota and current usage metrics in the Oracle Global Trade and Transportation Management user interface.

Configuration and Administration > Technical Support > Performance Collection

Select **Mail Quota** and click **Collect**.

The columns in the report with a "D" show the Daily volumes for the last 28 days.

It is important to understand that there are different types of quotas. There is an **Overall Quota**, an **Attachment Quota**, and a **Per Recipient Quota**.

- **Overall Quota**: Default Limit varies by Pod Size and is based on a rolling 24 hour period.
-
  - SMALL=35,000
  - MEDIUM=50,000
  - LARGE=100,000
- **Attachment Quota**: Default limit is 5,000 Emails with an Attachment in a rolling 24 hour period.

  Note: With 23B, the Emails with Attachments specific quota is removed.
- **Per Recipient Quota**: Default limit is 1,000 emails per hour to the same recipient.

Note: These are the default limits. With justification it is possible to request an increase in these limits by opening a Service Request with Oracle Support.

See the topics "Performance Collection" and "Performance Collection Types" in the online help for details.

Email Size Limitations

There are limits on the size of emails that can be sent from the Transportation and Global Trade Management service. For emails without attachments the default size limit is 2MB. For emails with attachments the limit is 5MB. Emails larger than these limits will still be sent, but the content/attachments will be converted to a link that the recipient can click on to retrieve the content.

For emails sent directly from BIPublisher, the email size is limited to 60MB.

Email Validation and Troubleshooting

The Mail Senders and Mail Validation user interfaces provide significant information for validating and troubleshooting issues with configuring the Email From Address. Please refer to the following Help Topics in the Oracle Transportation and Global Trade Management service for more detail on these topics.

- Mail Validation
- Mail Senders
- Mail Validation Troubleshooting

6 Configuring Oracle Analytics Server

Configuration

Business intelligence refers to the following optional product offerings:

- Transportation Intelligence (TI)
- Global Trade Intelligence (GTI)

TI and GTI business intelligence solutions are designed to enable strategic and tactical analysis of the various aspects of the trade and transportation business processes and to aid decision making.

Business intelligence solutions are developed using the Oracle Analytics Server (for the core analytics metadata and dashboard reports) and Oracle Data Integrator (for the core Extract, Transform, Load process) products. The following section provides some details on the configuration and use of these modules. For more information on these products, refer to the Transportation Intelligence and Global Trade Intelligence Reference Guide help topics.

The TI and GTI product options are disabled by default in the Cloud. By default the Extraction, Transformation, and Load (ETL) processes are disabled so the corresponding analytic database tables will be empty. You will receive the following warning if you click on one of the business intelligence Dashboard links "Business Intelligence is not currently licensed or installed on the server."

You will need to do the following in order to enable these product options. One or both of the following properties need to be set in order to enable the Oracle Analytics product options. Please refer to the Custom Properties section of this document for more detail on how to set properties. These properties should be set in the “CUSTOM” property set.

- TI property: ALLOW_ADVANCED_ANALYTICS=true
- GTI property: isAllowedGTIAnalytics=true

Once these properties are enabled the ETL will run automatically on a daily basis. The frequency of these ETLs is not configurable by the customer. In order to have visibility into the ETL process, the following property should be set. A summary of each ETL process will be sent to this email address when the process completes.

- `glog.odi.email.to.address=user@example.com`

It is possible to configure analytics using Oracle Analytics Server (OAS). The user interface for OAS is accessed via menu option **Transportation Intelligence > Administration**.

where `<servicename>` and `<identity-domain-name>` are the values that were specified during provisioning.

Users login OAS using the Transportation and Global Trade Management User ID/password.

> **Note:** Currently you must use the Transportation and Global Trade Management User ID (i.e. DBA.ADMIN), not the Transportation and Global Trade Management username. You also must first grant the User the BI Roles "BIAdministrators" and "BIAuthors". BI Roles are administrated using the Transportation and Global Trade Management User Manager. This page is located at **Configuration and Administration > User Management > User Manager**.

Note: Important! Before creating any reports or dashboards, you must create a catalog folder named "Custom" inside the existing "Shared Folders" folder. All reports and dashboards must be created inside this folder or a sub-folder. Defining reports and dashboards inside the “Custom” folder will ensure your customer-defined reports and dashboards are retained during future upgrades.

Enabling Fiscal Calendars

In order to enable fiscal calendars in the business intelligence applications, you must populate data in the AD_TIME table. Populate the AD_TIME table as follows:

- FISCAL_YEAR VARCHAR2(50)
- FISCAL_QUARTER_ID VARCHAR2(50)
- FISCAL_MONTH_ID VARCHAR2(50)
- FISCAL_WEEK_ID VARCHAR2(50)
- FISCAL_DAY VARCHAR2(50)

These columns correlate the calendar dates to fiscal dates. This data can be loaded using CSV files. For more details, see the "Using the CSV Utility to Import Data" help topic.

Global Currency Supported in TI and GTI

Oracle TI and GTI display reports in 3 different global currencies which are configured in OTM. Cost-related facts in the TRANSPORTATION INTELLIGENCE subject area contain 3 extra fields for each cost. You can use global currencies for the following analysis folders:

- Invoice Analysis
- Invoice Line Analysis
- Order Release Analysis
- Order Movement Analysis
- Shipment Analysis
- Shipment Line Analysis
- Shipment Order Release Analysis
- Shipment Order Release Line Analysis
- Tender Performance Analysis
- Bulk Plan Analysis
- Shipment Claim Analyis
- Rate Analysis

1. Configure 3 global currencies in OTM via the report common properties shown below. (Do not change 3 global currencies after the initial configuration as this might cause data discrepancy).
2. The exchange rates for the 3 global currencies are calculated as follows:
    a. Latest effective date is determined based on the shipment start time.
    b. The exchange rates for 3 global currencies are taken for the latest effective.

3. In the HDOWNER database, the fact tables for the analysis folders list above have 3 extra columns to hold global currencies' exchange rates.
4. The cost value for the global currency columns in each analysis folder is calculated as follows:
    a. Base cost * exchange rate of global currency.
    b. The multiplied amount is displayed for each of the global currency fields in each analysis folder.

Configure the following report common properties (**Business Process Automation > Power Data > Document Generation > Report Common Properties**):

Property	Default Value	Description
GLOBAL_CURRENCY1 **GLOBAL_CURRENCY2** **GLOBAL_CURRENCY2**		During installation in OTM, use these properties to configure three global currencies in which you would want to see the cost-based reports in TI. **Note:** Once these properties are set, it is recommended not to change the values.
EXCHANGE_RATE_GID	Default	Use this property to configure exchange rate in Oracle Transportation Management (OTM) to fetch exchange rates for objects (Bulk Plan, Order Release, Order Movement) that don't have SHIPMENT GID. These exchange rates will be used to display the global currency values in the cost-based reports.

Configuring Transportation Intelligence

Enabling Oracle Transportation Intelligence Agents in Oracle Transportation and Global Trade Management

The business objects in Oracle Transportation and Global Trade Management (like shipments, order releases, etc.) are loaded into the Transportation Intelligence tables when they have a status of READY_TO_LOAD. This status is set by automation agents in Oracle Transportation and Global Trade Management. To enable these automation agents, complete the following:

1. Log on to Oracle Transportation and Global Trade Management as DBA.ADMIN.
2. Go to **Business Process Automation > Agents and Milestones > Automation Agent**.
3. Search for and activate the following automation agents:
    - LOAD_ORDER_BASE_TO_HD (Default Event: Order base created)
    - LOAD_ORDER_RELEASE_TO_HD (Default Event: Order on shipment tendered)
    - LOAD_SHIPMENT_TO_HD (Default Event: Shipment tendered)

Unloading an Oracle Transportation and Global Trade Management Object from Transportation Intelligence

When an object is deleted from Oracle Transportation and Global Trade Management, it has to be removed from the Transportation Intelligence tables also. You need an agent that will automatically take care of deleting objects from TI tables when you delete the object in Transportation and Global Trade Management.

Automation gents need to be created for each object type in Oracle Transportation and Global Trade Management. To create an agent for SHIPMENT, perform the following steps:

1. Log onto Oracle Transportation and Global Trade Management as DBA.ADMIN
2. Go to **Business Process Automation > Agents and Milestones > Automation Agent**. Select **New.**
3. Select **Agent Type** as *SHIPMENT*.
4. Select **Agent Event** as *SHIPMENT-REMOVED* with restrictions of *INTEGRATION*, *INTERNAL*, or *USER*.
5. Add **Agent Action** as *UNLOAD SHIPMENT FROM HD*.
6. Give a suitable name for the Agent ID and save the agent.

Any shipments which are now deleted in Oracle Transportation and Global Trade Management will be deleted from the Transportation Intelligence tables when the subsequent ETL is triggered.

