Restricted Party Screening

Overview

About Restricted Party Screening

Oracle Global Trade Management (GTM) is a global trade automation platform that enables companies to optimize and streamline business processes related to cross-border trade. With well-structured compliance policies and trade automation tools to help implement and enforce those policies, companies can achieve best practices in global trade both within and outside of their organizations. Restricted party screening is one of the processes used to support trade compliance. GTM's Restricted Party Screening (RPS) services enable companies to perform screening of parties, trade transactions, and so on to ensure compliance with international shipping policies.

Government agencies throughout the world and other regional, unilateral, and multilateral agencies enforce regulations that restrict businesses and people from conducting trade with specific foreign entities (individuals, companies, countries). These entities are referred to as Denied, Debarred, and/or Restricted Parties ("Restricted Parties"). Examples of these entities include but are not limited to known terrorists, organizations that fund terrorists, and parties guilty of trade violations. Typically, the restricted parties are mainly countries subject to embargoes, and persons, businesses, and organizations subject to financial sanctions. Periodically, these agencies publish lists of entities that are marked as restricted parties.

In order to adhere to the regulations, companies screen their party master data and transactions against these lists, which can be very time consuming and laborious. Furthermore, if a business ships goods to a restricted party, it could incur fines, penalties, and ultimately the loss of export privileges.

GTM offers a configurable solution to screen parties against the various restricted party lists published by different government agencies. Parameters can be configured to optimize potential match results. The screening engine can be called at any point in a business process. You can screen parties at the time of party creation, which ensures they are cleared for compliance when transactions occur. You also have the option in GTM to screen parties at the time of transaction to ensure compliance. The following are the steps involved in the process of restricted party screening:

1. Data Content Source: Different government authorities release regular updates on various data content lists for compliance purposes. These government updates are regularly processed into a structured form by different content providers to be consumed and utilized by different companies. GTM content source helps companies to define the type of content (e.g. Restricted Party List, Product Classification, Rules of Origin, etc.) you want to download and access from different content providers. In addition, the content source defines how the content is downloaded using the HTTP protocol.
2. Download Data Content: This process enables you to download various trade content data to GTM, based on a data content source definition. You can trigger the download instantly or define a schedule for automatic downloads of data content at regular intervals.
3. Configure Screening Parameters: You can configure screening parameters to screen parties/contacts against the lists of restricted parties. GTM provides you with options to determine the potential matches based on matching engine (like keyword, dice engine), attributes for matching, threshold,

and weighting of the overall matching. Additional parameters include exclusion lists, punctuation marks, etc.

4. Perform Screening: You can perform the screening in two different ways. First, you can perform an ad hoc screening before entering a party into the party manager in GTM. Second, you can perform restricted party screening based on parties, trade transactions, or declarations. You can perform multiple screenings on a party to meet different business needs (for example, restricted party list screening, red flag screening, debarred country, etc.).
5. Review Screening Results: Once screening has been performed, you can view the restricted parties that might potentially match with your parties and determine whether you can conduct business with the party or not. There are multiple user interfaces (UIs) in GTM that enable you to perform this action. In addition, the Restricted Party Workbench and Work Queues are provided which enable you to quickly and efficiently review the screening results if you are working in environments with a high volume of parties.

Related Topics

Global Trade Content

Screen Service Configuration

Match Engines

Screening Restricted Parties

Restricted Party Screening Resolution

Restricted Party Screening PDF

Global Trade Content

Global Trade Content

Global trade practice requires companies to have access to and use the current trade data available. There are many types of trade data available with various sources, both nationally and internationally. Failure to use 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 including Rules of Origin

Follow the steps below to download your data content:

- Content Source Configuration
- Download Data Content

- Restricted Party List
- Restricted Party Exclusion List
- Purge Data Content
- Purge Data Version

Related Topics

About Global Trade Intelligence

Restricted Party Screening PDF

GTM Content Source

This page is accessed via Master Data > Power Data > Data Loading > Content Source.

Use this page to define the list of the countries and trade data being supported, the details of the content received from a third-party content provider, and how it is mapped to the GTM structure. You can specify information about your third-party content providers in the configuration section. This includes details such as URL and login credentials. GTM will use this information when it is time to update your content files. GTM ships with a public content source that you can use to download data related to restricted party screening, product classification, Rules of Origin, etc. If there is a data type you want to use that is not listed but is supported by the content provider, you can add it to the public content source.

On the Content Source UI, the Content Source Data Type grid must be configured with the details of what you want to download. The Content Source Data Type grid provides a mapping between the data the content provider sends and how GTM refers to this data. The Source Data Type and Source Country ID fields are the data type and the source country provided by the external provider. The Content Type field identifies the type of content to be downloaded and is set up in GTM (i.e. HTS-US, ML-US, RESTRICTED_PARTY, RULES OF ORIGIN, etc.). The "Supported" flag can be used to turn on or turn off the subscription for that data type. The system will only download files for those data types that have a check mark to indicate they are turned on.

At the bottom of the Content Source UI, the Configuration grid must be configured with the external system location and communication method (for example HTTPPOST) indicating how it should be downloaded.

Note: When multiple types of data are selected within one content source, the data loading exercise can be resource intensive.

Note: The best practice would be to split the types of data or group data type subscriptions into multiple content sources and schedule them to run at different times. For example, you could have one content source for restricted party data, a second content source for product classification data such as HTS or ECCN, and a third for Rules of Origin data.

Adding a Content Source

1. Enter an ID in the Content Source ID field.
2. Enter the name of the source in the Source Name field.
3. Select the domain for which this source will be used from the Domain Name drop-down list.

Content Source Data Type

1. Enter a sequence number in the Sequence field. This number determines in which order this data will be loaded if multiple data types are being downloaded.
2. Enter the data type from the data provider's status document in the Source Data Type field, for example ECCN. You can find the data type on the content provider's status document.
3. Enter the country ID from the content provider's document in the Source Country ID field.
4. Select the Supported checkbox if the data type is compatible with your system.
5. Enter the corresponding content type ID in the Content Type field.
6. Click Save.
7. Click Finished. The content source is saved.

Note: You can add as many content source data types as you need.

Configuration

Click New Content Source Config to open the Configuration window.

Related Topics

Content Source Configuration

Download Data Content

GTM Power Data

About Restricted Party Screening

Restricted Party Screening PDF

About Data Loading

Download Data Content

This page is accessed via Master Data > Process Management > Data Load > Download Data Content.

Use this page to download data from a content source. Once the content source is defined, you can trigger the download process from Download Data Content page.

This process connects to the external system using the URL specified for the external system in the content source and downloads an XML file known as a status document. The XML file downloaded from the third party data provider specifies the current status of the data available with the third party provider, the dates when it was last updated, and a link to download new data. It then parses the status document and downloads any data type available and that is supported by the Content Source. This process downloads only the new content available.

Note: If you have any issue with the previously downloaded content, try triggering the download content process manually without Force Reload. In case manual reload does not resolve the issue, you should check with GTM and the content provider. In case the active data version of any content type is corrupted due to

some other reason, you can edit the content source, turn on only that content type corresponding to the corrupted one, and turn off all other content types. Then perform download data content manually with Force Reload turned on. You can turn on the other content types after the download.

The Download Data Content process creates a content set record in the database. The Content Set ID in GTM corresponds to the "Version_ID" field in the content provider's status document. GTM then retrieves the zipped files specified as supported in the content source. For every data type or zip file downloaded, GTM adds a record in the Data Load table and an entry in the Content Set Detail section of the Content Set page. Next, GTM unzips the downloaded files, prepares a CSV file with the downloaded data and then moves the data into the database using the CSV upload utility. Finally, GTM sets the status in the Content Set Detail section as Processed.

You can search for a content set using the Content Set ID, on the last content set loaded, or other criteria. The status fields in the Content Set and the Content Set Detail sections convey whether or not the processing of the downloaded files was successful.

When you click the Data Load ID link in the Content Set Detail section, you can view information like the number of records processed (created or updated) by the CSV upload utility. The Number of Errors field informs you about any failure(s) that might have occurred while processing CSV records. Errors/failures are also logged during the data load process. If you want to see the log details related to the data load process, you can turn on the GTM Data load log ID.

On the Data Load page, you can see new or updated data version information. GTM uses Data Version to manage the different versions of data downloaded from the Content Source (i.e. the third party content provider). Both the product classification codes and restricted party list (RPL) have a data version associated with them. However unlike RPL, which is delivered incrementally (after the initial master data file), product classification codes are delivered as complete sets. Thus, when product classification codes are downloaded, a new data version is always created and marked as current. With DPL, delta data is appended to the existing data version.

When a data version is created or updated, a "GtmDataVersionContentUpdated" event is published, and an agent listening for this event can perform notification.

The following GTM tables are updated by the Download Data Content process for Restricted Party Lists:

- gtm_content_set
- gtm_content_set_d
- gtm_content_set_d_attr
- gtm_data_load
- gtm_data_load_detail
- gtm_data_load_attribute
- gtm_data_version
- gtm_denied_party

See gtm.dataload Properties topic.

