Gold Client for Data Protection
Solution 2.0
User Guide

Copyright

Trademarks

Introduction

This document serves as a guide for configuring and using the Gold Client for Data Protection Solution.

If a user needs to know how to Obfuscate a set data, this is the user guide that they should reference. The Obfuscation process consists of three basic steps: (1) Qualify, (2) Review, and (3) Obfuscate.

Illustrated within this document are the step-by-step instructions for executing the various steps within the obfuscation process, as well as how to use the other various (optional) features that are available. Additionally, this document covers the steps needed for restoring data that was previously obfuscated with Gold Client for Data Protection Solution.

Gold Client for Data Protection Solution

Overview

Transaction Code /GDPR/GCDPS will display the main screen.
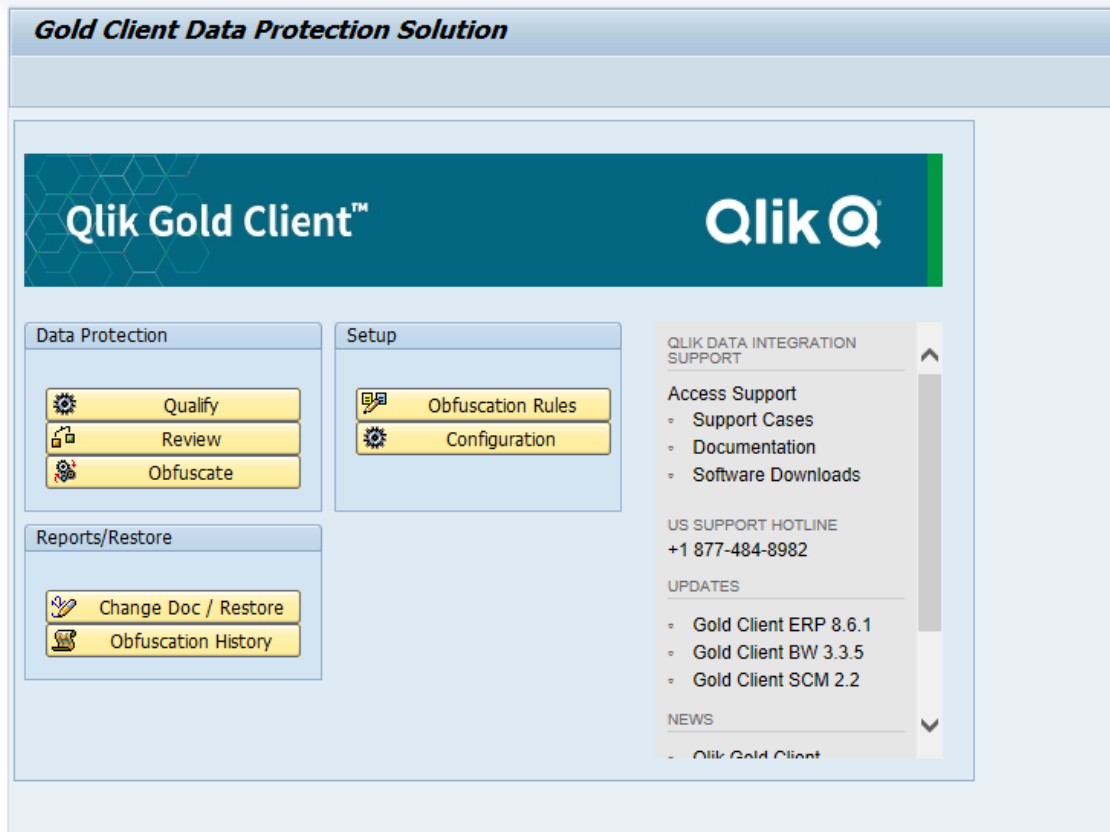
Data Categories

Qlik currently supports the following main data categories:

- Customer Master
- Vendor Master
- Business Partner
- Employee Master
- CRM – Transactions
- CRM – Business partners
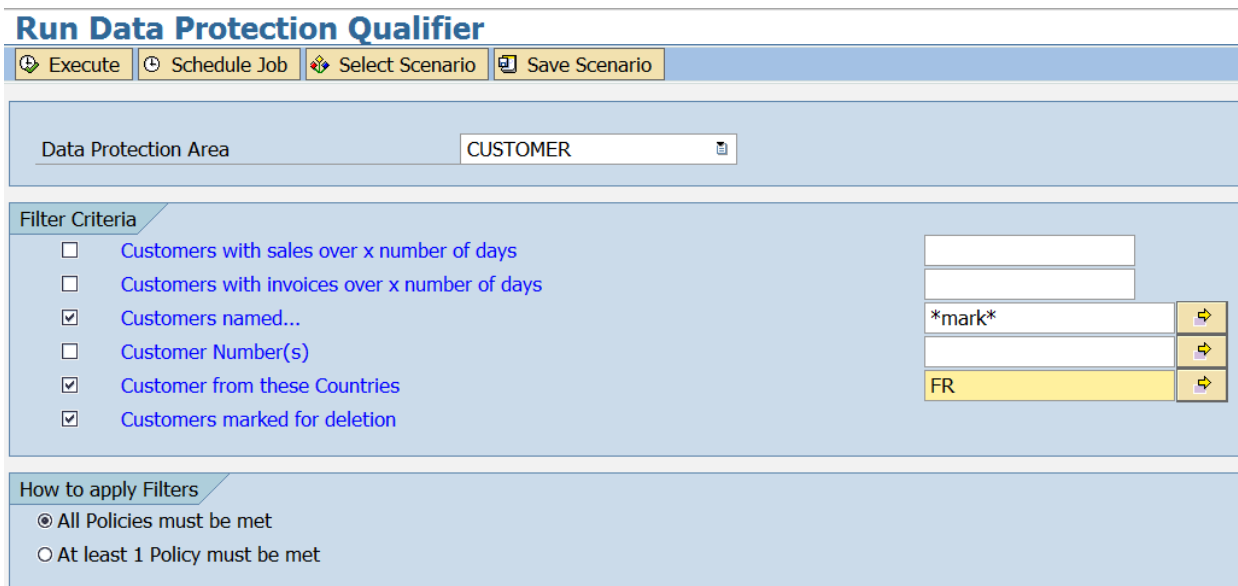
Qualify