Such automation agents need to be created for every needed object in Oracle Transportation and Global Trade Management (like order release, order base etc.). The list of **agent actions** available in Oracle Transportation and Global Trade Management are:

- UNLOAD BULK PLAN FROM HD
- UNLOAD INVOICE FROM HD
- UNLOAD ORDER BASE FROM HD
- UNLOAD ORDER BASE LINE FROM HD
- UNLOAD ORDER BASE SHIP UNIT FROM HD
- UNLOAD ORDER ITEM FROM HD
- UNLOAD ORDER MOVEMENT FROM HD
- UNLOAD ORDER RELEASE FROM HD
- UNLOAD QUOTE FROM HD
- UNLOAD SELL SHIPMENT FROM HD
- UNLOAD SHIPMENT FROM HD

Mandatory Oracle Transportation and Global Trade Management User Role (VPD Profile) Configuration

VPD profile determines what data the user is entitled to see. All users of Oracle Transportation and Global Trade Management should have **one** of the following profile sets.

- **FTI_DEFAULT**: All users who **ARE NOT** service providers in Oracle Transportation and Global Trade Management should have this profile. Use this profile to access the Logistics Network Modeling Intelligence and Logistics Machine Learning subject areas.

- **SERVPROV**: All the users who are service providers in Oracle Transportation and Global Trade Management.

Performing this step is mandatory for the proper operational behavior of Transportation Intelligence application.

Configuring Global Trade Intelligence

Loading an Oracle Global Trade Management Object into Global Trade Intelligence

By default, the Global Trade Management objects supported by GTI are all loaded into GTI. Please see the “Data Flow to Global Trade Intelligence” help topic for complete details.

Mandatory Oracle Transportation and Global Trade Management User Role (VPD Profile) Configuration

VPD profile determines what data the user is entitled to see. All users of Global Trade Intelligence should have the following profile set:

- **GTI_DEFAULT**: All users of Oracle Global Trade Intelligence should have this profile.

Unloading a Global Trade Management Object from Global Trade Intelligence

You can unload (soft delete) data from the Global Trade Intelligence historical database (HD). When data is deleted from Transportation and Global Trade Management, you can mark that record as deleted in the Global Trade Intelligence HD. The record remains in the HD, but is it filtered out using the GTI_DEFAULT VPD profile.

There are several PUBLIC automation agents and agent actions intended for use with Global Trade Intelligence to enable this functionality. Please see the “Data Flow to Global Trade Intelligence” help topic for complete details.

Configuring Oracle Analytics Publisher Reporting

Configuration

Oracle Transportation and Global Trade Management provides several reports which can be run from the Report Manager. You also have the ability to create customer-defined Reports using Oracle Analytics Publisher. The user interface for creating and modifying reports is accessed via menu option Transportation Intelligence > Administration > Manage Publisher.

Users log into Oracle Analytics Publisher using the Transportation and Global Trade Management User ID/password. You must first grant the User the BI Roles “BIAdministrators” and “BIAuthors”. BI Roles are administrated using the Transportation and Global Trade Management User Manager. This page is located at **Configuration and Administration > User Management > User Manager**.

> **Note: Important!** All reports must be created inside "Custom" folder or a sub-folder. Defining reports inside the “Custom” folder will ensure your customer-defined Reports are retained during future upgrades.

In order to run a report from Transportation and Global Trade Management you will need to obtain the Oracle Analytics Publisher Report Path. The Report Path can be obtained from Oracle Analytics Publisher by viewing the report and clicking **Actions > Share Report Link > Current Page**. For example:

```
https://myservice-mydomain.otm.<data-center>.oraclecloud.com:9704/xmlpserver/ /Custom/my_pickup_summary/
my_pickup_summary.xdo
```

In this example, the relative Report Path is:

```
Custom/my_pickup_summary/my_pickup_summary.xdo
```

> **Note:** Prior to Transportation and Global Trade Management 6.4.1, it was necessary to include the host name in the report path. This is no longer necessary.

After a report is created in Oracle Analytics Publisher, it is necessary to define the report in Transportation and Global Trade Management. This page is located at **Business Process Automation > Power Data > Document Generation > Reports**. To configure a report to run the following options should be selected:

- Run on Third Party Report Server - Enabled
- Select via UI – Enabled
- Default Display Format - PDF
- Third Party Content Type - ‘Embedded’
- Report Path – The Relative Report Path obtained previously

In order for users to be able to run Oracle Analytics Publisher Reports, it is first necessary to grant the user the BI Role “BIConsumer”.

Oracle Analytics Publisher Reports are primarily built using SQL queries. However, a few utility PL/SQL functions are available for use in Reports. For more details on creating Reports, please refer to the Transportation and Global Trade Management Report Designer’s Guide.

Configuring the Email From Address

To configure a email From address in Oracle Analytics Publisher reporting, complete the following:

1. Create an approved sender email in Oracle Cloud Infrastructure. See the "*Managing Approved Senders*" topic in the Oracle Cloud Infrastructure online help.
2. Set up an Email Address as an Approved Sender in Oralce Transportation Management. Please refer the customer to the *Configuring Approved Senders* and *Configuring a Custom Domain* sections of this guide for more details.
3. Add the sender in Oracle Analytics Publisher as follows:
   a. Log into OTM as DBA.ADMIN.
   b. Go to **Transportation Intelligence > Administration**.
   c. Click **Manage Publisher**.
   d. Click **Delivery Configuration**.

e. On Delivery Configuration tab, enter the email address created in step 1 above for both the **Email From Address** and **Delivery Notification Email From**.

4. Add a new server in Oracle Analytics Publisher as follows:
   a. Click the **Email** tab.
   b. Click **Add Server**.
   c. Enter a **Server Name**, **Host (SMTP)**, **Port**, **Username**, and **Password**.
   d. Set the "Access Control" to **Public**.
   e. Verify the connection by clicking **Test Connection**.
   f. Then click **Apply** to save your changes.

Report Permissions

By default, reports can only be run by the user that created the report in Oracle Analytics Publisher. In order to run reports from within Transportation and Global Trade Management, the permissions for the report must be set for the “BI Consumer Role”. Report permissions can only be set using OAS. The user interface for OAS is accessed via the following URL.`https://<servicename>-<identity-domain-name>.otm.<data-center>.oraclecloud.com/analytics/`

where <servicename> and <identity-domain-name> are the values that were specified during provisioning.

Please use the following steps to set permissions after creating customer-defined Reports.

1. After you log into to OAS, click on the **Catalog** link in the menu.
2. Click on the **Custom** link in the “Shared Folders” section of the catalog.
3. Click the **Permissions** icon on the “Tasks” menu.
4. Select the “BI Consumer Role” and choose “Full Control” for the “Permissions”.
5. Check “Apply permissions to sub-folders.” and “Apply permissions to items within folder.”
6. Click “OK”.

Report Distribution

Report Scheduling and Distribution via Oracle Analytics Publisher is not supported. Scheduled jobs in Oracle Analytics Publisher will not be preserved during upgrades. Report Scheduling and Distribution must be performed using the Transportation and Global Trade Management Notification capabilities. For more details on this topic, please refer to the “About Report Emails” Help topic.

7 IPP Printing

Introduction to IPP Printing

Transportation and Global Trade Management Cloud supports the printing of reports to an Internet Printing Protocol (IPP) compliant printer with specific support for a Common UNIX Printing System (CUPS) printer.

Set up a Printer for Oracle Cloud

When setting up an on-site printer, please note that the printer must meet the following prerequisites.

- The printer must support printing over the internet for which there are two options:
  - The printer is IPP (Internet Printing Protocol) enabled i.e. it natively supports printing over the internet.
  - If the printer doesn't support printing over the internet which can be the case for older printers, you need to set up an IPP print server at your location. Examples of IPP printer servers are CUPS (Common UNIX Printing System) and Windows IPP Print Server. For information on setting up CUPS or Windows IPP print servers and connecting network printers to them, refer to the CUPS or Windows IPP software vendor documentation.

    > **Note:** It is strongly recommended that a print server (CUPS or Windows) be used instead of connecting directly to the printer. This type of setup ensures that the printer is IPP enabled and that it can accept and process cloud-based print requests. A print server also allows for easier debugging through the availability of server level logs.

    > **Note:** CUPS refers to setting up a CUPS print server on site at your facility as a gateway to a printer. We use the CUPS print server URL to configure that printer in Oracle Business Intelligence Publisher (BI Publisher). It does not refer to setting up a CUPS server within BI Publisher which is no longer supported as of Release 9 (see *Doc ID 2089912.1*).