Downloading Data Content

1. Select a content source from the Content Source ID drop-down list.

2. Select the Force Reload Data Content checkbox.

   Note: You can select the Force Reload Data Content checkbox if you want to download a fresh copy of a data set, or if you want to download a new version of a data set. You can also select this checkbox to get the correct data set if a download results in errors and a manual reloading of the data does not resolve the error.

3. Enter a User Role. When you run, publish, or schedule a recurring process, you can specify the user role used to perform the process, just like when you run agents. The user role can be used to specify a separate VPD role or another domain to run the agent. When a recurring process is modified, the user role of the recurring process can be modified as well.
4. Select a Log Profile to generate focused logging when reproducing an error for the specific action. You cannot select a log profile when you choose to schedule a process, as automatic generation of action logs is not supported.
5. Select Execute, Publish, or Schedule to determine when the process will be executed.
6. Click Submit.

Related Topics

Process Management: Master Data

Content Set

Content Source

Content Type

About Data Loading

About Restricted Party Screening

Restricted Party Screening PDF

Restricted Parties

Note: This page is available in both the current user interface (UI) and the Redwood user interface. For pages available in both UIs, we encourage you to take a look at the new Redwood experience to see the more intuitive, modern, and efficient UIs. See the Redwood: About the Redwood Experience, Redwood: Ask Oracle Landing Page, Redwood: Data Entry, Redwood: Smart Search, and Redwood: Smart Search Results for details on using the Redwood UIs.

This page is accessed via Master Data > Power Data > Restricted Parties > Restricted Parties.

Use this page to add new parties to your list of restricted parties.

Once the data content is downloaded from the external content provider and processed successfully, you will see new or modified restricted party lists under a particular data version. You can view the details of the

restricted parties downloaded in the Restricted Party page. You can also create your own internal list or red flag list of restricted parties using this page.

Adding a New Restricted Party

While there are a large number of fields in the Restricted Party page, you are required to enter a value in only the Data Version ID field. This ID identifies the data subset to which the new restricted party will be added. It is important to note that the information you enter here - such as name and address details - may be used for restricted party screening. If you do not enter a Restricted Party ID, GTM will generate one for you.

Note: Make sure you always add additional restricted parties such as red flag lists to the data version that is marked as current and select the In Use checkbox. This is the default setting for the In Use option. Since the screening process runs on the data version that is marked as current, this will ensure any restricted parties you add are considered during screening.

Any information you record on this page will generate a screening match if the party being screened has similar information based on the configuration of your service parameters. For example, if you designate a last name of Frederick and a state of Texas, any party which matches those criteria will be identified as a restricted party.

Only restricted party records in the Public domain or the domain you are using will be used for screening purposes.

Parent Restricted Party

If the new restricted party is associated with another already restricted party (typically in a parent/child relationship) use this section to add that association.

1. Enter an existing restricted party ID in the Restricted Party ID field.
2. Click Save.
3. Continue adding as many parties as required.
4. When you have no more parties to add, click Finished.

Redwood: Adding a New Restricted Party

This page is accessed via Settings and Actions > Try the New Redwood Experience > Start Exploring. Enter a search string in the Ask Oracle search and select Restricted Party.

While there are a number of fields in the Restricted Party page, you are required to enter a value in only the Restricted Party ID and the First Name field, and then click Submit.

It is important to note that the information you enter here - such as name and address details - may be used for restricted party screening.

Note: It is recommended that you add additional restricted parties such as red flag lists and select the In Use checkbox. Since the screening process runs on the data version that is marked as current, this will ensure that any restricted parties you add are considered during screening.

Any information you record on this page will generate a screening match if the party being screened has similar information based on the configuration of your service parameters. For example, if you designate a last name of Frederick and a state of Texas, any party which matches those criteria will be identified as a restricted party.

Only restricted party records in the PUBLIC domain or the domain you are using will be used for screening purposes.

Related Topics

Restricted Party Screening Action

Restricted Party Screening

Restricted Party Exclusion List

GTM Power Data

About Restricted Party Screening

Restricted Party Screening PDF

About Data Loading

Restricted Party Exclusion List

This page is accessed via Master Data > Power Data > Restricted Parties > Restricted Party Exclusion List.

This page enables you to exclude certain restricted parties from the restricted party screening process. You can also edit the existing exclusions. When the restricted party screening process runs, GTM will first check if a restricted party is listed in the restricted party exclusion list. If the restricted party is on the exclusion list, GTM will not screen it against the party.

Adding a Restricted Party Exclusion

1. Enter an ID in the ID field.
2. Fill in as many of the remaining fields as possible.
3. If you are making this exclusion for a limited time, be certain to enter the expiration date in the Expiration Date field.
4. Select the domain in which this exclusion will apply from the Domain Name drop-down list.
5. Click Finished.

Related Topics

Restricted Parties

Restricted Party Screening - Potential Matches

GTM Power Data

GTM Screening Overview

About Restricted Party Screening

Restricted Party Screening PDF

Restricted Party Screening Profiles

This page is accessed via Master Data > Power Data > Restricted Parties > Restricted Party Screening Profiles.

A restricted party screening profile consolidates the required screening services (like name, address, company name, etc.) into a single profile. Using a screening profile enhances restricted party list screening performance.

Use this page to add a new screening profile or to modify the existing ones.

Adding a Restricted Party Screening Profile

1. Enter a unique identifier in the Restricted Party Screening Profile ID field. You will use this ID when you refer to this screening profile on other pages.
2. Select a domain in which this screening profile will be active from the Domain Name drop-down list.
3. If desired, enter additional information about the screening profile in the Description field.

Adding a Service Preference

Use this section to add service preferences to a screening profile. Restricted party list screening will be based on these service preferences.

1. Select an option from the Service Preference drop-down list.
2. Select an option from the Constraint ID drop-down list.
3. Click Save.
   You can add multiple service preferences to a profile.
4. Click Finished.

Related Topics

GTM Power Data

Service Preference

Service Parameter

GTM Screening Overview

About Restricted Party Screening

Restricted Party Screening PDF

Purge Data Content

This page is accessed via Master Data > Process Management > Data Load > Purge Data Content.

Use this page to purge data that is no longer useful once you have downloaded new data content.

Once the data content is downloaded from the external content source and processed successfully, you can use this page to delete all the downloaded physical files. You can configure your data content purge process to take place immediately, during the next scheduled process or on a specific day and time.

Note: This process does not delete the restricted party records you received and are now available in the Restricted Party List page, but it deletes the files that were downloaded from the content source.

Purging Data Content

1. Enter the required number of days (D), hours (H), and minutes (M) in the Older Than section. Records older than the mentioned duration will be considered for removal.
2. If there were errors during the most recent content upload and you prefer not to purge them until you have examined them, select the Exclude Data Load With Errors option.
3. Enter a User Role. When you run, publish, or schedule a recurring process, you can specify the user role used to perform the process, just like when you run agents. The user role can be used to specify a separate VPD role or another domain to run the agent. When a recurring process is modified, the user role of the recurring process can be modified as well.
4. Select a Log Profile to generate focused logging when reproducing an error for the specific action. You cannot select a log profile when you choose to schedule a process, as automatic generation of action logs is not supported.
5. Select Execute, Publish, or Schedule to determine when the process will be executed.
6. Click Submit.

Related Topics

Download Data Content

Process Management: Master Data

About Restricted Party Screening

Restricted Party Screening PDF

Mark for Purge

This page is accessed via Master Data > Power Data > Data Loading > Data Version > Actions > Mark For Purge.

As an administrator, you can perform a purge based on age of data, status information or domain name. You can purge downloaded data content (RPL, product classification codes, trade incentive program inventories and movement information, etc.) using the standard GTM purge capability available. This process is performed in two steps:

- You can identify and mark the data version to be purged using the Mark For Purge action available on the Data Version page.
- You can then run the Schedule Purge process which deletes all related data of a particular data version. The purge process identifies all data versions that are marked for purge and checks for references. If there are no references, the purge process deletes the data version and all its data from the child tables. You can configure your data content purge process to take place immediately, during the next scheduled process or on a specific day and time.

Note: Normally with every new download of the content type of restricted parties, GTM updates the existing data version. In this scenario, you may not be interested in purging the data version. But if you want to create a fresh list of restricted parties in a new version, then it is better that purge the old data version. Generally, the purged data version is more useful with the downloaded content type of “product classification” since every new download process creates a new data version and the old data version expires.

Different transaction tables are checked during the purge process of data version related to restricted party, product classification, and trade incentive program inventory and movement.

For restricted party related data version purge, the process checks for references in the GTM_PARTY_SCREENING table.

For product classification related data version purge, the process checks for references in the following tables:

- GTM_ITEM_CLASSIFICATION
- GTM_ITEM_CLASS_TEMPLATE_D
- GTM_REGISTRATION
- GTM_STRUCTURE
- GTM_STRUCTURE_COMPONENT
- GTM_TRANS_LINE_REPORT_QUANTITY
- GTM_TR_ITEM_STRUCTURE
- GTM_TR_PROD_CLASSIFICATION

For trade incentive program inventory and movement related data version purge, the process checks for references in the GTM_TIP_INVENTORY table.