The Qualify utility will allow you to select data based on policies. This is the first step of the data obfuscation process.
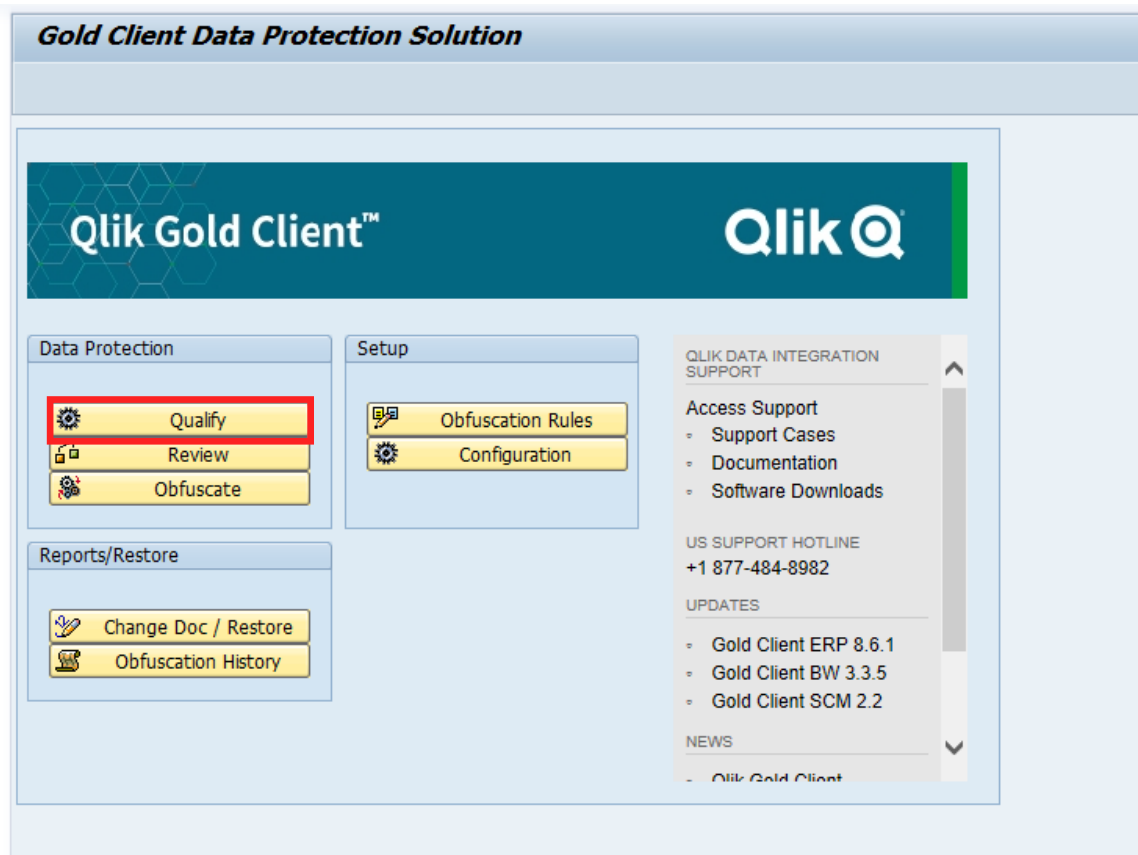
When you click on the Qualify button, it brings the following screen. Click Data Protection Area list box to select the area for which you want to run data qualification/Obfuscation.
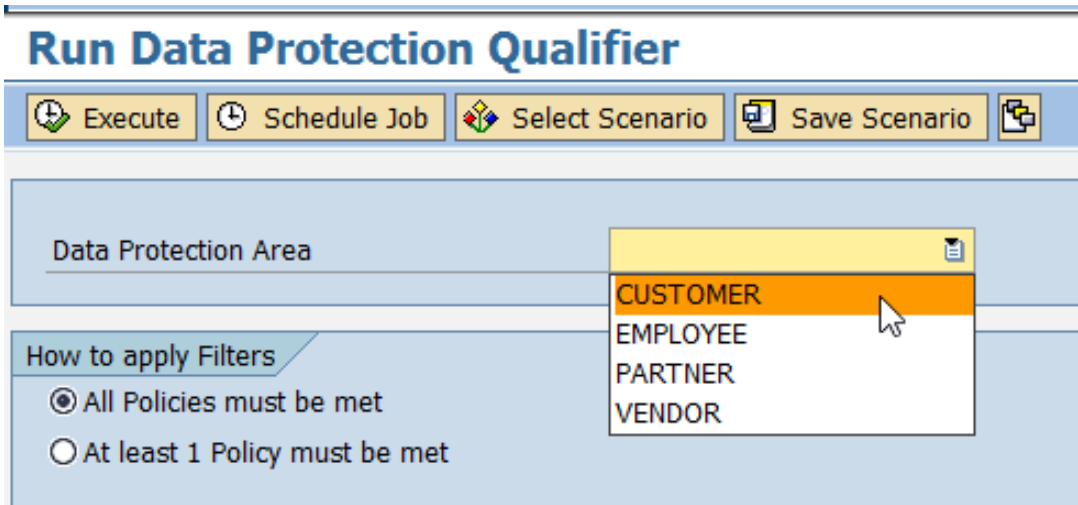

Once you select the data protection area, the program generates a dynamic selection based on the policies defined for the area.
A Selection Screen is created and one or several policies can be selected.

Previous saved scenarios can be used were by clicking on Select Scenario or you can create your own.
It can be executed the data qualifier in Foreground or Schedule a background job.
You can also save the policy selection as Scenario by clicking on Save Scenario button from the menu.