- The print server must present a valid SSL certificate signed by a trusted CA (Certificate Authority) such as GoDaddy, Verisign etc. Self-signed SSL certificates are NOT supported.
- The on-site printer must be accessible from the Oracle Public Cloud via the internet over a secure connection. If there is a firewall that is protecting customer internal servers, then a firewall policy/rule needs to be configured to allow incoming traffic to the onsite print server. For list of trusted Oracle IP addresses to add to the allowlist for your firewall, please open a Support Request.
- The print server host must be registered with the McAfee Site Address Filter. Please review the Trusted URL Registration section of the Oracle Logistics Cloud Getting Started Guide for more details.
- The printer should be set up with the authentication option enabled.
- The printer should be using either Basic or Digest authentication schemes. NTLM is currently not supported.

Configure a Printer in Oracle Analytics Publisher

This section lists the steps required to enable IPP printing either through a printer running from a CUPS server or directly via IPP.

If you are going to use a printer running through CUPS, your system administrator needs to add the printer to the CUPS server. Once your CUPS printer is set up, complete the following:

Log into the Oracle Analytics Publisher console.

1. Click **Sign In**.
2. Click **Administration**.
3. Click the **Printer** tab.
4. Click **Add Server**.

   For a CUPS or direct IPP printer:
5. Enter the **Server Name**. You will need to enter this into Transportation and Global Trade Management Cloud later, so make note of it.
6. Enter the URI for your server. For CUPS the form is `ipp://<CUPS host>:631/printers/<printer name>`.

   IPP uses the TCP port 631 for printing, so any firewalls between the client and the server must be configured to allow bi-directional traffic on that port. Please consult your network administrator if you think any configuration changes are necessary.
7. Check with your system administrator for any Filter requirements.
8. It is required to use SSL Encryption. Select **SSL** for the **Encryption Type** in the Security section.
9. It is also required to protect the Printer/Print Server using User Authentication. Please enter the corresponding details in the **Username**, **Password**, and **Authentication Type** fields. The **Authentication Type** must be **Basic** or **Digest**.
10. Click **Apply**.

A Direct IPP printer is set up the same way except for one difference. Instead of going through the CUPS server, you set up the URI to point to the server and IPP port directly. The URI would be entered in the following format, `ipp://<PRINTER_FQDN>:631`.

Print from Oracle Analytics Publisher

To ensure Oracle Analytics Publisher functionality, you can print a test page with your printers.

1. Click **Home > Report Job > Search**.
2. Click the **+** sign next to **Reports**.
3. Double click **domestic_packing_list**.
4. Highlight the **domestic_packing_list report**.
5. Click **Open**.
6. Select the **Output** tab.
7. Click the **Add Destination** button.
8. Select a printer. You can select all your printers by clicking the **Add Destination** button an appropriate number of times.
9. Click the **Schedule** button. Ensure the Frequency is correct, in this case “Once”.

10. Select **Run Now**.
11. Click **Submit**.
12. In the **Submit** pop-up, enter a **Report Job Name**.
13. Click **OK**.
14. Go to your physical printer and ensure that your jobs were printed.
15. Sign out of the Oracle Analytics Publisher console.

Configure Printer in OTM/GTM Cloud

After confirming that printing is working from within Oracle Analytics Publisher, you need to configure Transportation and Global Trade Management Cloud to use the printer defined in Oracle Analytics Publisher.

1. Navigate to **Business Process Automation > Power Data > Document Generation > Printers**.
2. Click **New**.
3. Enter the following:
    a. **Printer ID**: A printer ID
    b. **Printer Name**: The server name you gave your printer when you set up the printer in Oracle Analytics Publisher.
4. No other fields are necessary. The system uses the following fields if specified: Orientation, Sides, Number of Copies, and Media.
5. Click **Finished**. Repeat for as many printers as you have set up in Oracle Analytics Publisher.

Print from OTM/GTM Cloud

You have two options when print from the OTM/GTM Cloud.

- Option 1: Use the Send Content action from the Document Manager.
- Option 2: Use pre-packaged reports and send them to a printer.

Option 1

1. Navigate to **Business Process Automation > Document Manager**.
2. Click **Search**.
3. Select the check box next to a document.
4. Click **Actions > Send Content**.
5. In the Printers grid, enter your printer(s).
6. Click **Save**.
7. Click **Submit**.

   You should get a Confirmation dialog box.

Option 2

1. Navigate to **Shipment Management > Shipment Management > Buy Shipments**.
2. Click **Search**.

3. Select the check box next to a shipment.
4. Click **Actions > Business Process Administration > Reports > Domestic Packing List**.
5. Enter the following:
    a. **Report Format**: *PDF*
    b. **Delivery Method**: *Print*
    c. **Printer ID**
6. Click **Submit**.

    You should get an Information screen saying, “The report print request has been submitted to <YOUR_PRINTER>”.

Print Logging

This section details how to turn on and view print logging as follows.

Enable Logging

You can turn on some printing logging as follows:

1. Navigate to **Configuration and Administration > Power Data > General > Log Files**.
2. Select a **Type** of *System*.
3. Click **Search**.
4. Edit the SYSTEM log.

    > **Note:** To edit the SYSTEM log you must be logged into Transportation and Global Trade Management Cloud as DBA.ADMIN.

5. Add the following log IDs to the SYSTEM log:
    - Print
    - PrintDebug
    - PrintDetails
6. Click **Finished**.

View Logging

1. Open any Process Management screen. For example, Shipment Management > Process Management.
2. Under Logs, click **System**.
3. In the **From** field, change the time to when you submitted the first print job.
4. In the **Log** field, select *SYSTEM*.
5. In the **Severities** field, leave the default setting.
6. Select the following IDs:
    - Print
    - Print Debug
    - PrintDetails
7. Leave the **Top Level Process** field blank.

8. Click **View Results**.

You should see something like the following:

```
Debug Print Sending print: Domestic Packing List to <YOUR_PRINTER> (<#>) [transport - IPP - 1]
Debug PrintDebug File to print /middleware/app/otm641/otm/temp/prt714623267893139703.pdf [transport - IPP -
 1]
Debug PrintDebug BIP Print Service URL: http://pod-primary-1.otmgtm-cloud.oracle.com:8704/xmlpserver/
services/v2/ScheduleService [transport - IPP - 1]
Debug PrintDebug BIP Print Soap Request:
Debug PrintDebug BIP Print Soap Response:
Debug Print Print successful: Domestic Packing List to <YOUR_PRINTER> (<#>) [transport - IPP - 1]
```

Debugging Using CUPS Print Server

It is highly recommended to use a CUPS printer server. Using a print server will make it easier to diagnose issues since you can view the status of the printer and printer jobs.

1. Log into the printer server host.
2. Click the **Printers** tab.

   You will see a list of CUPS printers and ancillary information. Look for the “Status”.
3. Click on your printer in the queue **Name** column.
4. Click **Show Active Jobs**.
5. Scroll to the bottom of the page, and you should see a job “spooling”.

If your job spools it is in the printer queue which indicates that your job has been recognized and is being processed.

IPP Printing FAQ

Is there an alternative means of printing reports, documents, etc.?

Yes. Reports can be viewed and printed on a local printing using a web browser.

What is the standard Protocol for printing directly from the Oracle Logistics Cloud?

IPP over HTTPS.

Does direct printing from the Oracle Logistics Cloud require an SSL certificate from a Certification Authority?

Yes, the print server must present a valid SSL certificate signed by a trusted certificate authority such as GoDaddy.

Can a self-signed SSL certificate be used, rather than a certificate from a Certification Authority?

No. Self-signed certificates are not supported.

Can the print server be the printer itself, or, must a print server be, for example, a CUPS (Common UNIX Printing System) server?

The IPP print server can be the printer itself. Newer printers already have built in IPP over HTTPS support. Consult the printer’s user guide for specific setup requirements and availability.

If the printer does not natively support IPP over HTTPS, then a CUPS server (or print server that supports IPP over HTTPS) can be used. For CUPS (or similar) based setup, Oracle Analytics Publisher will connect to the print server, and

then the print server would connect to the printer. All required setups will need to be completed and tested by Cloud customers.

Is it mandatory to use SSL and client authentication?

Yes. For cloud customers, those are enforced by default and should not be modified by the customer.

How to test that my printer is working?

You can run any report and redirect the print output to the newly setup printer. If the job completes successfully and the printer receives the print request then the setup is good.

Can we use client side certificate instead of username/password for cloud printer authentication?

No. Supported authentication methods are basic or digest both of which use username/password.

Are there any troubleshooting tips in case the print request doesn't go through?

Review and make sure the prerequisite steps are followed.

Verify the print server logs to check if it received the print request. Refer the IPP print server, CUPS or Windows IPP software vendor documentation for more details on where to find the logs.

