



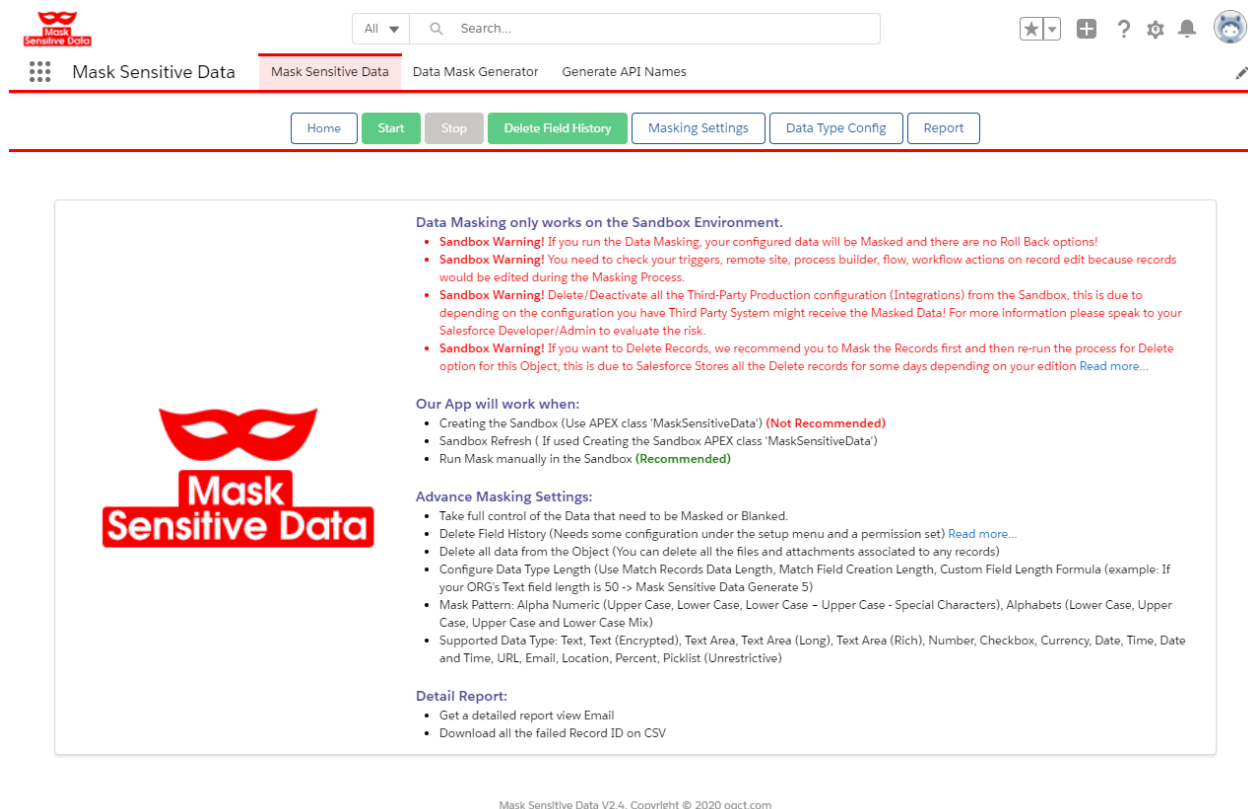
Mask Sensitive Data 2.4 Guide

User Guide

1. Introduction.....	5
1.1. About Application	6
1.2. Warning!	7
1.3. General App Information	8
1.4. Button Actions	8
1.5. Features	10
1.6. Requirement.....	11
2. Install Instructions.....	11
2.1. Step-1: Assign Permission Set.....	13
2.2. Step-2: Deliverability	14
2.3. Step-3: (Recommended in Sandbox).....	15
3. App Configuration.....	18
3.1. Step-4: Configure the Metadata	18
3.2. Step-5: Email and URL Format	20
3.3. Step-6: Phone Data Type Format	22
3.4. Step-7: TEXT Data Type Format	23
3.5. Step-8: Number, Currency, Percent Data Type Format.....	25
4. How to ?	27
4.1. How to Mask Manually?	27
4.2. How to Mask Data Automatically (While Sandbox refresh)	28
4.3. How to Delete Field History ?.....	29
4.4. Data Mask Generator - Manual.....	30
4.5. Data Mask Generator - CSV	32
4.6. Generate API Names	32
4.7. Assign App to New Admin.....	33
4.8. How to find Failed Masking Data	36
4.9. How to Stop Masking	38
5. App Uninstall	38

6. Contact us 40

1. Introduction



Mask Sensitive Data

Data Masking only works on the Sandbox Environment.

- **Sandbox Warning!** If you run the Data Masking, your configured data will be Masked and there are no Roll Back options!
- **Sandbox Warning!** You need to check your triggers, remote site, process builder, flow, workflow actions on record edit because records would be edited during the Masking Process.
- **Sandbox Warning!** Delete/Deactivate all the Third-Party Production configuration (Integrations) from the Sandbox, this is due to depending on the configuration you have Third Party System might receive the Masked Data! For more information please speak to your Salesforce Developer/Admin to evaluate the risk.
- **Sandbox Warning!** If you want to Delete Records, we recommend you to Mask the Records first and then re-run the process for Delete option for this Object, this is due to Salesforce Stores all the Delete records for some days depending on your edition [Read more...](#)

Our App will work when:

- Creating the Sandbox (Use APEX class 'MaskSensitiveData') (**Not Recommended**)
- Sandbox Refresh (If used Creating the Sandbox APEX class 'MaskSensitiveData')
- Run Mask manually in the Sandbox (**Recommended**)

Advance Masking Settings:

- Take full control of the Data that need to be Masked or Blanked.