Related Topics

GTM Power Data

About Restricted Party Screening

Restricted Party Screening PDF

Match Engine

Match Engine Overview

GTM supports the following match engines for you to select from and to specify the algorithm that will be used for restricted party screening. You can select a particular engine to be used in a screening task by specifying it in the Master Data > Power Data > Configurations > Service Preference window. Following are the match engines available:

- Exact Match engine checks for a complete match between the party and the restricted party details.
- Substring Match engine checks whether the party details match with that of the restricted party and vice-versa.
- Keyword Match checks for the number of restricted party words present for the party.
- Dice engine checks for common bigrams to calculate a dice coefficient, which in turn is used to calculate the match factor. It is used as the default match engine if no other engine is selected.
- Inverted Index engine uses an inverse indexing algorithm for indexing restricted parties by bigrams. The occurrence of bigram characters (two characters) in the party and the restricted party data are used to compare and compute a coefficient value, which in turn is used to determine the match percentage.
- Soundex and Metaphone engines are phonetic algorithms. These engines encode the party and the restricted party data and then apply the dice engine on the encoded results to find possible matches.

Note: The match factor determined using Exact or Substring engine will always be 0 or 1, but for other match engines it can vary from 0 to 1.

Note: If a character has an accent associated with it, GTM will consider the character and only provide a match if the accent appears on both the party and the restricted party. For example, if the party has a company name of including the word "Göteborg", it will not be considered a match to Goteberg where the accent is not present over the letter 'o'.

Related Topics

About Restricted Party Screening

Restricted Party Screening PDF

Exact Match

You can select the engine to be used for screening by specifying it in the Master Data > Power Data > Configurations > Service Preference window.

This engine identifies exact matches between the party data and the restricted party data. For example, if you are using this engine for screening, the match factor of matching the word “OSIEL” against “OSIEL CARDENAS GILLEN” is 0 as it is not an exact match.

Related Topics

Match Engine Overview

Substring Match

Keyword Match

Dice

Inverted Index

Soundex

Metaphone

Restricted Party Screening PDF

Substring Match

You can select the engine to be used for screening by specifying it in the Master Data > Power Data > Configurations > Service Preference window.

This engine checks if the party detail is present for the restricted party or the denied party detail is present for the party. The match factor of matching the word “JORGE” against the words “JORGE SALINA AGUILAR” or matching the words “JORGE SALINA AGUILAR BIN LADEN” against the word “JORGE” is 1, as the matching is bidirectional.

Note: This match engine should be used only if the matching takes place both ways.

Related Topics

Match Engine Overview

Exact Match

Keyword Match

Dice

Inverted Index

Soundex

Metaphone

Restricted Party Screening PDF

Keyword Match

You can select the engine to be used for screening by specifying it in the Master Data > Power Data > Configurations > Service Preference window.

This engine looks for the number of restricted party words present for the party to determine the match percentage. It works in only one direction - from restricted party to party. For example, matching the word “Nuclear” against the words “Nuclear Corporation” results in 0.5% as match factor, but matching the words “Nuclear Corporation” against the word “Nuclear” results in 1 as match factor.

Related Topics

Match Engine Overview

Exact Match

Substring Match

Dice

Inverted Index

Soundex

Metaphone

Restricted Party Screening PDF

Dice

You can select the engine to be used for screening by specifying it in Master Data > Power Data > Configurations > Service Preference.

This engine uses the occurrence of bigram characters (two characters) in the party and the restricted party data to compare and compute a coefficient value, which in turn is used to determine the match percentage. The output match factor can vary from 0 to 1. Dice can be employed to compare double-byte characters as well.

Matching Factor Calculation by Dice Engine

The Dice engine performs screening using the following process:

1. Simplify abbreviations.
   Abbreviations can contain spaces or full stops (.).
   Abbreviations containing a space will have the space removed. For example, "U S A" will be changed to "USA".
   With the list of punctuation marks specified in the property gtm.rpsservice.punctuationmarks containing a period (.), abbreviations having a full stop will have it removed from the logic. For example, "U.S.A." will be changed to "USA".
2. Remove punctuation based on the property gtm.rpsservice.punctuationmarks. All the punctuation marks mentioned in this property will be converted to a space.
3. Split the party and the restricted party details into words.

4. Since there can be multiple words for the party and the restricted party, GTM prepares all possible combinations of two words (one from party detail and another from restricted party detail), computes their bigrams and then checks for their matching percentage using Dice Coefficient.

   GTM calculates the Dice Coefficients between two words (one from the party and other from the denied party) using the following formula:

   Dice Coefficient Formula = [2 * NC/{NC + Maximum(N1 , N2)}]
   where,
   Number of Bigrams of Party word = N1
   Number of Bigrams of Restricted Party word = N2
   Number of common Bigrams of Party and Restricted Party word= NC

5. Remove all that are not a match: two words with zero Dice Coefficient is not a match.
6. For every party word, identify the best target word match.
7. Calculate the match factor using the best matches.

Detailed Example of Match Factor Calculation Using Dice Engine (Forward and Backward Configuration):

Let us take an example of a restricted party with the name "ZIDAN EMAD ABDELHADIE" and party "ZIDA ABDELHADI" with same address. You can configure a match threshold of 0.85 for name parameter match. Following are the steps showing how the forward and backward match factor is calculated.

1. Split the party and the restricted party full name into words.
   1. Source Tokens = {ZIDAN, EMAD, ABDELHADIE}
   2. Target Tokens = {ZIDA, ABDELHADI}
2. Create bigrams of every party and restricted party word.

Party	Restricted Party
ZIDAN = ZI, ID, DA, AN [4 BIGRAMS]	ZIDA = ZI, ID, DA [3 BIGRAMS]
EMAD = EM, MA, AD [3 BIGRAMS]	ABDELHADI = AB, BD, DE, EL, LH, HA, AD, DI [8 BIGRAMS]
ABDELHADIE = AB, BD, DE, EL, LH, HA, AD, DI, IE [9 BIGRAMS]	

3. Prepare a combination of two words (one from the party and the other from the restricted party) and calculate Dice Coefficient for each such combination.

Party: Name	Restricted Party: Name	Common Bigrams	Number of Common Bigrams	Dice Coefficient Formula = [2 * NC/{NC + Maximum(N1 , N2)}]
ZIDAN = ZI, ID, DA, AN [4 BIGRAMS]	ZIDA = ZI, ID, DA	ZI, ID, DA	3	2*3/[3+ Max(4, 3)] = 6/7 = 0.85

	[3 BIGRAMS]			
	ABDELHADI = AB, BD, DE, EL, LH, HA, AD, DI [8 BIGRAMS]	Nil	0	2*0/[0+ Max(4, 8)] = 0
	ZIDA = ZI, ID, DA [3 BIGRAMS]	Nil	0	2*0/[0+ Max(3, 3)] = 0
EMAD = EM, MA, AD [3 BIGRAMS]	ABDELHADI = AB, BD, DE, EL, LH, HA, AD, DI [8 BIGRAMS]	AD	1	2*1/[1+ Max(3, 8)] = 2/9 = 0.22
	ZIDA = ZI, ID, DA [3 BIGRAMS]	Nil	0	2*1/[1+ Max(3, 8)] = 2/9 = 0.22
ABDELHADIE = AB, BD, DE, EL, LH, HA, AD, DI, IE [9 BI-GRAMS]	ABDELHADI = AB, BD, DE, EL, LH, HA, AD, DI [8 BIGRAMS]	AB, BD, DE, EL, LH, HA, AD, DI	8	2*8/[8+ Max(9, 8)] = 16/17 = 0.94

4. Remove all non-matches (i.e. with zero Dice Coefficient) and arrange the remaining matches in the order of Dice Coefficient.

   The remaining combinations are:

Party: Name	**Restricted Party: Name**	**Dice Coefficient**
ABDELHADIE	ABDELHADI	0.94
ZIDAN	ZIDA	0.85
EMAD	ABDELHADI	0.22

Identify the best matches among the remaining combinations. ABDELHADI from Restricted Party is considered a better match with the ABDELHADIE from Party (94%) than EMAD from party (22%). Hence, EMAD vs ABDELHADI (22%) is discarded. Thus remains:

Party: Name	Restricted Party: Name	Dice Coefficient
ABDELHADIE	ABDELHADI	0.94
ZIDAN	ZIDA	0.85

5. Calculating the number of characters for each party and restricted party word and calculating forward and backward match factor:
   Party = ZIDAN [5 Characters – 85% matching] + EMAD [4 Characters - 0% matching] + ABDELHADIE [10 characters - 94% matching] = 19 Characters

   Restricted Party = ZIDA [4 Characters – 85% matching] + ABDELHADI [9 characters - 94% matching] = 13 Characters

   Forward Match Factor = Total Number of Matching Characters of Party/Total Number of Characters of Party
   = (0.85 * 5 + 0 * 4 + 0.94 * 10)/ (5 + 4 + 10)
   = (4.25 + 0 + 9.4)/19
   = 13.65/19
   = 0.71

   Backward Match Factor = Total Number of Matching Characters of Restricted Party /Total Number of Characters of Restricted Party
   = (0.85 * 4 + 0.94 * 9)/ (4 + 9)
   = (3.4 + 8.46)/13
   = 11.86/13
   = 0.91

   Here, the party will be considered as match to restricted party using backward direction as 0.91 match factor is greater than 0.85 threshold. But it will not be considered as a match using forward direction as 0.71 is less than 0.85 threshold. It is possible that the data of party and restricted party might be the other way causing the forward match factor to be 0.91 and backward match factor to be 0.71. You can use 'Both' option as match direction to perform both forward and backward match and take the best out of the two.