In case you are still unable to receive the print requests on the print server from Oracle cloud, please log an SR to engage Oracle Support in debugging any setup issues on Oracle cloud. When logging the SR, please provide the following details:

- Screen shot of print server setup in Oracle Analytics Publisher
- Complete printer URL

8 Complementary Products

Oracle Transportation Mobile Web Application

Oracle Transportation and Global Trade Management integrates with Oracle Transportation Mobile Web Application, a mobile web application. For more information on how to configure Oracle Transportation and Global Trade Management to work with the Oracle Transportation Mobile Web Application, see the **About Mobile Applications** in the online help on the *Oracle Help Center*.

Pre-Built Integrations

Oracle Transportation and Global Trade Management includes pre-built integrations to optional components for Geo-coding, Distance, and Rate Calculation. The following section provides information on configuring Oracle Transportation and Global Trade Management to use these products. It is your responsibility to contact the corresponding vendor for additional details on their product offerings and corresponding license agreements.

Geo-coding and External Distance/Time

Geo-coding a location refers to setting the latitude and longitude (lat/lon) coordinates on the location. The lat/lon is necessary for displaying locations on a map. Oracle Transportation and Global Trade Management has two methods for geo-coding a location. One option is to configure an external distance engine. The other option is to load data into the geo_postal_point or geo_cityprov_point tables.

Oracle Maps Cloud

Oracle Maps Cloud is available as an external distance engine. In order to use the Oracle Maps Cloud External Distance Engine, configure the following properties:

- `OracleSpatial.host=elocation.oracle.com`
- `OracleSpatial.port=7777`

> **Note:** The "glog.ExternalDistanceEngine.OracleSpatialEngine.protocol" is set to "https" by default and should not be modified. For more details on configuring Oracle Maps Cloud, see the "External Distance Engines" help topic.

PC Miler Web Service

PC Miler Web Service is an external distance engine which can be used for geo-coding and distance calculation. Oracle Transportation and Global Trade Management can be configured to use the PC Miler Service for distance and time calculation. Before you can use PC Miler Web service, you must set the corresponding ExternalDistanceEngine

Properties. In order to use the PCMiler web services, you will need to obtain a license key from ALK and set the following property:

- **glog.ExternalDistanceEngine.PCMilerWS.AuthorizationKey**

This property should be added to the CUSTOM Property Set. Refer to the "Property Sets" section of this document for information on how to set properties.

> **Note:** The "glog.ExternalDistanceEngine.PCMilerWS.WCFWebserviceWSDLUrl" property is set by default and should not be changed. For more details, see the "Configuring PCMiler Web Services" help topic.

ALK Technologies, Inc.: *http://www.alk.com/*

PC Miler Rail Web Service

PC Miler Rail Web Service is an external distance engine that can be used for distance calculation for rail. Oracle Transportation and Global Trade Management can be configured to use the PC Miler Rail Service for distance calculation between Rail Stations or SPLCs or City Province. Before you can use PC Miler Rail Web service, you must set the corresponding ExternalDistanceEngine Properties. In order to use the PC Miler Rail web services, you will need to obtain a license key from ALK and set the following property:
glog.ExternalDistanceEngine.PCMilerRailWS.AuthorizationKey

This property should be added to the CUSTOM Property Set. Refer to the “Property Sets” section of this document for information on how to set properties.

> **Note:** The "glog.ExternalDistanceEngine.PCMilerRailWS.WsdlUrl" property is set by default and should not be changed. For more details, see the "Configuring PC*MILER RAIL Web Services" help topic.

ALK Technologies, Inc.: *http://www.alk.com/*

HERE

HERE is an external distance engine which can be used for geo-coding, distance and time calculation. Before you can use HERE REST API, you must set these HERE properties.

You will need to specify authentication credentials through properties defined below:

- **here.app_id**
- **here.app_code**

You will need to specify geo-coding URL through properties defined below:

here.geocode.host=http://geocoder.api.here.com/6.2/geocode.xml

You will need to specify routing URL for distance and time calculation through properties defined below:

here.route.host=https://route.api.here.com/routing/7.2/calculateroute.xml

This property should be added to the CUSTOM Property Set. Refer to the “Property Sets” section of this document for information on how to set properties.

HERE: *https://www.here.com/strategic-alliances/oracle*

External Rating

SMC RateWareXL with Carrier Connect Web Service

Oracle Transportation and Global Trade Management can be configured to use the RateWareXL with Carrier Connect Service hosted by SMC. This web service provides a call to get rates and transit time. The following properties are used to configure the Rating engine to use this service.

- **`glog.RatingEngine.RatewareXL.Username=`**
- **`glog.RatingEngine.RatewareXL.Password=`**
- **`glog.RatingEngine.RatewareXL.License=`**

These properties should be added to the CUSTOM Property Set. Refer to the “Property Sets” section of this document for information on how to set properties.

> **Note:** The "glog.RatingEngine.RatewareXL.Wsdl.URL" [property is set by default and should not be modified. For more information on this topic, refer to "How to Set Up an SMC Rate" in online help.

SMC3: *http://www.smc3.com/*

Maps

By default, Oracle Transportation and Global Trade Management maps use workbench maps as follows:

- PUBLIC workbench layouts which may include:
  - Dispatch Board (Fleet Management > Dispatch Board)
  - Network Workbench (Shipment Management > Itinerary Management > Network Workbench)
  - Planning Workbench (Operational Planning > Planning Workbench)
- Mapping actions available on the order release, shipment, location, and operational planning Managers use workbench maps including:
  - Map Bulk Plan Results
  - Map Fleet Bulk Plan Results
  - Map Inbound Shipments
  - Map Order Releases
  - Map Outbound Shipments
  - Map Shipments
- All user-created workbench layouts that contains a map component. A workbench is a type of screen that allows you to create multi-panel layouts containing tables, maps, and Gantt charts. Layouts define the look and feel of a workbench. Each layout can have multiple regions, with each region displaying different,

but related, information. The workbench designer allows you to create and edit workbench layouts. The workbench supports the following vendors. This page is accessed via **Configuration and Administration > User Configuration > Workbench Designer**.

See the "About Workbench Layouts" help topic for more details.

You can integrate Oracle Transportation and Global Trade Management with HERE Platform for Business, ALK Maps, or Oracle Map Cloud Services (formerly eLocation) by setting the properties mentioned in the rest of this section. These additional properties are not configured by the installer. On your existing Oracle Transportation and Global Trade Management installation, adding the following properties using the Property Set Manager. See Section 0 for more information on property sets.

HERE

After acquiring a version 3.1 map licensing from HERE, the following properties need to be set in order to enable this feature:

Property	Description
here.api_key	Contains the API key generated by HERE.
here.core_url	Set to https://js.api.here.com/v3/3.1/mapsjs-core.js
here.core_legacy_url	Set to https://js.api.here.com/v3/3.1/mapsjs-core-legacy.js
here.css_url	Set to https://js.api.here.com/v3/3.1/mapsjs-ui.css
here.event_url	Set to https://js.api.here.com/v3/3.1/mapsjs-mapevents.js
here.service_legacy_url	Set to https://js.api.here.com/v3/3.1/mapsjs-service-legacy.js
here.service_url	Set to https://js.api.here.com/v3/3.1/mapsjs-service.js
here.ui_url	Set to https://js.api.here.com/v3/3.1/mapsjs-ui.js
here.useLatestApi	Set to true.

HERE: *https://company.here.com/here/*

ALK

After acquiring map licensing from ALK, the following property needs to be set in order to enable this feature:`alk.api_key=`

ALK Technologies, Inc.: *http://www.alk.com/*

Oracle Maps Cloud

After acquiring map licensing from Oracle Maps Cloud, the following properties need to be set in order to enable this feature:

```
elocation.mapviewer_url=
elocation.elocation_url=
```

Note: All customers may use the following to configure Oracle Maps Cloud.

Oracle Maps Cloud: *https://www.oracle.com/middleware/technologies/ofm-mapviewer.html*

Business to Business Connectivity

Carrier Integration

Oracle Transportation and Global Trade Management supports communication with carriers via the Carrier Portal, which is a UI that can be exposed to external users for the purpose of reviewing and accepting or rejecting shipment tenders, providing shipment status information, submitting invoices, and more. Alternatively, Oracle Transportation and Global Trade Management also supports integration with carriers in the same way as other external systems, as described in the “Integrating with Other Systems” section of this document.

Customers who transact with a large number of carriers may wish to consider a B2B connectivity partner to manage the integration process with each individual carrier. Most B2B providers are capable of providing such services, though the partners identified below have created turn-key solutions specifically for Oracle Transportation and Global Trade Management customers. Please note that Oracle does not offer packaged integration with any of these partners. Rather, it is the B2B providers who own and support these integrations. Thus it is the responsibility of the customer to perform due diligence and identify whether such a solution is needed and which partner solution best fits their organization’s requirements.