Once you click on Execute or Schedule Job, a pop screen comes up with default Obfuscation rule for the data protection area. You can choose a different obfuscation rule.
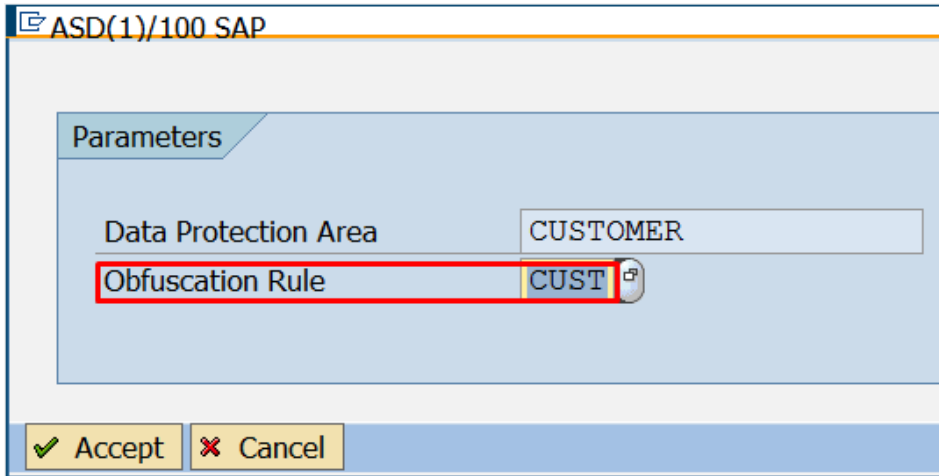
Click on Accept to continue. If you want to cancel the run, click on Cancel button. When running in Online mode, you will get a popup screen with a summary of how many total records qualified for the policy selection that include new and old which are still waiting for review for further processing.
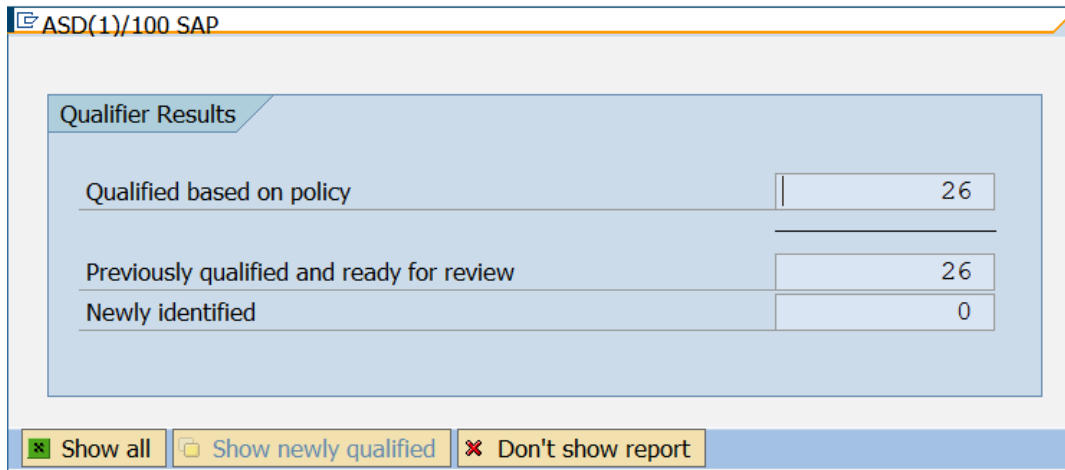
Click on Show All to view all the qualified data (old and new), Click on Show newly qualified to only see new data or click on Don't show report if you do not want to review the data right away. You can always to Review screen from main screen to view and act on the qualified data.

When you click on Show all or Show newly qualified, it takes you to review details screen where you can see the details and take required action.

Gold Client Qualifier Data Review

Data Protection Area	CUSTOMER
Transformation Rule ID	CUST
Runtime ID	20181203125831BOKWFG

🔍 🖨 🏷 🔍 🔍 ▽🗋 ⊞ 🔧 | 🖋 Approve | 🖋 Reject | 🔠 Exclude | 🗑 Obfuscation Queue

General Data in Customer Master

Custom.	C.	Name 1	Name 2	City	Post.Code	Rg	Search term	Street	Telephone 1	Fax Number
3090	US	Star Supermarkets		CHICAGO	60660	IL	MSA	1 1 100 Drury Street	333-23222-123	333-23222-124
3215	US	Inrstore Superma		OCEANP	07757	NJ	SERVICES	180 180 West Des	732-870-3200	732-870-3208
3720	US	Woodfield Super		Chicago	60173	IL	MSA	4321 Buffalo Rd	312-440-3570	312-440-3590
20008	US	Supermarket chai		WASHIN	20005	D	TPM	103 Beach St		
100140	US	First Hyper's Sup		New York	10015		HYPER'S SU	3999 West Chester		
100206	US	First Hyper's Sup		New York	10015		HYPER'S SU	3999 West Chester		
300831	US	Intermarket HQ		NORTH C	14514	N	TPM	75 Roseship St		
300832	US	Intermarket North		SILVER L	14549	N	TPM	86 Strawberry St		
300833	US	Intermarket 1086		SOUTH P	10090	N	TPM	5 Raspberry St		

Review

This utility to review and approve the recent qualified data. This is the second step of the data obfuscation process.

Select the data protection area to display the list of all qualifier run header level details (Runtime ID, Area, Date and Time, User, Record Count and Obfuscation rule) where you have several options:

Show Details:

Select any row(s) and click on Show Details button to the qualified data.

Approve Data:

Select the row(s) click on Approve button to add the record to the obfuscation queue.
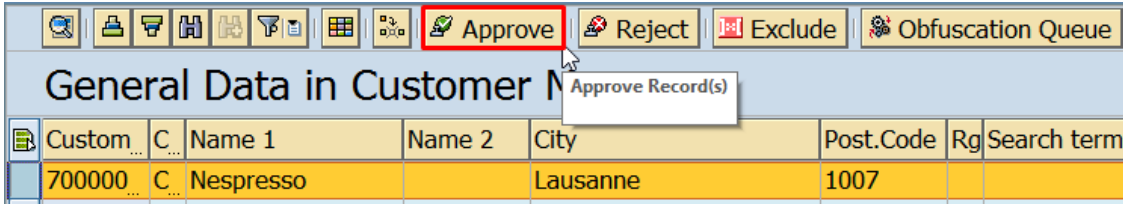
A popup will be prompted to confirm the action. Once the record(s) is approved it will disappear from the queue.
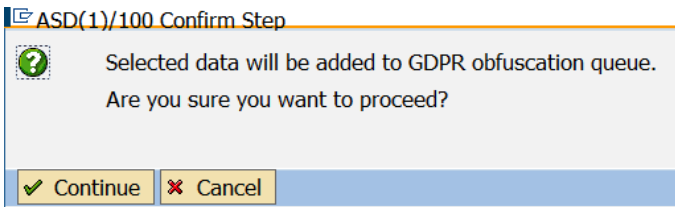
Click on Continue to add the record to the queue or click cancel if do not want to proceed further.