Related Topics

Match Engine Overview

Exact Match

Substring Match

Keyword Match

Inverted Index

Soundex

Metaphone

Restricted Party Screening PDF

Inverted Index

You can select the engine to be used for screening by specifying it in the Trade Master Data > Screening Service Configuration > Service Preference window.

This engine uses an inverse indexing algorithm for indexing restricted parties by bigrams. This engine uses the occurrence of bigram characters (two characters) in the party and the restricted party data to compare and compute a coefficient value, which in turn is used to determine the match percentage. The output match factor can vary from 0 to 1.

Note: Match direction is not applicable for Inverted Index engine. So even if you select any option from the Match Direction drop-down list on the Service Parameter page, it will not be considered during restricted party screening using this engine.

Matching Factor Calculation by Inverted Index Engine

The Inverse Index engine performs screening using the following process:

1. Split the party and restricted party into bigrams.
2. GTM calculates the match factor between the two parameters using the following formula:

   Match factor Formula = [2 * NC/{N1 + N2}]

   where,

   Number of Bigrams of Party word = N1

   Number of Bigrams of Restricted Party word = N2

   Number of common Bigrams of Party and Restricted Party word= NC

Example

Party full name: MOHAMED ABU ABDA

Bigrams = [MO, OH, HA, AM, ME, ED, AB, BU, BD, DA]

N1 = 10

Restricted party full name: MOHAMED MUMU

Bigrams = [MO, OH, HA, AM, ME, ED, MU, UM]

N2 = 8

Common bigrams: [MO,OH,HA,AM,ME,ED]

NC = 6

Match factor = (2*(6))/(10+8) = 0.667

Related Topics

Match Engine Overview

Exact Match

Substring Match

Keyword Match

Dice

Soundex

Metaphone

Restricted Party Screening PDF

Soundex

You can select the engine to be used for screening by specifying it in the Master Data > Power Data > Configurations > Service Preference window.

This engine uses a phonetic algorithm and fixed-length keys for indexing names by sound, as pronounced in English. Soundex code for a string consists of a letter followed by three numerical digits. The letter is the first letter of the name and the digits encode the remaining consonants. Similar sounding consonants share the same digit. Vowels can affect the coding, but are not coded themselves except as the first letter. Matching is performed in two steps:

1. Encoding of the party and the restricted party details.
    - b, f, p, v => 1
    - c, g, j, k, q, s, x, z => 2
    - d, t => 3
    - l => 4
    - m, n => 5
    - r => 6

    - h, w are not coded
    - Two adjacent letters with the same number are coded as a single number.
    - Letters with the same number separated by an h or w are also coded as a single number.
    - Continue until you have one letter and three numbers. If you run out of letters, fill in 0s until there are three numbers.
2. Matching the encoded output using the Dice Engine.

Detailed Example of Matching the Encoded Output:

Let us take an example of a party with the name “MULLAH” and a restricted party with the name “MAULAVI”. Following are the steps showing how the encoded output is matched.

1. Encoding.

    Party: Full Name **Restricted Party: Full Name**

    Encoding(MULLAH) = M400 Encoding(MAULAVI) = M410

2. Dice engine matching:
    1. Bigrams(ML) = {M4, 40, 00}, Bigrams(MLF) = {M4, 41, 10}
    2. Common Bigrams = {M4}
    3. Dice Coefficient = (2*1)/(1+3) = 0.50
    4. Total Number of Letter Matches for Party word (MULLAH) = 0.5 * 6 = 3
    5. Match factor of Full Name = Number of Letter Matches/Total Number of Letters on Party = 3 /6 = 0.5 = 50%

Related Topics

Match Engine Overview

Exact Match

Substring Match

Keyword Match

Dice

Inverted Index

Metaphone

Restricted Party Screening PDF

Metaphone

You can select the engine to be used for screening by specifying it in the Master Data > Power Data > Configurations > Service Preference.

This engine uses a phonetic algorithm and variable length keys for indexing names by sound, as pronounced in English. Matching is performed in two steps:

1. Encoding of the party and the restricted party detail.

   If the word begins with 'KN', 'GN', 'PN', 'AE', 'WR', drop the first letter. E.g.: KNOWLEDGE becomes NOWLEDGE.

   'PH' transforms to 'F' e.g.: 'PHONE' transforms to 'FONE'.

   'Q' transforms to 'K' e.g.: 'QUEEN' transforms to 'KUEEN'.

2. Matching the encoded output using the Dice Engine.

Detailed Example of Matching the Encoded Output

Let us take an example of a party with the name “MULLAH” and a restricted party with the name “MAULAVI”. Following are the steps showing how the encoded output is matched.

1. Encoding.

   Party: Full Name **Restricted Party: Full Name**

   Encoding(MULLAH) = ML Encoding(MAULAVI) = MLF

2. Dice engine matching:
   1. Bigrams(ML) = {ML}, Bigrams(MLF) = {ML, LF}, Common Biagrams = {ML}
   2. Dice Coefficient = (2*1)/(1+2) = 0.67
   3. Removing non matches and finding out best matches
   4. Total Number of Letter Matches for Party word (MULLAH) = 0.67 * 6
   5. Match factor of Full Name = Number of Letter Matches/Total Number of Letters on Party = 0.67 * 6/6 = 0.67 = 67%

Related Topics

Match Engine Overview

Exact Match

Substring Match

Keyword Match

Dice

Inverted Index

Soundex

Restricted Party Screening PDF

Screening Restricted Parties

Screening Restricted Parties

Screening is a process whereby each individual or company (business partners) with whom you are planning to do business is screened against the restricted party list (denied, debarred and/or restricted parties) to check whether you can conduct business with them. Standard screening is performed based on first name, last name or company name. Additional optional fields like alternate name, address, postal code, city, province, and country can be used to determine the potential matches during screening. Oracle Global Trade Management (GTM) supports transactional and non-transactional screening of parties.

Government agencies throughout the world and other regional, unilateral, and multilateral agencies enforce regulations which restrict businesses and people from conducting trade with specific foreign entities (individuals, companies, countries). These entities are referred to as Denied, Debarred, and/or Restricted Parties. Typically, the restricted parties are mainly countries subject to embargoes, and persons, businesses, and organizations subject to financial sanctions. Periodically, these agencies publish lists of entities that are marked as restricted parties.

GTM provides the functionality to download this list from third party content providers and perform screening of involved parties against the list of "Restricted" parties identified by the government.

When you first download restricted parties into GTM from a content provider, you can compare all your parties in GTM to the entire restricted party list. As a content provider updates the restricted party lists, based on updates to the regulations, content providers will only send in the updates to the existing lists in GTM, also known as a delta list. At this time, GTM will then perform delta screening where all parties in GTM are screened against the delta list.

Performance Improvement Tips for Restricted Party List Screening (RPLS)

- Utilize Global Exclusion Service Preference Instead of Exclusion Words at the Service Preference Level
  In GTM, global exclusion words are used to filter out parties from RPLS. Stored in the Global Exclusion Service Preference and cached in memory, these words speed up processing by excluding matching parties before screening starts. This method is faster than using exclusion words at the Service Preference level, which slows down the screening process.
    - Set gtm.rpls.useExclusionWords = GlobalExclusionServicePreference to use Global Exclusion Service Preference.
- Utilize Service Parameter Level Thresholds
  The RPLS Service Parameter Threshold in GTM defines the limits for processing during screening. By setting forward and backward thresholds, you can optimize performance, better manage resources, and improve overall screening efficiency.
- Use Single User Data Source Profile
  A Single User Data Source Profile in GTM is a high-performance connection pool assigned to a single user, eliminating the need for additional Virtual Private Database (VPD) calls. This setup improves performance by reducing connection overhead and is ideal for high-speed data access scenarios.