SPS Commerce (*http://www.spscommerce.com/*) offers pre-mapped Transportation and Global Trade Management XML to EDI messages for the shipment tender, tender response, shipment status, and invoice transactions. Their offering includes professional services for all carrier on-boarding and testing activities. SPS Commerce is based in Minneapolis, MN and has offices in ANZ, APAC, and EMEA. For more information, contact *mailto:info@spscommerce.com*.

Justransform (*http://www.justransform.com/*) is a cloud-based, self-service integration platform. Their solution includes packaged maps for all supported Transportation and Global Trade Management versions to/from applicable transactions in all available versions of EDI X12 and EDIFACT, as well as many other integration capabilities. Justransform is based in Cupertino, CA. For more information, contact *mailto:support@justransform.com*.

Transporeon (*http://www.transporeon.com/*) offers pre-mapped Transportation and Global Trade Management XML to EDI messages for the shipment tender, tender, response, shipments status, and invoice transactions. Their offering includes professional services for all carrier on-boarding and testing activities. Transporeon is based in Ulm, Germany and has offices throughout EMEA and in North America. For more information, contact *mailto:info@transporeon.com*.

Global Trade Management

Global Trade Content

Global trade practice requires companies to have access to and utilize the current trade data available. There are many types of trade data available with various sources, both nationally and internationally. Failure to utilize the most up-to-date data can result in inaccurate screenings which may lead to significant fines and penalties, delays, revocation of trade privileges, and lost revenues. Examples of trade content include, but are not limited to:

- Denied Party Screening Lists
- Harmonized System and Classification Information
- Tariff and Duty Rates
- Binding Rules and Regulations
- Free Trade Agreement Information

Global Trade Management provides an integration solution for automatically downloading much of this data directly from *Descartes*. For more information on this topic, please refer to “Global Trade Content” in on-line Help.

Customs Filing

U.S. export shipments require an export declaration to be filed with the U.S. Census. The export declaration is represented as EEI (Electronic Export Information) and is filed with the U.S. Census. The Oracle Global Trade Cloud Service supports filing with U.S. Customs and Border Protection’s (CBP) Automated Export System (AES) interface via Descarte’s Global Logistics Network (GLN) system. For more details on this topic, please refer to the Filing with AES via Descartes’s GLN System section in the Customs Filing Integration Guide.

9 Integration

Integrating with Other Systems

Integration to/from Oracle Transportation and Global Trade Management is accomplished via XML or JSON documents. In the Oracle Public Cloud, all inbound and outbound integration is transferred via XML or JSON documents, transported over HTTPS. The XML content may optionally be contained in a SOAP Web service request.

Inbound and Outbound Integration via Transmissions are only supported with the HTTP protocol, including REST and SOAP Web Services. There is no support for FTP, Direct Database, or Oracle Advanced Queues (OAQ).

Inbound Integration

Sending data to Oracle Transportation and Global Trade Management is supported using one of the following methods:

- HTTP POST
- REST JSON (See REST API section)
- SOAP Web Services.

HTTPPOST

HTTPPOST integration is achieved by posting XML documents to the following URL: `https://<servicename>-<identity-domain-name>.otm.<data-center>.oraclecloud.com/GC3/<servlet endpoint>`

The `<servicename>` and `<identity-domain-name>` values should be replaced with the values that were specified during provisioning. For example: See the **Input Provided During Provisioning** and **Resulting URLs** sections.

Refer to the *Cloud Integration Guide* for a description on the supported servlet endpoints and their corresponding use cases.

Input Provided During Provisioning

- **Service Name**: myotm
- **Identity Domain Name**: companyname

Resulting URLs

- https://myotm-companyname.otm.<data-center>.oraclecloud.com/GC3/glog.integration.servlet.WMServlet
- https://myotm-test-companyname.otm.<data-center>.oraclecloud.com/GC3/glog.integration.servlet.WMServlet

If a specific port number is required by the upstream posting system, the port that should be used is 443. For proper security, the downstream system should require a username/password for user authentication. When the username

and password fields are specified on an External System, they are automatically added to the Transmission Header in the generated XML document.

SOAP Web Services

You can also send data to Oracle Transportation and Global Trade Management via a SOAP web service call.

The web service call can be generated using the WSDL URL. The following URL is for the TransmissionService:

- `https://<servicename>-<identity-domain-name>.otm.<data-center>.oraclecloud.com/GC3Services/TransmissionService/call?wsdl`

The `<servicename>` and `<identity-domain-name>` values should be replaced with the values that were specified during provisioning.

Input Provided During Provisioning

- **Service Name**: myotm
- **Identity Domain Name**: companyname
- **Data Center Name**: us1

Resulting URLs:

- https://myotm-companyname.otm.us1.oraclecloud.com/GC3Services/TransmissionService/call?wsdl
- https://myotm-test-companyname.otm.us1.oraclecloud.com/GC3Services/TransmissionService/call?wsdl

Alternatively, the WSDL file and corresponding XSD schema files can be retrieved via **Process Automation > Integration > Integration Manager > Retrieve WSDLs**. The WSDL should be saved to a file and subsequently imported into the source system.

Transportation and Global Trade Management enforces Web Service Security policies on all inbound and outbound Web Services. The Web Service Security Specification is an OASIS standard for defining security related information as part of a SOAP message. See *http://www.oasis-open.org/*. In the Oracle Public Cloud, Transportation and Global Trade Management only supports the WS-Security Username Token Profile.

Inbound

For Inbound integration, the username and password must be specified in the SOAP Header of the XML document. Please refer to the example below:

```
<SOAP-ENV:Header>
<Security xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
<UsernameToken>
<Username>XYZ.OTMUSER</Username>
<Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-
profile-1.0#PasswordText">password</Password>
</UsernameToken>
</Security>
</SOAP-ENV:Header>
```

Integration User Role

In order to send data to Oracle Transportation and Global Trade Management, it is necessary for the remote system to authenticate with valid user credentials. In addition this user must have the correct Access Control List entry points. To facilitate this, Oracle Transportation and Global Trade Management provides by default the following options for inbound integration users:

- 'INTEGRATION' user role for your inbound integration users. Assign this user role to your user.
- 'INTEGRATION' ACL for your inbound integration users. Assign this parent ACL to your customer-defined user role or your user.
- 'External Integration' ACL for your inbound integration users. Assign this child ACL to your customer-defined user role or your user.

Inbound Integration and SSL Certificates

All inbound integration requires that the transport be protected using HTTPS. Communications over HTTPS are encrypted using SSL. These SSL communications are initiated using SSL Certificates. The SSL Certificates must be from a trusted signing authority (no self-signed certificates). It is possible that the list of trusted signing authorities on the system does not contain the signing authority used for the Oracle Public Cloud certificates. In that case it may be necessary to download and install the Certificate in the source system.

The following instructions explain how to obtain the Root and Intermediate Certificate for an Oracle Transportation and Global Trade Management instance. Both the Root and Intermediate Certificates must be imported in order to prevent issues when the Certificate expires each year. You should install the root and intermediate certificate only, NOT the complete certificate chain. The instructions below assume the use of the Firefox web browser, but the steps will be similar with other browsers.

First you have to identify the type of cloud server on which your service is provisioned, as described in the *Getting Started Guide*, as the instructions vary for Oracle Generation 2 Cloud Infrastructure (Gen2) and legacy Oracle Public Cloud (OPC).

Oracle Generation 2 Cloud Infrastructure (Gen2)

For Gen2, follow these instructions to retrieve the SSL certificate:

1. Open the Firefox browser and log into your instance. You must ensure you are logged in successfully to the Oracle Transportation and Global Trade Management application otherwise you will be downloading the Identity Cloud Service certificates.
2. After confirming you are successfully logged into Oracle Transportation and Global Trade Management, click on the **padlock** (lock symbol) next to the URL.
3. Click the arrow next to **Connection Secure** to show connection details, then click the **More Information** option at the bottom of the window.
4. Under the **Security** tab, click the **View Certificate** button.
5. There will be 3 tabs, one for the **Site Certificate**, the **Intermediate Certificate**, and **Root Certificate**. You must export both the Root and Intermediate certificates and import them into your keystore in order to recognize the OTM certificate. It is NOT necessary to install the site certificate. If you install the site certificate you will need to update this at every yearly certificate renewal.
6. Select the intermediate certificate "DigiCert Global CA G2" and then click on the "Download PEM (CERT)" hyperlink. This should prompt you to save the file. You must remember the location where you saved the files.

7. Repeat the above step 6 for the root certificate "DigiCert Global Root G2".
8. Import both the root and intermediate certificates into the sending system keystore to recognize the OTM certificate by application using the keystore.
9. To confirm installation check your local copy of "keystores" on the source system making the calls to make sure that the intermediate and root certs are present.