Reject Data:

Select the row(s) click on Reject button to reject the data. The record(s) will be deleted from review Qualification area.

By doing this the record(s) can be Qualified again.
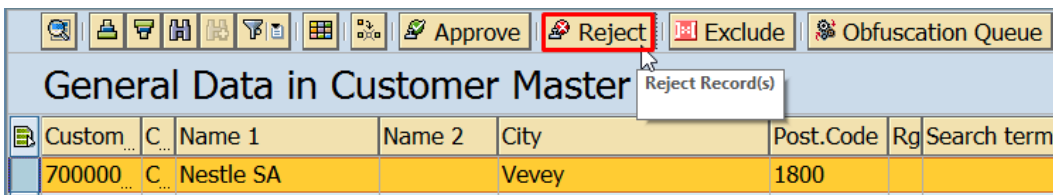
A popup will be prompted to select a reason and confirm step.
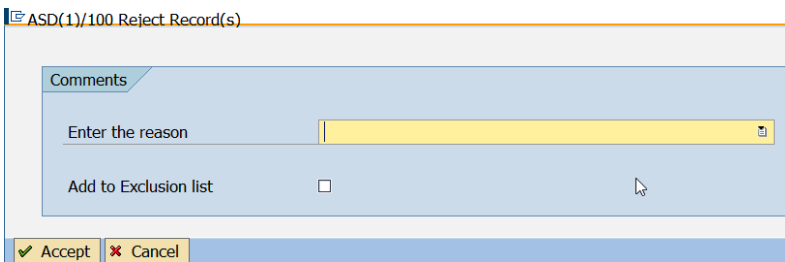
Click on the pre-populated reason list and select a reason. You can also click on the checkbox to add the record to exclusion list. Click on Accept to continue or click cancel to cancel the action.

Exclude Data:

Select the row(s) click on Exclude button to add the record(s) to the exclusion list.
These records are always excluded from re-qualification and/or data processing.
The exclusion List can be managed from Review -> Exclusion Report

A popup will be prompted to select a reason and confirm step.
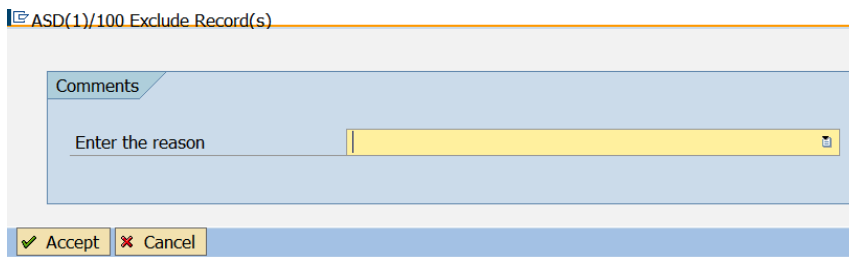

Click on the pre-populated reason list and select a reason. Click on Accept to
continue or click cancel to cancel the action. To view all the previously excluded
records, go back to main screen and click on Exclusion report from ALV menu.

Obfuscation Queue:

Click on the Obfuscation Queue button to go straight to Obfuscation and view the
data that have been already approved for obfuscation.
*Is not required to select any row(s) for this function.
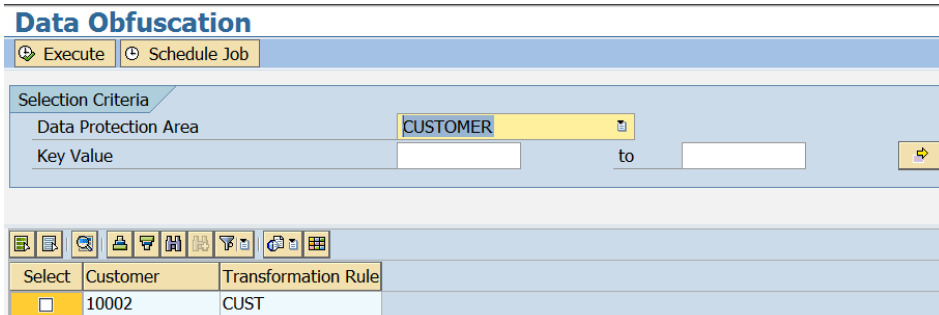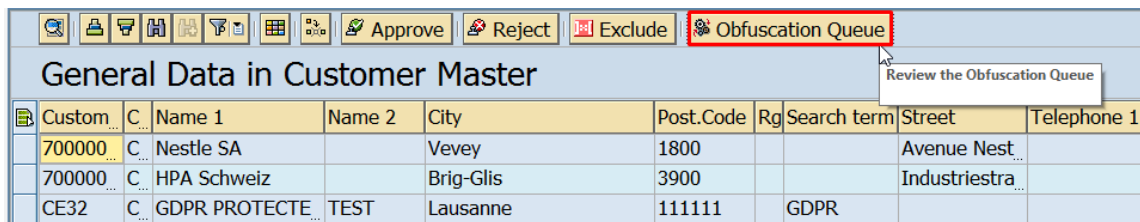
Exclusion Report:

Click on the Exclusion report button to review/manage all the records that have been marked as Excluded.
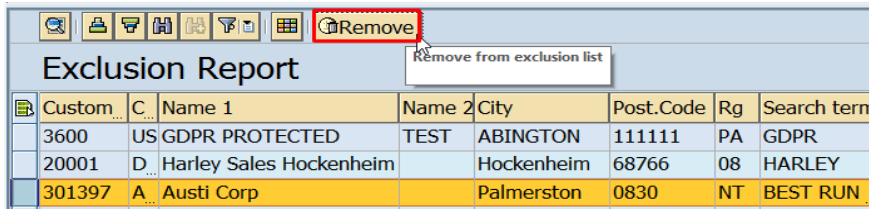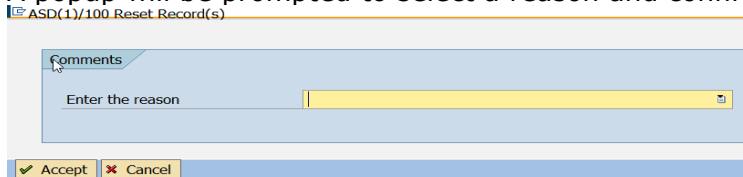

Exclusion Report - Remove:

Select any row(s) from the list and click on Remove button to remove the record from the exclusion list. Once you do this, the record will re-qualify on the next policy run.