    - To use this, log in to application and switch to User Role created which uses SINGLE USER data source profile. Please refer below on how to set up User Role for Single User Data Profile.
- Suppress Lifetime Events During RPLS
  Suppressing Lifetime Events in GTM prevents the generation of GTM_PARTY_LAST_SCREENING events after each RPLS. By suppressing these events, unnecessary event generation is avoided, resulting in better performance, especially during high-volume screenings.
    - Set gtm.rpls.suppressLifetimeEventsAfterScreeningDataUpdate = true to suppress GTM_PARTY_LAST_SCREENING lifetime events.
- Suppress the generation of CONTACT - RP SCREENING MATCH VALID, CONTACT - RP SCREENING ALL MATCHES INVALID and CONTACT - SERVICE EXECUTED events during each RPLS. By suppressing these events, unnecessary event generation is avoided, resulting in better performance, especially during high-volume screenings.
    - By default, the optional feature SUPPRESS RPS AND SANCTION SCREENING EVENTS is enabled. The application suppresses the generation of CONTACT - RP SCREENING MATCH VALID, CONTACT - RP SCREENING ALL MATCHES INVALID and CONTACT - SERVICE EXECUTED events during screening.
- Improvements to the RPLS Service Process
    - Use Tasklist for Parallel Processing: Allows multiple tasks to be processed simultaneously, speeding up screening.
        - Set gtm.rpls.process.useTaskList = true to use Tasklist.
    - Avoid Lifetime Security Checks: Helps improve processing speed by bypassing unnecessary security checks.
        - Set glog.workflow.task.flags.ScreenPartyProcess = ABORT_ON_TIMEOUT,LOG_BATCHES,NO_LIFETIME_SECURITY to avoid lifetime security checks.
        - On adding the new flag NO_LIFETIME_SECURITY, agent events raised by tasks circumvent entry point security checks.
    - Avoid Party Locking: Reduces delays caused by locking during bulk screenings, enhancing throughput.
        - Set gtm.rpls.avoidLockingPartyForBulkScreening = true to avoid locking the parties during screening.
- Improvements to RPLS Screening via Agents
    - Use Single User Data Source for Agents: This ensures high-performance data access and reduces overhead during agent-driven screenings. To use this,
        - In the Automation Agent that runs Restricted Party Screening, set,
        - Run As = USER ROLE
        - User Role = <User Role created which uses SINGLE USER data source profile>

By implementing these best practices, you can significantly enhance the efficiency and speed of the RPLS process in Oracle GTM.

Steps to setup User Role for Single User Data Profile

Managing Data Source Profiles

If the SINGLE USER profile is available to a customer, a DBA.ADMIN user must grant user role(s) access to it. The section on the Data Source Profile manager allows the superuser to decide which profiles are granted to which user roles and which are denied. For example, a customer may want a user role to have access to both the DEFAULT and SINGLE USER data source profiles; or they may want a user role to only have access to SINGLE USER. By default, all user roles have access to DEFAULT, even if not given an explicit grant. But by adding an explicit denial of the DEFAULT grant, a customer can better limit which profile a user role can choose.

Once a user role is granted to SINGLE USER, the user role can be modified on the User Role manager to change its default data source profile to SINGLE USER. Users then can be assigned a default user role pointing to SINGLE USER, or granted rights to that user role to change dynamically.

Note: This enhancement required we reopen the Data Source Profile manager back up to Administration users. The screen has been changed, however, to show only read-only header information and the user role grants. Data function assignments are not shown. See the Data Source Profile Security section below for more information on securing this feature.

User Roles for SINGLE USER Profile Access

Creating a user role that uses the SINGLE USER role is a three-step process:

1. Create the user role using the DEFAULT data source profile. This is the only profile available to all user roles.
2. Have a DBA.ADMIN user grant the new user role rights to the SINGLE USER data source profile.
3. Edit the user role and change the data source profile to SINGLE USER.

Obtaining a SINGLE USER Profile

The use of a SINGLE USER profile could theoretically double the connection needs for a customer. If half of a customer's work is with a user role assigned to SINGLE USER and the other half to DEFAULT, the system may fully use connections from both under heavy load.

For this reason, we do not provide use of the SINGLE USER profile out-of-the-box. A customer must request a CR from OPS to obtain the SINGLE USER profile, along with any requisite database resource increases needed for the new pools. The CR would contain three parameters:

1. What VPD user is needed for SINGLE USER. For a customer needing to optimize out all VPD predicates, this could be DBA.ADMIN. For one needing to avoid VPD.set_user round trips, it could be the primary planning user.
2. The maximum size of the SINGLE_USER_LOCAL_JTS pool. If omitted, this is set to the pod size of the LOCAL_JTS pool.
3. The maximum size of the SINGLE_USER_PRIMARY_THIN pool. If omitted, this is set to the pod size of the PRIMARY_THIN pool.

Relinquishing the Use a SINGLE USER Profile

A customer may no longer need the resources of the SINGLE USER profile. To relinquish it, they must request a CR from OPS. This would:

1. Remove all user role grants to SINGLE USER.
2. Switch any user role using the SINGLE USER data source profile back to DEFAULT.
3. Remove access to the SINGLE USER profile.
4. Release database resources granted for SINGLE USER access

Related Topics

AD-HOC UI Screening

Screening Service

Party Screening

Transaction Screening

Review Match Factor Action

Restricted Party Screening PDF

Restricted Party Screening (Legacy) - Ad Hoc

This page is accessed via:

- Restricted Party Screening > Restricted Party Screening (Legacy)
- Ask Oracle > Restricted Party Screening

Ad hoc Restricted Party Screening allows you to screen the data of any party without creating a party in GTM. You can provide all the information about the party on this screen. On this screen, information in all of the fields is compared to restricted party information already on file. The more fields you can complete, the more accurate the screening will be. Any field containing "unknown" will be ignored. You can also provide a service preference or a restricted party screening profile to perform the screening.

Any information you provide on this page will generate a screening match, based on the service preference used if there is a restricted party with similar information. Once the screening is completed, the Restricted Party Screening – Potential Matches results page will show the list of restricted parties matched. For every Restricted Party match, GTM shows the Match Factor, indicating the percentage of Match. It also highlights the matching characters if the Disable Highlighting option is not selected on the Service Parameters page. You can also set the gtm.deniedparty.highlight property to toggle the highlighting feature.

Note: The application is configured to automatically purge and archive the Restricted Party List Screening ad hoc audit results after 60 days.

Screening Criteria

Enter a first name, last name, and/or company name into the respective fields.

Additional Screening Criteria

Type address information into the respective fields. The address, city, province, country, and postal code are all looked at during the screening process.

Reference Information

Use this section if you are screening a specific source system, or if you prefer to screen using a specific service preference or multiple service preferences using a restricted party screening profile.

When you have finished entering the information you wish to screen, click Match. The Restricted Party Screening - Potential Matches window opens with the results of the screening.

Note: If your screening criteria are an exact match to an excluded party, no screening will be performed. If any restricted party in the results is a complete match to an excluded party, the party will not appear in the returned results.

Note: The maximum number of matches that are returned is determined by the gtm.rpsservice.maxresponse property. The property's default value is 500.

Note: If you do not provide a service preference, the screening will be performed using the default service preference. You can set up a default service preference for ad hoc restricted party screening on the GTM Logic Configuration page.

Note: The audit details of ad hoc screening are displayed on the ad hoc Restricted Party Screening audit page.

Related Topics

About Restricted Party Screening Menu

Restricted Party

Restricted Party Screening - Potential Matches

Restricted Party Exclusion List

gtm.rps Properties

GTM Internal Status Designations

GTM Screening Overview

About Restricted Party Screening

Restricted Party Screening PDF

Screening Service

Restricted Party Screening has been built as a service that can be invoked without the need to create a party in GTM. You can send a ServiceRequest XML with the input data to the Restricted Party Screening service, which performs the screening on the input data and returns a ServiceResponse XML. You can invoke the service request via HTTP post or Web services. See the Integration Guide for more details on the input and output schema/WSDL definition of this service.

Related Topics

Screening Restricted Parties

About Restricted Party Screening

Restricted Party Screening PDF

Integration Guide

Party Screening

This page is accessed via Master Data > Parties.

Any party (individual or company) defined in GTM can be screened against the restricted party list using the web, agent action, or process actions available in GTM. You can execute multiple screenings (e.g., BIS, OFAC, and Red Flag) with different service preferences on the same GTM party. Regardless of how you trigger it, the screening process executes the following steps:

1. Screening service gets the party and a service preference or a restricted party screening profile as inputs.
2. Locks the Party.
3. GTM checks whether there is any restricted party data version or restricted party or service preference or exclusion list changes after the last screening date of the party. It continues with the next steps only if there is any change after the last screening date of the party or if the party was never screened earlier.
4. Retrieves the list of restricted parties based on the service preference and uses attributes like Data Source, Data Version, Agency Code, etc.
5. For every restricted party, the screening is performed for each service parameter configured in the Service Parameters page (e.g. first name, last Name, Company Name, Address, City, Country, etc). Screening of the service parameter with a higher threshold is performed before screening of the service parameters with a lower threshold in order to reduce the number of matches.

   Note: Party data includes fields labeled Province and Province Code. When restricted party screening is performed, the Province field is compared to the State or Province field. If there is no data in the Province field, then the province code data will be screened against the State or Province field on restricted party data.