For more details on this topic, please refer to the following My Oracle Support Note:

- *OTM/GTM Gen2 OCI: How to Retrieve Security Certificates for Inbound Integration using Firefox (Doc ID 2905156.1)*

Oracle Public Cloud (OPC)

For OPC follow these instructions to retrieve the SSL certificate:

1. Open the Firefox browser and type in the URL *https://otmcertificate.otm.us2.oraclecloud.com/*.
2. Click on the padlock (lock symbol) next to the URL.
3. Click the arrow next to "**Connection Secure**" to show connection details, then click the **More Information** option at the bottom of the window.
4. Under the **Security** tab, click the **View Certificate** button.
5. There will be 3 tabs, one for the Site Certificate, the Intermediate Certificate, and Root Certificate. You must export both the Root and Intermediate certificates and import them into your keystore in order to recognize the OTM certificate. It is NOT necessary to install the site certificate. If you install the site certificate you will need to update this at every yearly certificate renewal.
6. Select the intermediate certificate "DigiCert TLS RSA SHA256 2020 CA1" and then click on the "Download PEM (CERT)" hyperlink. This should prompt you to save the file. You must remember the location where you saved the files.
7. Repeat the above step 6 for the root certificate "DigiCert Global Root CA".
8. Import both the root and intermediate certificates into the sending system keystore to recognize the OTM certificate by application using the keystore.
9. To confirm installation check your local copy of "keystores" on the source system making the calls to make sure that the intermediate and root certs are present.
10. Import both root and intermediate certificates into keystore to recognize Transportation and Global Trade Management certificate by application using the keystore. All the above steps mentioned are for the customer PODS in US2 data center. For the other data centers please follow the same steps as above. The URL to enter is different for different data centers:
    - https://otmcertificate.otm.em2.oraclecloud.com
    - https://otmcertificate.otm.em3.oraclecloud.com
    - https://otmcertificate.otm.us6.oraclecloud.com

    For more details, refer to the following My Oracle Support (MOS) Note:
    - *OTM/GTM Gen1 OPC: How to Retrieve Security Certificates for Inbound Integration using Firefox (Doc ID 2105818.1)*

Note: For Inbound Integration which uses the Oracle E-Business Suite – GTM ITM Adapter, refer to the following MOS Note for details on how to handle SSL Certificates: *How to Retrieve and Change Security Certificates for Inbound Integration to GTM from EBS ITM (Doc ID 2455210.1)*. In order to avoid an interruption of service when the Certificate is renewed, you will need to open a Service Request to obtain the latest SSL Certificate from Oracle a month prior to when the current Certificate will expire.

Integration Data Queues

It is important to note that in the Cloud service all Inbound integration utilizes the Integration Data Queue feature. This feature persists all inbound Transmissions into a database table. A polling process on the application server queries the corresponding table and processes Transmissions in batches. The Cloud Service is configured by default to have 4 polling threads with a batch size of 8, that poll every 2 seconds. This allows for a maximum throughput of 57,600 Transmissions per hour. You can change these settings using the Data Queue manager, available on the menu at **Business Process Automation > Integration > Data Queues**. The "INTEGRATION IN" Data Queue controls the processing of Inbound Integration.

The Integration Data Queue feature prevents the application server from being overwhelmed by a peak in integration volume. Customers can increase the inbound integration throughput by adjusting this configuration. However, the risk is that unnecessarily increasing the throughput could negatively affect the performance of other parts of the system. For more details on this topic, please refer to the Integration Guide. It is important to note though that the configuration of the Integration Data Queue feature is limited.

Trusted URL Registration

All web traffic out of the Oracle Public Cloud is verified using a McAfee Site Address filter. This applies to outbound integration as well as IPP Printing. Customers need to verify their outbound URL site's reputation at the following site.

https://sitelookup.mcafee.com/

Oracle recommends selecting the product “McAfee Web Gateway v7.x/6.9.x (resident).” If the URL is not trusted, the owner of the URL should submit a request to add the URL with the proper business category on the McAfee feedback site. Once the URL has been added to proper business category it will be allowed as per OPC URL filter policy.

McAfee® provides an online tool that enables you to check if a site is categorized within various versions of the SmartFilter Internet Database or the Webwasher URL Filter Database. After you check a URL, this tool also allows you to suggest an alternative categorization for a site. These requests will be addressed within an average of 3-5 business days with some requests requiring additional review and taking longer.

Please email *mailto:sites@mcafee.com*if you have any issues with this site.

XSL Stylesheets for Inbound Integration

Oracle Transportation and Global Trade Management service supports the ability to transform XML Documents during Inbound Transmission Processing. This capability is supported using the TransformerServlet. Use the following steps to load your customer-defined XSL files for Inbound Integration.

1. Create Stylesheet Content: Create a Stylesheet Content record and upload the corresponding XSL file. This page is located at **Business Process Automation > Power Data > Event Management > Stylesheet Content**.
2. Set the stylesheet_name attribute in your XML file to the Stylesheet Content GID: `<?gc3-int-translate stylesheet_name="db:GUEST.MYSTYLESHEETCONTENTGID"?>`

Note: For more detail on this topic, please refer to the "Transform Inbound XML with XSL" section in the *Transportation and Global Trade Management Integration Guide* .

REST API

Transportation and Global Trade Management provides multiple public REST APIs that can be used to access data stored in Transportation and Global Trade Management and construct integrations to other systems. You can make many types of HTTP requests using Oracle REST APIs. You can easily make requests to view, create, update, or delete records.

Where possible a REST API should be used in preference to the Transmission XML via SOAP or HTTP. REST supports synchronous and asynchronous messaging for almost all resources which is an expansion of the Transmission XML capabilities. However, REST does not yet support all the capabilities available using Transmission XML and these capabilities will be added over the next few updates to the REST API. In cases where the feature is not yet available the Transmission XML message must be used.

For detailed instructions on how to use REST APIs, see the *REST API for Transportation and Global Trade Management guide*.

OAuth Client Credentials Flow

The inbound HTTP POST and REST interfaces also support authentication and authorization using OAuth in addition to HTTP Basic Authentication. See the *Cloud Integration Guide* for configuration details.

Outbound Integration and Notification

Outbound Integration from Oracle Transportation and Global Trade Management is supported using HTTPPOST and Web Services. In either case an External System is created to define the target system for the integration. Please refer the Integration Guide for more details on this subject.

Web Services

You can send data from Oracle Transportation and Global Trade Management via a web service call. For proper security, the downstream system used in outbound integration should require a username and password for user authentication. If the downstream system uses the WS-Security Username Token Policy, the username and password should be specified when creating the Web Service EndPoint.

OutXMLProfile for Outbound Integration and Notification

Out XML Profiles allow you to generate outbound XML and exclude portions of outbound XML with a high degree of control. This is done by specifying what XML builder class files should be excluded when generating XML documents or by selecting an XML template on which you can base the outbound XML. Outbound XML includes integration and notification. Unnecessarily large outbound integration is a common cause of performance issues. Reducing the size of the XML will greatly reduce the load on the database and application server.

XSL Stylesheets for XML Document Generation and Email Notification

Oracle Transportation and Global Trade Management supports the ability to configure XML Document Generation and Email Notification via XSL stylesheet. The following steps should be followed to upload an XSL stylesheet and apply it to an External System or Contact Notification.

1. Create a Stylesheet Content record and upload the corresponding XSL file.

   This page is located at **Business Process Automation > Power Data > Event Management > Stylesheet Content**.
2. Create a Stylesheet Profile record, specifying the previously created Stylesheet Content.

   This page is located at **Business Process Automation > Power Data > Event Management > Stylesheet.**
3. Create/Edit Contact Notification by setting the Stylesheet for the 'Email' Communication Method to the Stylesheet Profile created in Step #2.

   This page is located at **Business Process Automation > Communication Management > Contact Notification.**
4. For XML Document Generation, create/Edit External System by setting the Stylesheet Profile to the Stylesheet Profile created in Step #2.

   This page is located at **Business Process Automation > Communication Management > External Systems.**

XSL Stylesheets to Customize Email Notifications

Oracle Transportation and Global Trade Management service supports the ability to download default XSL files for notifications. Please use the following steps to download default XSL files for customization.

1. Select Stylesheet Content: Select a default Stylesheet Content record and download the corresponding XSL file. This page is located at Business Process Automation > Power Data > Event Management > Stylesheet Content.
2. Customize the downloaded XSL file and upload the newly created file to Stylesheet Content. This page is located at Business Process Automation > Power Data > Event Management > Stylesheet Content.
3. To refer another stylesheet in an XSL file or to To import another stylesheet, which is already present in the database, then the import statement is to be given as below:

   ```
   <xsl:import href="db:<STYLESHEET_CONTENT_GID>"/>
   ```

Note: db: specifies that the stylesheet to be imported should be looked up in the STYLESHEET_CONTENT table.