A popup will be prompted to select a reason and confirm step.

Click on the pre-populated reason list and select a reason. Click on Accept to continue or click cancel to cancel the action.

Delete:

Select any row(s) and click on Delete button to delete the quailed data from review staging area. This permanently deletes the records from /GDPR/ tables and a new Qualification will be required.
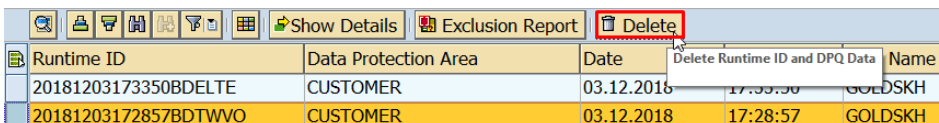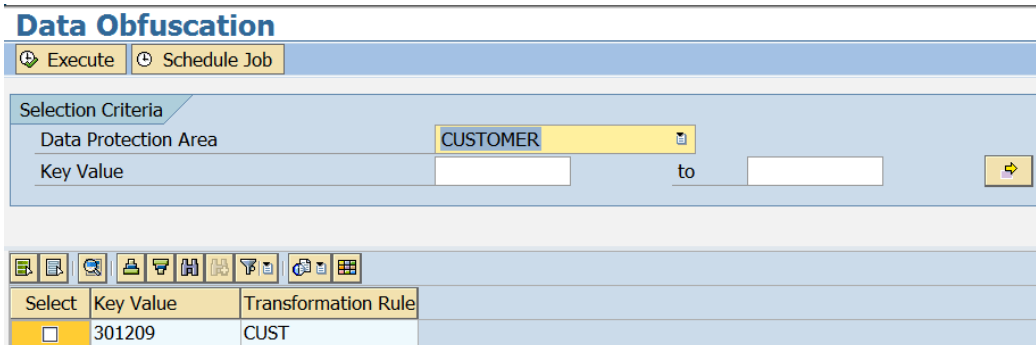
Obfuscate

This utility applies the data obfuscation rules to the data and update the database tables. This is the third and final step of the data obfuscation process.
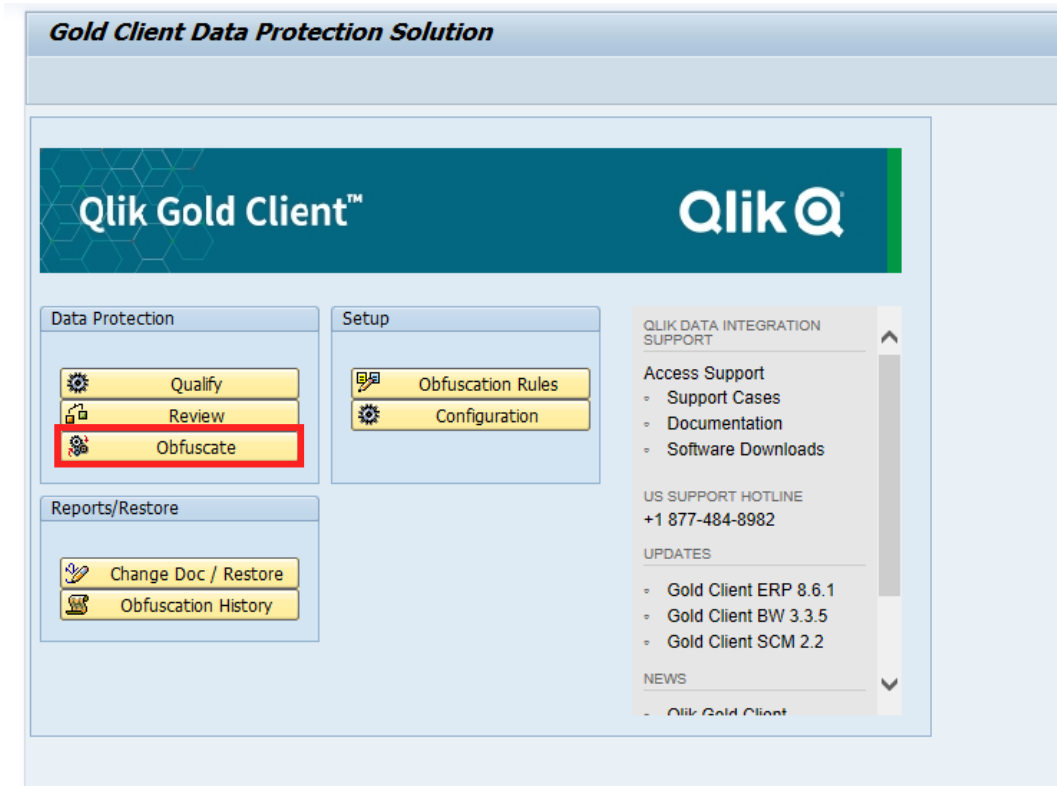
By selecting Obfuscate button and Data Protection Area, it will display all the qualified and reviewed records.

From this screen you can select the record(s) to be Obfuscated
After the data selection, click on Execute to run in online mode or schedule a background job.

Summary report is displayed for all the records that are processed.

Once the data is processed, change history is updated. You can view the changed values by going to Change Doc/Restore utility.

Change Doc/Restore

Execute this utility to view the change doc history for the records that have been obfuscated. It also allows you to restore the original values if required.

When you execute the report, it displays header level information. You can filter records based multiple selection criteria.
Click refresh button from the menu to refresh the data selection.

To view the field level details for a change doc, double click anywhere on the row.

Change Doc/Restore - Restore

To restore the fields to its original values, select the record from main screen and click on Restore button from the menu. The utility reads the change history table records and updates to the last original values that are available. Once the data is restored, the records may re-qualify on the next qualifier process run.

Obfuscation History

This provides complete trace of when the data was qualified, and subsequent actions taken. You have many options to query the data to find out specific details.

By default, all deleted records are removed from original selection screen.