   Note: To ensure better screening performance, keep the following in mind:
   Use Country and/or City as service parameters with a non-zero threshold.

Use Content Source, Agency Code, and or Data Version lists as service preference parameters.
Use excluded words to reduce the number of unwanted matches.

6. Each service parameter is matched using the match engine specified in the Service Preference page and a match factor is determined.
    - UNKNOWN value on any field or XX value on Country Code field of the Restricted Party is treated as an empty value.
    - GTM considers a Restricted Party and party as NOT a match if there is empty value (including UNKNOWN) against any parameter for which Match attribute on the Service Parameter is configured as NO Match.
        - If the company name is configured as a parameter, GTM performs the screening using the company name and calculates the match factor. Then an additional screening is performed using the alternate name of the party and another match factor is calculated. The higher of the two match factors is considered as the resultant match factor for the parameter.
7. If the match factor value is less than the threshold specified in the Service Parameter page, the restricted party is assumed as not a match and screening against the restricted party is stopped. If the match factor value is greater than or equal to the threshold, an adjusted match factor is calculated.

    Note: You can use the property gtm.rpls.prorateEmptyParamterWeight to exclude an empty parameter as part of the Overall Match Factor and hence, reduce the number of false positives returned during restricted party screening. When the property is set to "true" and the Match Default is MATCH, weightage of the empty parameters is prorated among the non-empty parameters while calculating the overall match factor and is then compared with the threshold on the service preference.
    Overall Match Factor without prorating = Sum of weighted Match Factor for all non-empty parameters
    Overall Match Factor with prorating = Sum of weighted Match Factor for all non-empty parameters/ Sum of weight of all non-empty parameters

8. An overall match factor is calculated by adding all the adjusted match factors. The restricted party is considered as match only if the overall match factor is greater than or equal to the overall threshold specified in the Service Preference page.
9. All the matched restricted parties are saved against the party as a “POTENTIAL MATCH” and the status of the party is set as “REQUIRES REVIEW”. In case there are no matched restricted parties, the status of the party is set to “PASSED”.
10. In case GTM finds any previous potential match of party as no longer a match, the status of the restricted party will be deleted.

    Note: A status will be assigned when the screening process is completed. For more information about internal status designations, see GTM Internal Status Designations.

11. Lock on the party is released.

GTM supports the following restricted party screening:

- Web: Use this action to immediately trigger the screening process on a party and display the potential match results.
- Agent: Use this action to trigger the screening process in the background, based on events. You can listen/subscribe to events like CONTACT – CREATED, CONTACT – NAME OR ADDRESS MODIFIED, LOCATION – ADDRESS MODIFIED.

- Process: Use this action to perform mass screening of all parties.

Party Screening Examples

Following is a detailed explanation of the use of the screening options available in GTM for different business scenarios.

- Scenario-1: A Restricted Party List is available in GTM and a new GTM party is created. You can perform restricted party screening on this party using the web action or an agent action. This is called full screening since you are screening the party against the entire list of restricted parties.
- Scenario-2: A Restricted Party List is available in GTM and a GTM party is modified after a previous screening. You can perform a rescreening against the restricted party list using the web action or agent action. A full screening will be performed, i.e. screening of modified party will be performed on the entire list of restricted parties.
- Scenario–3: A Restricted Party List is available in GTM and all GTM parties are previously screened. There are no changes to party, service preferences, or the restricted party list. You can perform re-screening of the party against the restricted party list. Since there are no changes to the party, service preferences or the restricted party list, the screening is up to date and GTM will not perform any screening. This is also referred to as no screening.
- Scenario–4: A Restricted Party List is available in GTM and all GTM parties are previously screened. A user decides to modify the service preference (e.g. updating the exclusion words, changing the punctuation marks, modifying the screening field parameters, changing the individual field threshold or overall threshold, etc.). Since the service preference was changed, you will need to perform re-screening of all parties. GTM will perform screening on each party against the entire list of restricted parties. You can perform this by using the Restricted Party Process page and selecting all the parties for screening.

- Note: This process is a full screening of the entire party master against the restricted party list and hence, the system could take time to complete the whole process.

- Scenario–5: A Restricted Party List is available in GTM and all GTM parties are previously screened. A user downloads the latest restricted party list and there are new or modified restricted parties added to the existing restricted party list. You will need to perform re-screening of all the parties against updates to the restricted party list. GTM will perform screening of each party against the updates to the existing list, also called the delta list of restricted parties. This screening is also referred to as delta screening. You can perform this by using the Restricted Party Process page and selecting all the parties for screening.
- Scenario–6: A Restricted Party List is available in GTM and all GTM parties are previously screened. A user downloads the new restricted party list. This list is a replacement of a previous restricted party list, has a new data version, and is marked as the current list. You will need to perform re-screening of all parties against the entire new restricted party list. GTM will perform screening of each party against the entire new list of restricted parties. This is also referred to as full screening. You can perform this by using the Restricted Party Process page and selecting all the parties for screening.

  Note: This process is a full screening of the entire party master against the restricted party list and hence, the system could take time to complete the whole process.

- Scenario–7: A Restricted Party List is available in GTM and all GTM parties are previously screened. If you already performed restricted party screening against this list, GTM would not perform any screening as there is no change in data between the current and the previous screening. However, if you want to perform a force screening, you can modify the service preference update_date attribute via backdoor SQL. Once this is done, you can perform screening of each party against the entire new list of restricted parties. This is also referred to as full screening. You can perform this by using the Restricted Party Process page and selecting all the parties for screening.

You can turn on the GtmPartyScreen log before screening and identify from the logs whether a full screening or delta screening was performed. For example, the logs show that the party was last screened on 2014-03-11 10:41:50 UTC and after that there was no change to the party, service preference configurations, data version or exclusion list. Hence, full screening was not performed; but the last change made to some denied parties was on 2014-03-11 10:43:48 UTC and hence, the delta screening was performed against all those denied parties changed between the 2014-03-11 10:41:50 UTC and 2014-03-11 10:43:48 UTC.

Note: This is for diagnostics purpose only and should be rarely used.
Turn off the GtmPartyScreen log after verifying the kind of screening.

Related Topics

Screening Restricted Parties

About Restricted Party Screening

Party

Restricted Party Screening PDF

Transaction Screening

In order to ensure you do not ship to a restricted or denied party, you should screen the parties on your transactions against the restricted party lists.

The screening process executes the following steps on your transaction:

1. Screening service gets a service preference or a restricted party screening profile as an input.
2. All the parties on the trade transaction/declaration as well as the corresponding lines are retrieved.
3. Screening is performed on any party not screened previously. You can avoid screening of any party on trade transaction/declaration by excluding it using gtm.rps.involved_party_qual.exclude property. For example, you may want to exclude screening of all your SHIP_FROM involved parties since all the facilities you ship from are company owned. Since all the facilities are internal, you can bypass screening for them.
4. Next, the RPLS status of trade transaction/declaration line is set to:
    - TL_RPLS_FAILED if there is even one party with the RPLS_FAILED status.
    - TL_RPLS_REQUIRES REVIEW if there is no party with the RPLS_FAILED status but at least one party with RPLS_REQUIRES REVIEW status.
    - TL_RPLS_PASSED if none of the parties have the RPLS_REQUIRES REVIEW or RPLS_FAILED status.

5. Then, the RPLS status of trade transaction/declaration is set to:
    - TS_RPLS_FAILED if there is even one trade transaction/declaration line with the RPLS_FAILED status.
    - TS_RPLS_REQUIRES REVIEW if there is no trade transaction/declaration line with the RPLS_FAILED status but at least one trade transaction/declaration line with RPLS_REQUIRES REVIEW status.
    - TS_RPLS_PASSED if none of the trade transaction/declaration lines have the RPLS_REQUIRES REVIEW or RPLS_FAILED status.

    Note: The shipment execution is stopped for any transaction with an RPLS_FAILED status.

It is recommended to:

- If there is a change in any of the restricted party screening properties, you should trigger complete re-screening.
- When there are a large number of parties to be screened, you can scale up by increasing the threads on the event groups 'agentGtmRPLS' for party screening and 'agentGtmCompliance' for trade transaction screening.
- When there are a large number of parties to be screened, you can scale up using the scalability capability. By using scalability, you can route the restricted party screening request to a dedicated application instance.
- You can increase the WebLogic TLA parameter to help when maximum number of threads are in use and are struggling for resources.

Related Topics

Screening Restricted Parties

About Restricted Party Screening

Restricted Party Screening PDF

Review Match Factor Action

This action is accessed via the following:

- Restricted Party Screening > Parties > Actions > Screening Services > Review Match Factor
- Master Data > Parties > Actions > Screening Services > Review Match Factor

This page depicts the processing details of matching the party with the restricted party. In the Party Screening – Potential Matches results page, the upper grid of the page displays all the party details while the lower grid lists all the potential restricted party matches.

Use the Review Match Factor action available in the Party manager page to determine why a particular restricted party is not considered as potential match or displayed as part of the restricted party screening result.