Outbound Integration and SSL Certificates

All outbound integration requires that the transport be protected using HTTPS. Communications over HTTPS are encrypted using SSL. These SSL communications are initiated using SSL Certificates. The SSL Certificates must be from a trusted signing authority (no self-signed certificates). It is possible that the list of trusted signing authorities in the

Oracle Public Cloud will not contain the Certificate for your signing authority. In that case an SR will need to be raised to request the Certificate be reviewed for possible inclusion.

Only 1-way SSL handshaking is supported. 2-way SSL functionality is planned for a future release. For more information, see, *Logistics Cloud: How to Configure Outbound Integration (Doc ID 2110592.1)*.

IP Allow List

All outbound integration from the Oracle Public Cloud is routed through a proxy server. Customers may have a firewall with IP restrictions on inbound integration (outbound from the Cloud). In that case a Service Request will need to be logged to request the outward facing IP range used by the proxy server.

In Gen1, all outbound integration from the Oracle Public Cloud is routed through a proxy server. In Gen2, all outbound integration is instead routed through a NAT Gateway. If you have a firewall with IP restrictions on inbound integration to your data center (outbound from Oracle Cloud), please refer to one of the following MOS Notes for details on obtaining the IP Addresses.

- **Gen1**: *What are the OPC Proxy (Legacy) IP Addresses for Outbound Integration? (Doc ID 2206655.1*)
- **Gen2**: *What are the OCI Gen2 IP Addresses for Outbound Integration? (Doc ID 2662320.1)*

Note: You will need to request the IP range for both the Primary and Disaster Recovery Regions.

Follow these steps to obtain the Public IP Address for Inbound Integration to Oracle Transportation and Global Trade Management cloud service.

1. Login to the My Services Cloud Portal.
2. Click on the “Transportation Management” link.
3. Scroll down to the “Service Environments” section.
4. Copy the “Service Environment URL” for each environment by right clicking on the URL and select “Copy Link Address”.
5. Run `nslookup` using only the Host from the URL. For example.

```
nslookup otmgtm-test-myotminstance.otmgtm.us-ashburn-1.ocs.oraclecloud.com
Server: 10.1.1.1
Address: 10.1.1.1#53

Non-authoritative answer:
otmgtm-test-myotminstance.otmgtm.us-ashburn-1.ocs.oraclecloud.com canonical name =
 1586234534085.otmgtm.us-ashburn-1.ocs.oraclecloud.com.
Name: 1586234534085.otmgtm.us-ashburn-1.ocs.oraclecloud.com
Address: 199.999.99.99
```

   In this example, the Public IP Address for Inbound Integration is 199.999.99.99.

Outbound Integration and PaaS/IaaS

The following instructions are intended to provide high-level information for integrating Transportation and Global Trade Management with an application hosted on Oracle Public Cloud PaaS/IaaS services. For more detail on this topic, please refer to the documentation corresponding to your particular PaaS service. Integration from Transportation and Global Trade Management to any other application hosted on an Oracle Public Cloud service must be performed via a publicly accessible IP address and publicly accessible ports. By default, access to Oracle Public Cloud Services

are available via port 80 (HTTP) and 443 (HTTPS). If the service is not provisioned with a public IP address, it will be necessary for the customer to reserve a public IP address for their service.

It is highly recommended that the customer register their service using a Public Domain Name and use the Domain Name in the URL, rather than the IP address. It is also recommended that the customer obtain an SSL Certificate for their Domain Name and require that all communication use HTTPS. Depending on the Certificate Authority used, it may be necessary to open a Service Request to have the SSL Certificate loaded into the Transportation and Global Trade Management instance. Some Oracle Public Cloud Services support the ability to define a Security IP List, allowing you to limit inbound traffic to a range of IP addresses. In the case of Transportation and Global Trade Management, you would need to register the IP range of the Oracle Public Cloud proxy server. You can open a Service Request in order to request this IP range. Further security is available with optional VPN access for Cloud Services.

> **Note:** In Oracle Public Cloud it is possible for the you to use non-standard ports, though additional configuration on the IaaS/PaaS environment is required to make this work. However, this is not supported in Gen2.

You should test all URLs from outside of Transportation and Global Trade Management first using a web browser or a utility such as JDeveloper, SOAPUI, curl, or wget. For more details, please refer to the "Register a Custom Domain Name with a Third-Party Registration Vendor" and "Obtaining the SSL Certificate" topics in the Infrastructure as a Service documentation.

Outbound REST Integration

In addition to the HTTP (POST) and SERVICE (SOAP Web service) communication methods there is now a REST option which can send out the JSON REST resource format and Transmission XML messages. The determination of which format to use is controlled by the content type defined on the target external system. See the *REST API documentation* for details.

10 Data Management

Migration Projects

The Migration Project feature is a standard way to define and manage one or more datasets for the purpose of migrating data from one Transportation and Global Trade Management instance to another.

Although the Transportation and Global Trade Management application is fully functional “out of the box”, an operational system will typically require some configuration. Best practice would be for such a configuration to be developed and tested in a pre-production environment, accepted by product and business/operational experts and then promoted to the production environment.

For more details on using Migration Projects to move data between instances, please refer to the Migration Project section of the Data Management Guide.

Business Data Purge and Archive

In order to maintain optimal performance, it is necessary to periodically purge or archive data from the operational database. Oracle Transportation and Global Trade Management uses multiple methods for purging and archiving data. This section explains these concepts in more detail.

Purging old data helps maintain optimal performance in the operational system. Archiving is used in conjunction with purging for critical business objects which need to be accessible for an extended period of time. When data is archived, it is moved to an archive database schema and compressed. Data in the archive schema can be queried, but cannot be modified.

Note: Templates are not deleted when you purge data.

These business objects support archiving, with the following settings:

- **Operational Retention Period**: How long the data is kept in the operational database. If the data has not been updated for the period specified by Operational Retention Period, then it is archived. The Operational Retention Period is **2 years** for Shipment, Invoice, Work Invoice, Order Release, OB Order Base, DM Transaction, GTM Campaign, Device and P_BID entities. The Operational Retention Period is **5 years** for GTM Transaction entity.
- **Frequency**: How often the job runs to archive data. The Frequency is **weekly**.
- **Archive Retention Period**: How long the data is kept before it is permanently purged from the system. The Archive Retention Period is **10 years**.

Business Objects that Support Archiving

All objects found in **Configuration and Administration > Process Management > Mark for Purge** in the Purge Type field support archiving.

Archived data are found in the Report Manager in the "Archive" reports section. The archive reports take a single parameter, which is the ID of the object to be retrieved from the archive. The search for the ID allows you to query the archive schema business objects using flexible criteria. Some sample archive reports are provided upon installation.

Documents associated with the business objects above are archived when the business objects are archived. A DBA or Admin user role may access the archived documents using the Archived Documents UI, via **Business Process Automation > Document Management > Archived Documents**. Not all documents are associated with business objects, and those which are not associated are not archived or purged.

> **Note:** There are no indexes on the archive schema database tables, thus the performance of the search is expected to be slower than the operational database. If the data returned by the sample report is not sufficient, it is recommended to copy the default report and modify it as needed.

Scheduled Purges

Scheduled purges are used for purging miscellaneous transient and diagnostic data. The following table defines the retention period and purge frequency. The timing and frequency of these processes should not be altered.

Retention period and purge frequency

Entity	Retention Period	Purge Frequency
Bulk Plan Results	30 days	Weekly
Bulk Reporting	30 days	Weekly
Device Association	2 years	Weekly
Planning Diagnostics	30 days	
Email Delivery Suppression	30 days	Daily

Partitioned Purges

Oracle Transportation and Global Trade Management contains several integration and logging tables that can become quite large very quickly; these tables have been partitioned to allow for quick purges of older data. By partitioning the tables, a particular partition (segment) can be truncated, instead of records being individually deleted, which is inefficient for large amounts of data. The following table explains the time period which is used to create the partitions and the number of partitions for each entity.

Time period which is used to create the partitions and the number of partitions

Entity	Time Period	Partitions
Data Queues	Daily	12
Explanation	Daily	7
Integration Logging	Monthly	4
Integration Logging(Mobile)	Daily	7
Login History	Monthly	4
Mobile Messages	Daily	7
Object Lock	Daily	7

Entity	Time Period	Partitions
Problem	Monthly	4
Process Control History	Quarterly	4
Transaction(Mobile)	Daily	7
Transaction(Inbound)	Bi-Weekly	4
Transaction(Outbound)	Weekly	4
Transaction(Mobile)	Daily	7
Transmission(Inbound)	Bi-Weekly	4
Transmission(Outbound)	Weekly	4
Tender Transmission(Outbound)	Quarterly	4

These jobs are set to run at 1 AM on the last day of the cycle. Every table reuses its partitions, because the intention is that before the end of the cycle, the oldest partition is purged in preparation for the new cycle. In other words, for a monthly table, on April 30th, partition 1 should be purged to remove January's data, which will then be used for May. For example:

If the time period of the table is monthly, then the data is segmented as follows:

- Jan – partition 1
- Feb – partition 2
- Mar – partition 3
- Apr – partition 4
- May - partition 5
- June – partition 6, etc.