Obfuscation Rules

Setup obfuscation rules for protecting your data.
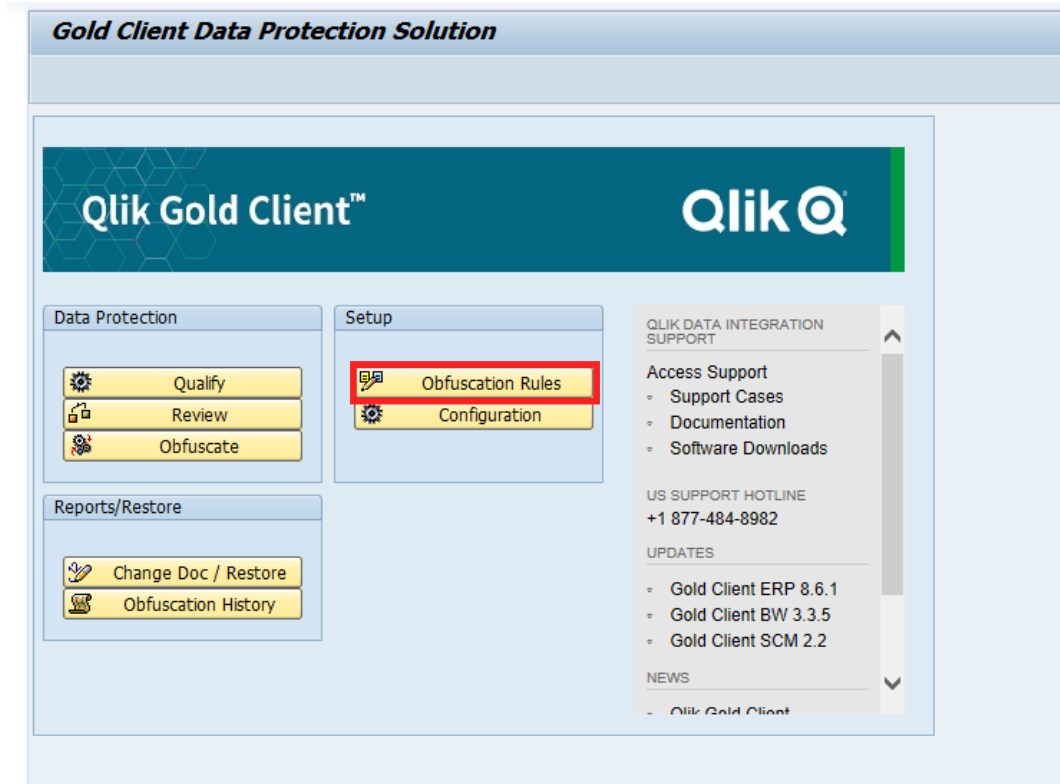
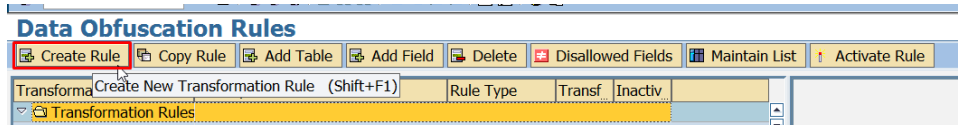Qlik delivers pre-configured rules that can be changed based on your need.

Create Rule:

To create a new obfuscation rule, click on the Create rule button from the menu.

It opens a popup window with proposed rule id.
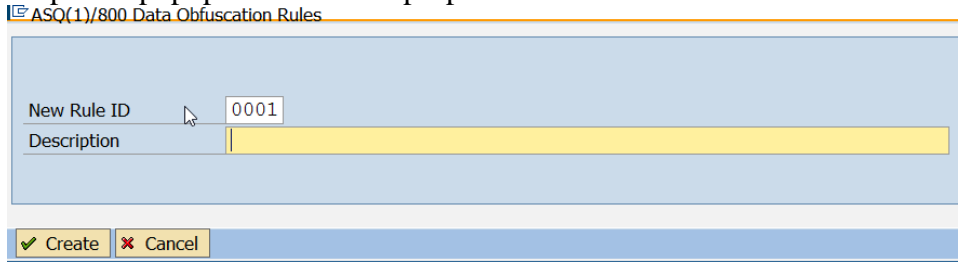
You can enter any alpha numeric value or keep it. Enter the description and click on Create button.
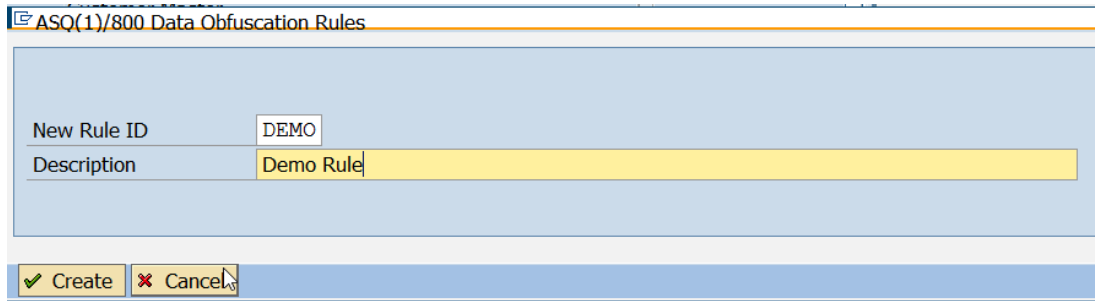
Or you can select a rule, make a copy and make the changes you want.
After creating the rule, click on Add Table to add that to the rule. The table name needs to be added in the configuration utility "Maintain Data Prot. Tables".
After that you need to click on Add Field to add specific fields that you want to obfuscate. When we add field, by default they are assigned rule type "Blank". Double click on the field name to open the rule and select the rule type from the available options and set the values.