Additional properties that control the behavior of match factor determination are described below. The default values, which are shown below, are the recommended values.

- gtm.rps.match.useCountryCode=true specifies that the country code will be matched instead of Country Name.
- gtm.rpls.match.setMatchFactorToZero=true nullifies the contribution of unknown or empty parameter towards the overall match factor.
- gtm.rpsservice.maxresponse property specifies the maximum number of screening matches that are returned. The default value for the property is 500.
- gtm.rpls.prorateEmptyParamterWeight property to exclude an empty parameter as part of the Overall Match Factor and hence, reduce the number of false positives returned during restricted party screening. When the property is set to "true" and the Match Default is MATCH, weightage of the empty parameters is prorated among the non-empty parameters while calculating the overall match factor and is then compared with the threshold on the service preference.
  Overall Match Factor without prorating = Sum of weighted Match Factor for all non-empty parameters
  Overall Match Factor with prorating = Sum of weighted Match Factor for all non-empty parameters/ Sum of weight of all non-empty parameters
  The default value of the property is false.

Use this action to review the results of match outcome for any party against a restricted party. You need to provide Restricted Party ID and Service Preference ID values.

Note: Inverted Index matching engine is supported by this action for a quicker performance.

Reviewing Match Factor

1. Select a service preference from the Service Preference ID drop-down list.
2. Select Restricted Party.
3. Click Review Match Factor. The Review Match Factor window displays match details for each field configured in the service parameter.

Related Topics

Party Actions and SmartLinks

Screening Restricted Parties

About Restricted Party Screening

Restricted Party Screening PDF

Restricted Party Screening Resolution

Restricted Party Screening Resolution

Once restricted party screening is performed on the parties, the trade compliance user must manually verify all potential match results and mark each potential match as valid or invalid. As there can be a large number of parties and performing the review of all potential matches may be time consuming, GTM provides the concepts of Restricted Party Screening Workbench and Restricted Party Screening Work Queue to help trade compliance users quickly resolve their potential matches.

Related Topics

About Restricted Party Screening

Using the Restricted Party Screening Workbench

Creating and Using a Restricted Party Screening Work Queue

Restricted Party Screening PDF

Using the Restricted Party Screening Workbench

This page is accessed via Restricted Party Screening > Restricted Party Screening Workbench.

The Restricted Party Screening Workbench is a highly efficient clearing environment for restricted party screening potential match resolution. It provides the following capabilities:

- It uses a workbench layout to provide you with a user-friendly interface, showing all the data you need to make a resolution regarding the potential matches.
- Saved query capability helps you to determine which parties should be available in the workbench.
- Different buttons, like the Pass, Fail, Escalation, Comments, and Match Factor Review buttons are available to help you quickly take action against all potential matched restricted parties associated with a party.

To get a detailed description of all the features available on this page, please refer to the topic Restricted Party Screening Workbench.

Related Topics

About Restricted Party Screening

Creating and Using a Restricted Party Screening Work Queue

Restricted Party Screening PDF

Creating and Using a Restricted Party Screening Work Queue

A Restricted Party Screening Work Queue is a highly efficient clearing environment for restricted party screening potential match resolution. It enables you to define how work is divided into separate queues for each user to complete. It provides the following capabilities:

- Works in the same way as the Restricted Party Screening Workbench, but uses work queues to pull parties into the workbench layout instead of a saved query.
- Provides a configured distribution of work among various users with separate queues assigned to each user.
- Provides the ability to reclaim work that has been given to specific users and put it back into the primary queue.

You can create a restricted party screening work queue as follows:

1. Create a saved query.
2. Create a work queue.
3. Copy or create your new restricted party screening work queue workbench layout.
4. Add you new layout to a menu.

Then, you are ready to use your new restricted party screening work queue.

Creating a Saved Query for the Work Queue

In order to create the restricted party screening work queue, you need to first create a saved query for the work queue to use. This example creates the saved query directly in the Parties finder.

1. Go to Restricted Party Screening > Parties.
2. Enter the current domain name.
3. Click the Status tab.
4. Under Status Value 1, select the following:
    1. RPLS
    2. RPLS_REQUIRES REVIEW
    3. Same As
5. Click Save to save this as a saved query.
6. Enter a Query Name. The query name identifies the saved query and must be unique. The text that you enter is also used as the Saved Query ID.
7. Click OK. Notice that the newly created query appears in the Saved Query drop-down list.
8. Write down the new saved query ID.

Creating the Work Queue

Next, you define the details of the work queue.

1. Go to Master Data > Power Data > Configurations > Work Queue.
2. Click New.
3. Enter an ID for the work queue in the Work Queue ID field.
4. Select an Object Type of Contact.
5. Enter a Filter Limit of 50. This filter limit value limits the number of records assigned to a specific user.
6. In the Saved Query ID field, enter the saved query created above that will populate this work queue.
7. In the Assignment Duration field, enter the number of minutes of 15 for how long an assignment will last. This is only a suggestion. You can use whatever assignment duration makes the most sense for your use case.
8. From the Domain Name drop-down list select the domain of the person to whom this queue will be assigned.
9. Click Finished.
10. Write down the new work queue ID.

Now, you are ready to create a workbench layout.

Copying the Restricted Party Screening Workbench Layout

If you like the look and feel of the Restricted Party Screening Workbench, you can copy it and just the Parties region to use a work queue.

1. Go to Configuration and Administration > User Configuration > Enhanced Workbench
2. From the Layout drop-down list, select RESTRICTED PARTY SCREENING ENHANCED WORKBENCH | PUBLIC. This is the workbench that ships with GTM.
3. Click Copy.
4. Enter a Layout name.
5. Update the Description.
6. Click OK.
7. Above the Parties region, click Edit (the pencil icon).
8. Change the Population Method to Work Queue.
9. Select the Default Work Queue that you created above.
10. Click OK to save the content.

Creating a New Workbench Layout

Or, you can create your own workbench layout.

Creating a New Workbench Layout

1. Go to Configuration and Administration > User Configuration > Enhanced Workbench
2. Click the Create icon to create a new workbench layout.
3. Enter a Layout.
4. Enter a Description.
5. Select the WORKBENCH DEFAULT Logic Configuration. The list contains Workbench logic configurations. The settings defined in the selected logic configuration determine how the workbench will look and perform.
6. Select a Layout Format of Super Compact to reduce white space and make your layout more compact. This is only a suggestion. You can use whatever layout format makes the most sense for your layout.
7. Select a Domain.
8. Click OK. The blank area surrounded by the dotted line represents your workbench.

Creating the Parties Region

When creating or editing the workbench, several icons appear in the section you are editing:

1. Click  (Split Vertically) to create 2 regions.
2. To add content to the top region, click  (Add Content) in the top region.
3. Select a Component Type of Table.
4. Select an Object Type of Contact.
5. Enter a Tab Name of Parties.
6. Select a Screen Set of GTM_CONTACT_SCREENING_BOARD.
7. Select a Population Method of Work Queue.
8. Select the Default Work Queue that you created above.

9. Click OK to save the content.

Creating the Matched Restricted Parties Tab

Next, you add content to the matched restricted parties region.

1. To add content to the bottom region, click (Add Content) in the bottom region.
2. Select a Component Type of Table.
3. Select an Object Type of Party Matched Restricted Party.
4. Enter a Tab Name of Matched Restricted Parties.
5. Select a Screen Set of GTM_PARTY_SCREENING.
6. Select the Detail Table checkbox.
7. Under Associated Master Tables, select a Parties Saved Search of PARTY SCREENING MATCH QUERY.
8. Click OK to save the content.
9. When you are finished adding and editing content, click Done at the top of the page to exit edit mode and view the finished layout.

Configuration

You can set the URLs that appear in the Restricted Party pane Federal Regulation URL column to be working hyperlinks. To do so, set the following properties:

- glog.web.security.url.http.trustedDomain = www.mkdenial.com
- glog.web.security.url.https.trustedDomain = www.mkdenial.com

Adding the Layout to a Menu

Once you have created a workbench layout, you can add it to a user-defined menu to use it.

1. You can limit access to workbench layouts based on the via Configure Workbench User Access. By default, a user has access to all workbench layouts in any domains to which they are granted access via domain grants.
2. Add the workbench layout to a user-defined menu.
3. Use Manage User Access to use the menu. This can be managed at the User, Level or User Role levels.

Using the Restricted Party Screening Work Queue

Use the Restricted Party Screening Work Queue to both view and process large numbers of restricted party list screening (RPLS) results. This work queue enables a user to have exclusive access to specific records.

In addition to the enhanced workbench table icons and buttons, you see a row of icons across the top each table. You can use these icons to trigger a variety of actions.