Schedule at which oldest partition is purged in preparation for the new cycle

Time Period	Oldest Partition Purge Schedule
Daily	Every day at 10 PM UTC
Weekly	Every Monday at 4 AM UTC
Bi-Weekly	Every other Sunday at 4:30 AM UTC
Monthly	Every last day of the month at 5 AM UTC
Quarterly	Every last day of the quarter at 6 AM UTC

Loading Legacy Data

Loading legacy Business Transaction data from a previous instance of Transportation and Global Trade Management is permitted. A maximum of two years of data is permitted. Legacy data will adhere to the same data retention policies previously described. It is important that the original insert_date of the data be preserved during the data upload in order to prevent the data from prematurely getting archived and to prevent performance issues during archiving. The Oracle Transportation and Global Trade Management Service does not provide any mechanism for loading the data. Loading the legacy data is the responsibility of the customer and/or the corresponding implementation partner and must be performed using a support integration technology (i.e. CSV or XML).

Virus Scan

It is important to understand that all document upload interfaces to Oracle Transportation and Global Trade Management are protected with virus scanning for your added security. There is no configuration required and this feature cannot be disabled. If you encounter any issues with uploading documents, please open a Service Request.

Database Replication Enablement for Oracle Transportation and Global Trade Management

Database Replication Enablement is an optional, separately priced feature (Part# B91919) of the Transportation and Global Trade Management that provides for a near real time replication of the main data from the Transportation and Global Trade Management production schema, which can be used for purposes of integrated reporting with other systems, or population of an external data lake. The key advantage to this feature is that it allows SQL access to a read-only copy of the Cloud database, a database which is owned by the customer and not part of the SaaS offering. The replication is performed using the Oracle GoldenGate product, which must be licensed by the customer along with the target database license.

The replication is performed on the glogowner and reportowner schemas (not hdowner or archive) and copies the data, structure and indexes. It does not copy the VPD information. The tables listed below are excluded from replication because they either include sensitive data or they contain high-volume transient data that is not required for analytics type reporting. It is important to understand that deletions, including Business Data Purge for Orders, Shipments, etc., are also replicated. Customers will need to propagate the data in the corresponding tables to another table or database if they intend to keep the data longer than the purge period. For more details on the setup and configuration required, please review this MOS note, ***GoldenGate Deployment for Oracle Transportation and Global Trade Management (OTM) (Doc ID 2497511.1)*** .

Table Name

- APP_MACHINE_FAILOVER_T
- APP_MACHINE_T
- APP_POWER_ACTION_ACCESS_T

- APP_SERVER_DATA_QUEUE_DEF_T
- APP_SERVER_DOMAIN_T
- APP_SERVER_FUNCTION_T
- APP_SERVER_MACHINE_T
- APP_SERVER_QUEUE_T
- APP_SERVER_T
- BUSINESS_PROCESS_LOG_T
- CONNECTION_POOL_T
- DATA_PURGE_HISTORY_DETAIL_T
- DATA_Q_DEF_RELATED_Q_DEF_T
- DATA_QUEUE_DEF_T
- DATA_QUEUE_EXECUTOR_T
- DATA_QUEUE_INDEX_COL_T
- DATA_QUEUE_INDEX_T
- DATA_QUEUE_POLLER_INDEX_T
- DATA_QUEUE_POLLER_T
- DATA_QUEUE_TABLE_T
- DATA_SOURCE_T
- DB_TRACE_FILE
- DBPATCH_LOG_T
- DOMAIN_COPY_SCRIPT
- DOMAIN_COPY_SEQ_CACHE
- EBR_TABLE_T
- ERROR_LOG_T
- EXCEPTIONS
- EXPLANATION_T
- GL_LOGIN_HISTORY_T
- I_LOG_DETAIL_T
- I_LOG_T
- I_TRANSACTION_ACK_T
- I_TRANSACTION_DETAIL_T
- I_TRANSACTION_REFNUM_T
- I_TRANSACTION_T
- I_TRANSMISSION_ACK_T
- I_TRANSMISSION_PGROUP_T
- I_TRANSMISSION_REFNUM_T
- I_TRANSMISSION_REPORT_T
- I_TRANSMISSION_T
- JMSCONSUMER_T

- JMSDESTINATION_T
- JMSMESSAGE_T
- JMSMESSAGEQUEUE_T
- JMSTABLEID_T
- OBJECT_LOCK_T
- PLAN_TABLE
- Q_INTEGRATION_IN_EXCEPTION_T
- Q_INTEGRATION_IN_T
- Q_INTEGRATION_OUT_EXCEPTION_T
- Q_INTEGRATION_OUT_OVERFLOW_T
- Q_INTEGRATION_OUT_T
- Q_LIFETIME_EVENT_EXCEPTION_T
- Q_LIFETIME_EVENT_T
- Q_MESSAGE_EXCEPTION_T
- Q_MESSAGE_T

Production to Test Cloning (P2T)

Oracle Transportation and Global Trade Management service supports the ability to have the production database instance cloned to your test instances. This is often a good idea to have done shortly after go-live in order to facilitate issue replication. It is also highly recommended to have this done prior to an upgrade. P2T requests are made by opening service requests.

The entire production database is cloned with the following exceptions.

- Recurring processes are disabled with a **Next Process Time** set in the distant future to prevent production processes from running on test data. These may be edited as needed to run in the test system.
- All users other than Service Administrators (users with the 'DBA.ADMIN" role) are expired in order to prevent inadvertent use of the test system. There is a "Manage User Expiration Date" action available on the User Manager, which can be used to un-expire a group of users.
- The Transportation and Global Trade Management password for Service Administrators is retained from production. Note: This password would only be used if the DBA.ADMIN user was used for Integration processing, which is highly discouraged. Regardless, it is highly recommended to change this password immediately following a P2T.
- The web services are unlinked from the External System record. Edit the corresponding External Systems and relink them to the test web service after the P2T is complete.
- Environment Specific data and data potentially containing Personally Identifiable Information (PII) is not propagated. The following table outlines the data that is not propagated.

Non-Propagated Data

Table Name	Column Name
ADHOC_NOTIFY	COM_ADDRESS

Table Name	Column Name
APP_MACHINE	MACHINE_URL
CONTACT	CELL_PHONE
CONTACT	EMAIL_ADDRESS
CONTACT	FAX
CONTACT	PHONE1
CONTACT	PHONE2
CONTACT_POINT	COM_ADDRESS
CUSTOMER_TAX_INFO	All Columns
DOMAIN_SETTING_TAX_INFO	All Columns
DRIVER	DATE_OF_BIRTH
DRIVER_CDL	All Columns
EXTERNAL_SYSTEM	HOSTNAME
EXTERNAL_SYSTEM	URL
EXTERNAL_SYSTEM	IP_ADDRESS
EXTERNAL_SYSTEM_SERVICE	All Columns
I_MESSAGE	CELL_PHONE
NOTIFY_REQUEST	COM_ADDRESS
ORDER_RELEASE	EM_PHONE_NUMBER
PROBLEM	PROBLEM_URL
PROCESS_CONTROL_REQUEST	NEXT_PROCESS_TIME, for all public entries
REPORT_EMAIL	EMAIL_ADDRESS
SHIPMENT	EM_PHONE_NUMBER
X_UN_LOC_CODE	EMAIL_ADDRESS

CSV/DB.XML

The Oracle Transportation and Global Trade Management service provides capabilities for importing and exporting configuration data. The options are Comma Separated Value (CSV) or DB.XML. The remote interfaces for these features are thoroughly documented in the Data Management Guide. It is important to understand that limits are imposed on the amount of data that can be contained in a single request. This is necessary to prevent these features from affecting critical operations.

- **CSV Export**: 512MB

- **DB.XML Export/Import**: 10MB

11 Documentation

Additional Documentation

- The following link provides additional instructional and training materials for Oracle Transportation and Global Trade Management.
  - *https://cloud.oracle.com/saasreadiness/scm?readinessRID=1415317857162*
- The following My Oracle Support note captures the key differences between the On-Premises and Cloud product offerings:
  - *Note 1926811.1: Key Differences between Oracle Logistics On-Premises and Cloud*