Configuration
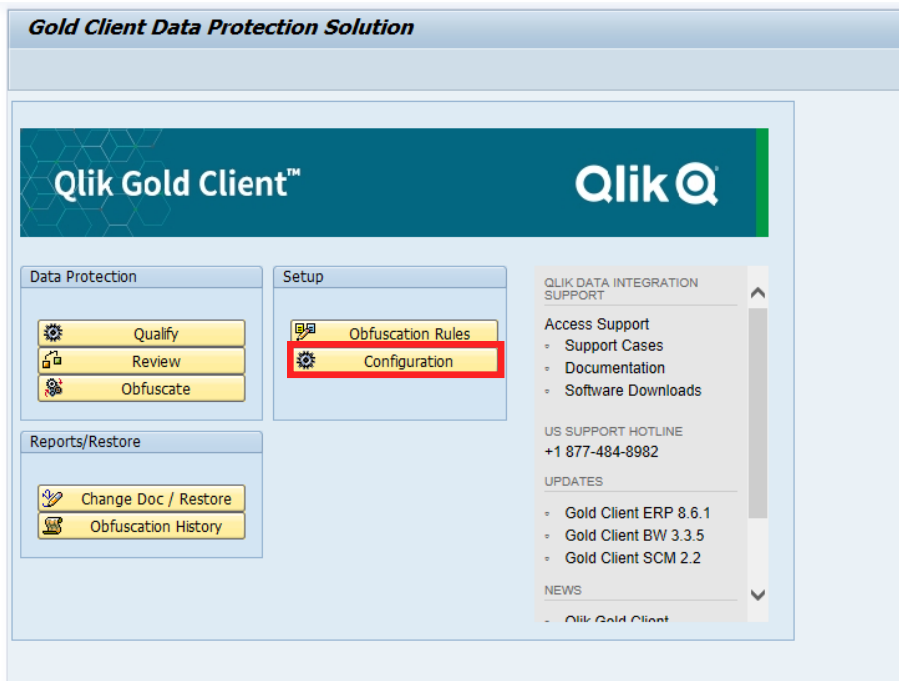
Click on the configuration button to access various configuration utilities. You need to have change authorization to make any changes.
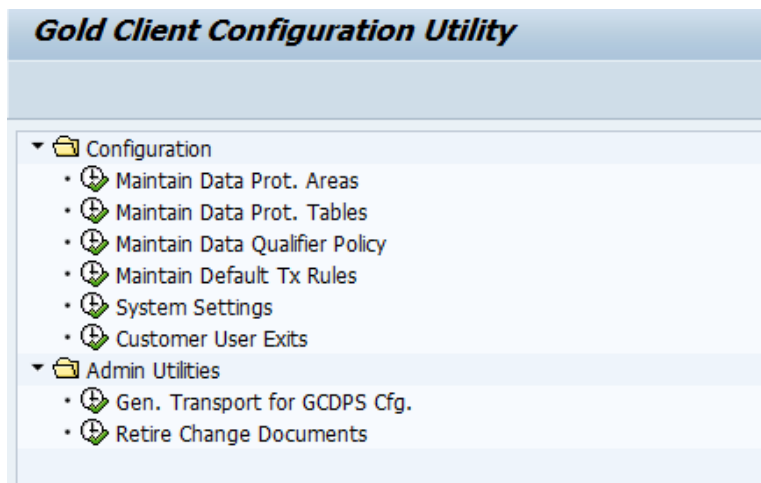
Maintain Data Protection Areas:

This is pre-populated, and no changes should be made to this.

Maintain Tables for Data Protection Areas:

The tables listed here are only allowed for obfuscation rules. Currently this is very limited and should not be changed.

It's possible to map standard tables (ex: BUT000) or Custom Tables (ex: ZCARLOS), but you have always available our own structures (ex: /GDPR/BUSINESSPARTNER) that reflects the standard tables, standard fields and any append custom fields/structures.

Maintain Data Qualifier Policies:

This is a crucial utility to maintain the policies that are required for data qualification. The directly controls the Qualify selection screen parameters.
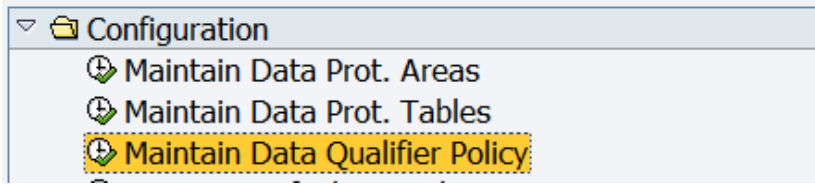
Select the data protection area from the list.

Maintain Data Qualifier Policies

Data Protection Area	
	BUS.PARTNER
	CUSTOMER
	EMPLOYEE
	VENDOR
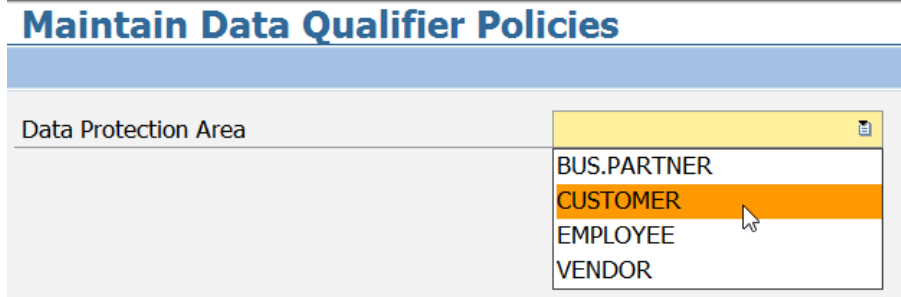
It will display all the policies that have been defined for the data protection area. You can add new policy and/or change, delete policies based on your requirements. For each new policy you need to either create a new function or raise a request to Gold Client support team. Once a policy is used for a saved scenario, you cannot change or delete it.

Maintain Policy Functions for CUSTOMER

DPR	Policy	Function	FM Description	SelScr Element Type	Active
CUSTOMER	1	/GDPR/DPQ2_CUSTOMERS_NAMED	Customers named...	Select Option	☑
CUSTOMER	2	/GDPR/DPQ2_CUST_DELETION_MARK	Customers marked for deletion	No Input Required	☑
CUSTOMER	3	/GDPR/DPQ2_CUSTOMERS_KUNNR	Customer Number(s)	Select Option	☑
CUSTOMER	4	/GDPR/DPQ2_CUST_COUNTRY	Customer from these Countries	Select Option	☑
CUSTOMER	5	/GDPR/DPQ2_CUST_SLS_OVER_XDAY	Customers with sales over x number of days	Parameter (Numeric)	☑
CUSTOMER	6	/GDPR/DPQ2_CUST_INVC_OVER_XDAY	Customers with invoices over x number of days	Parameter (Numeric)	☑

You can add/create your own by just maintain the DPR and incremental policy number.