Party Table (Contact object type)

- (Requires Review): Designates the party record as one that must be reviewed in order to determine status. The RPLS status is set once GTM performs restricted party screening of a party and there are potentially matched restricted parties assigned.
- (Passed): Sets the RPLS status of the selected party record as passed. Usually this status is set (1) if a party is screened and does not have any potentially matched restricted parties assigned or (2) by a user who reviews all the potentially matched restricted parties assigned to a party and does not see a verified match.
- (Failed): Sets the RPLS status of the selected party record as failed. Usually this status is set by a user who reviews all the potentially matched restricted parties assigned to a party and confirms a verified match between the party and a matched restricted party.
- (Escalated): Marks the selected party record for a closer examination and sets the RPLS status as escalated.
- (Add Comment): Opens the Comments on the Contact window where you can add a comment for a specific party.

Matched Restricted Parties Table (Party Matched Restricted Party object type)

- (Potential Match): Designates the matched restricted party for a particular party record as one that must be reviewed. The RPLS status is set once GTM performs the restricted party screening of a party and there is a potentially matched restricted party assigned.
- (Not a Match): Sets the RPLS status of the matched restricted party for a particular party record as passed. Usually this status is set by a user who reviews the potentially matched restricted party assigned to a party and it is not a verified match.
- (Verified Match): Sets the RPLS status of the matched restricted party for a particular party record as failed. Usually this status is set by a user who reviews the potentially matched restricted party assigned to a party and confirms there is a verified match between the party and restricted party.
- (Escalated): Marks the selected matched restricted party record for a closer examination and sets the RPLS status of the matched restricted party as escalated.
- (Review Match Factor): Displays the details for how the match factor is calculated for a specific party and matched restricted party combination.
- (Add Comment): Opens the Comments on the Party window where you can add a comment for a specific party and matched restricted party combination.

Related Topics

About Restricted Party Screening Menu

GTM Screening Overview

Restricted Party Screening Workbench

About Restricted Party Screening

About Enhanced Workbench Layouts

Enhanced Workbench

Adding Content to an Enhanced Workbench Layout

Using an Enhanced Workbench Table

Screening Service Configuration

Screening Service Configuration

GTM offers multiple trade compliance services (e.g. product classification, restricted party screening, control, license, etc.) to meet different business needs. You can define flexible configurations to meet different business needs or fine tune each service by using a combination of the service parameters and service preference entities (like Match Engine and Threshold). GTM ships with a default restricted party service preference called AD_HOC_PARTY_SCREENING_SERV_PREF. During restricted party screening, you can use the default preference or create your own service preference.

Related Topics

About Restricted Party Screening

Global Trade Content

Restricted Party List Filtering

Match Engine

Exclusion Words

Punctuation List

Match Attributes Selection

Restricted Party Screening PDF

Restricted Party List Filtering

This page is accessed via Master Data > Power Data > Configurations > Service Preference.

In GTM, you can have multiple data versions of the type 'restricted party' that are marked as current. Each of these data versions represents a restricted party list (e.g. BIS, OFAC, etc.) specified by the government, a company or a division, or red flag words list. You can specify the restricted party list against which the screening will have to be performed, using the following service preference attributes:

- Data Source: the content source for the data.
- Data Version: the data version you want to screen against.
- Agency Code: the specific agency that is responsible for the list you are screening.

Note: It is strongly suggested to filter by specifying at least one Data Source to improve the restricted party screening process.

Related Topics

Screening Service Configuration

Service Preference

About Restricted Party Screening

Restricted Party Screening PDF

Exclusion Words

This page is accessed via Master Data > Power Data > Configurations > Service Preference.

Use this page to maintain a list of exclusion words (e.g., PTE, PVT, GMBH, BLVD, etc.) as part of a service preference. You should define exclusion words that have no descriptive value or do not need to be screened. For example, the word ‘company’ is a good choice to be specified as an exclusion word as it adds no useful information to a party screening. However, words like ‘airline’ or ‘computer’ are not suitable words for exclusion. Restricted party screening service excludes these listed words from party attributes, if present, before actually performing the screening.

See the properties gtm.rpls.globalExclusionWords and gtm.rpls.useExclusionWords for more details on defining exclusion words.

Note: It is strongly recommended that you avoid including a large number of words in the exclusion list as it could result in a large number of false positives or risk of not identifying valid matches.

Related Topics

Screening Service Configuration

Service Preference

About Restricted Party Screening

Restricted Party Screening PDF

Punctuation List

This page is accessed via Master Data > Power Data > Configurations > Service Preference.

You can maintain a list of punctuation marks (e.g., hyphen "-", question mark "?", exclamation mark "!", comma ",", semicolon ";" etc.) that should be excluded in the property gtm.rpsservice.punctuationmarks. The restricted party screening service excludes these marks from party attributes and restricted party attributes, if they are present, before performing the screening. It is an application level property that will be applied to all restricted party screening services.

Related Topics

Screening Service Configuration

About Restricted Party Screening

Restricted Party Screening PDF

Match Attributes Selection

This page is accessed via Master Data > Power Data > Configurations > Service Parameter.

Restricted party screening is all about matching the party with a restricted party list. As part of this process, one of the important points is to identify the right attributes of the party to be matched with a restricted party to determine if it is a potential match or not. You can specify the list of attributes that should be considered during the screening process using the Service Parameter page. The service parameter is assigned to a service preference which is used during restricted party screening.

One practice is to use direct matching attributes, such as:

- Country attribute of the Party is matched with Country attribute of the Restricted Party
- Province attribute of the Party is matched with Province attribute of the Restricted Party
- City attribute of the Party is matched with City attribute of the Restricted Party
- First Name attribute of the Party is matched with First Name attribute of the Restricted Party
- Last Name attribute of the Party is matched with Last Name attribute of the Restricted Party
- Company Name attribute of the Party is matched with Company Name attribute of the Restricted Party

This means that when you are creating or modifying party information, you should be sure to enter the right value in the right field. Add first name in the First Name attribute or add city in the City attribute instead of entering both these attributes in the Address attribute field.

However, there may be instances where name, city or country information is entered in the Address attribute field. In such a situation, you can use a parameter such as “nameCompanyAddressCityProvinceCountry”. This parameter will internally concatenate all the attribute values of name, company, address, city, province, and country for both the party and the restricted party and then perform the match.

Note: It is strongly recommended that you use direct matching attributes (e.g. country parameter) wherever possible and enter the right value in the right field. By using a parameter such as “nameCompanyAddressCityProvinceCountry”, the quality of the match results might decrease and could produce a large number of false positives or might not identify valid matches.

Other key points related to parameter selection are match factor and weight, which contribute towards the overall matching of a party with a restricted party.

For every parameter (match attribute) configured, GTM determines a match factor (matching percentage) between the party and the restricted party and then compares it against the corresponding threshold. The threshold field can be used to filter out the restricted parties which have low match factor for a particular

parameter with the result that they are not considered possible match. You can define a threshold between 0 and 1.

Once GTM determines that a parameter is a match between the party and the restricted party, its match factor is used along with the weight to calculate the adjusted match factor for that parameter. After all the parameters are screened and determined to be a match, an overall match factor is calculated using the adjusted match factor of individual parameters according to the following formula. The sum of all parameter weights should be equal to 1.

Overall Match Factor = (Match Factor * Weight) of Parameter1 + (Match Factor * Weight) of Parameter2 + ……+ (Match Factor * Weight) of last Parameter, where, Adjusted Match Factor of parameter1 = (Match Factor * Weight) of Parameter1

Note: It is strongly recommended that you provide a higher threshold (1 or near to 1) for parameters wherever possible. By default, the restricted party screening process will first match those parameters that have the highest threshold. If the match threshold fails, GTM stops matching other parameters immediately and thereby increases restricted party screening performance.

Note: It is strongly recommended that you set the weight of parameters (match attributes) such as country and/or city as 0. Setting the weight of parameters to 0 means that these specific parameters (e.g. country or city) will have to pass the individual parameter match factor threshold, but they would not contribute towards the overall match factor. Another way of looking at it could be that you want the country and city attributes to match completely, while you want other attributes like address, company name to contribute more towards the overall match factor.

Additional properties that control the behavior of match factor determination are described below. The default values, which are shown below, are the recommended values.

- gtm.rps.match.useCountryCode=true specifies that the country code will be matched instead of Country Name.
- gtm.rpls.match.setMatchFactorToZero=true nullifies the contribution of unknown or empty parameter towards the overall match factor.
- gtm.rpsservice.maxresponse property specifies the maximum number of screening matches that are returned. The default value for the property is 500.
- gtm.rpls.prorateEmptyParamterWeight property to exclude an empty parameter as part of the Overall Match Factor and hence, reduce the number of false positives returned during restricted party screening. When the property is set to “true” and the Match Default is MATCH, weightage of the empty parameters is prorated among the non-empty parameters while calculating the overall match factor and is then compared with the threshold on the service preference.
  Overall Match Factor without prorating = Sum of weighted Match Factor for all non-empty parameters
  Overall Match Factor with prorating = Sum of weighted Match Factor for all non-empty parameters/ Sum of weight of all non-empty parameters.
  The default value of the property is false.

Related Topics

Screening Service Configuration

Service Parameter

About Restricted Party Screening

Restricted Party Screening PDF