Assign Default Obfuscation Rules for Data Protection Area:
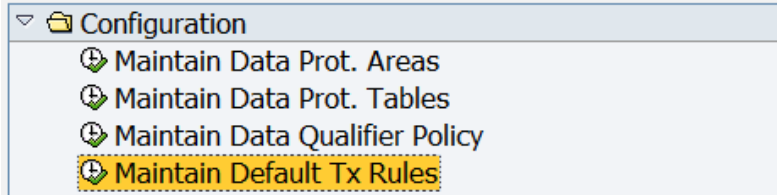
To be able to run Obfuscation you must connect the Data Protection Area to the Transformation rule.

System Settings:

These are global setting that can impact different process and only ADMIN's should add and/or change.
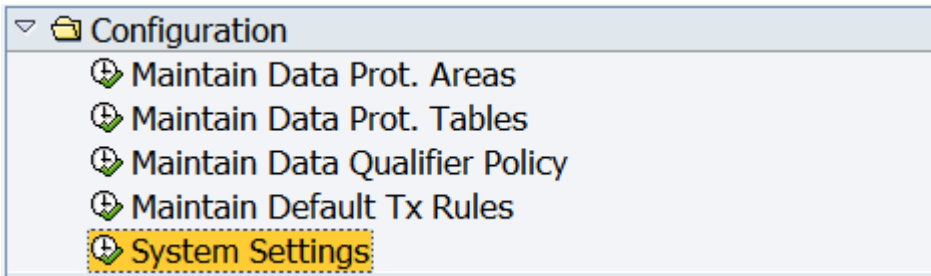
CDRETENTIONPERIOD
- Retention period in days (ex: 30 to 180)

FRAMEWORKLOG
- Must be '**X**' to have audit on workflow (change traceability)

INITSAPCHANGEDOC
- Must be '**X**'

X_ALLOW_CONFIG_CHANGES
- Must be '**X**' To allow configuration changes

X_DISABLE_SECURITY
- Must be '**X**' To disable security (authorizations) to run the GC4DPS

Customer User Exits:

This utility allows the users to run external ABAP code, leveraging the GC4DPS transformation rules and process control tables to track the changes.
With this its possible to manage other areas that GC4DPS cannot address.

Gen. Transport for GCDPS Configuration.

This utility allows the user to create transport(s) for the GC4DPS configuration to be moved to production.

Retire Change Documents

This utility put the Obfuscated data to be Expired, no change/restore will be possible after this step.
It updates /GDPR/ tables that hold the original field values with a fixed text "Expired". Once the values are marked as expired, they cannot be used for restoring the fields to its original values.

© 2012-2021 Qlik Analytics (ISR) Ltd.
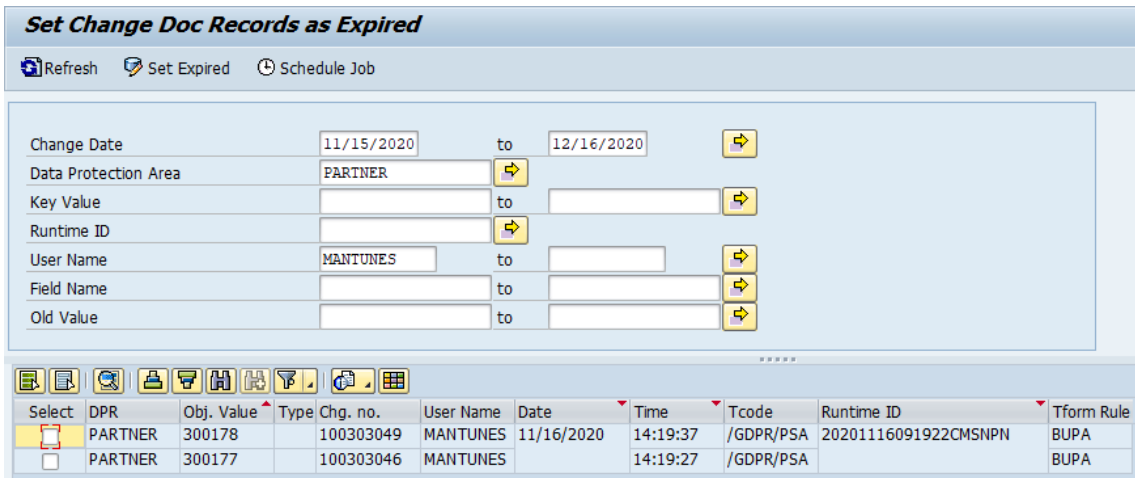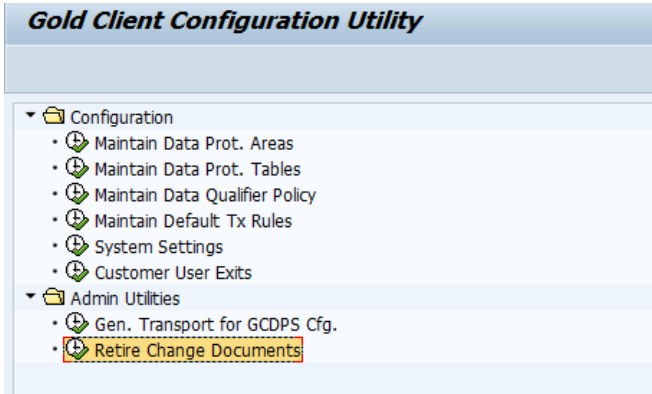
Support Information

Qlik Analytics (ISR) Ltd. can be contacted either by telephone or via email. Any support related issue regarding problems with or use of the Gold Client software and process can be reported for resolution.

If our offices are closed, or staff is unable to directly respond to a support request, we will respond within 24 hours of the initial call. Problems related to the export or import processing may require code enhancements. If a code enhancement or fix is required, resolution time may vary.

As per the maintenance agreement, any repairs or enhancements to the Gold Client software will immediately be deployed to all customers up-to-date with their maintenance contract. It is the choice of the customer as to if and when such enhancements are implemented. In addition, customers may request a planning session with Qlik to review changes in the software and how the changes might impact their environment.

We can also be contacted to discuss application or feasibility of using the Gold Client process to resolve a current challenge the project team faces. When this is required, a planning session can be scheduled in advance to ensure proper participation by both Qlik and the client.

Corporate Offices:

QLIK TECHNOLOGIES INC.
211 South Gulph Road
Suite 500
King of Prussia, PA 19406
United States

Website:

https://www.qlik.com/us/products/qlik-gold-client

Contact:

goldclient.support@qlik.com

1-877-484-8982 (Toll Free in the USA)