- Delete Field History (Needs some configuration under the setup menu and a permission set) [Read more...](#)
- Delete all data from the Object (You can delete all the files and attachments associated to any records)
- Configure Data Type Length (Use Match Records Data Length, Match Field Creation Length, Custom Field Length Formula (example: If your ORG's Text field length is 50 -> Mask Sensitive Data Generate 5))
- Mask Pattern: Alpha Numeric (Upper Case, Lower Case, Lower Case - Upper Case - Special Characters), Alphabets (Lower Case, Upper Case, Upper Case and Lower Case Mix)
- Supported Data Type: Text, Text (Encrypted), Text Area, Text Area (Long), Text Area (Rich), Number, Checkbox, Currency, Date, Time, Date and Time, URL, Email, Location, Percent, Picklist (Unrestrictive)

Detail Report:

- Get a detailed report view Email
- Download all the failed Record ID on CSV

Mask Sensitive Data V2.4, Copyright © 2020 oqct.com

Mask Sensitive Data App is designed to Mask your Production Sensitive Data in Sandbox. We developed this app so you do not have to worry about having your production Data in the Sandbox Environments!

For Small Cost our app will help you to:

- Comply GDPR Law
- Comply CCPA
- Protect your Customer Data in Sandbox Environment
- Speed your Development
- Speed your Testing/ Bug Fix before going Live with Real Masked Data
- If your Sandbox ORG connected to Third Party Test Systems and if you want to Mask both system! (You ORG must have a connection in place between both system and you must send data every time when a Data Modification happens)

Please read our Warning! Section before buying our application!

1.1. About Application

Mask Sensitive Data application will aid users who want to secure their sensitive data in the production environment on moving it in the Sandbox environment.

The Problem:

The primary concern from a corporate governance perspective is that personnel conducting work in these non-production environments are not always security cleared to operate with the information contained in the production data. This practice represents a security hole where data can be copied by unauthorized personnel and security measures associated with standard production level controls can be easily bypassed. This represents an access point for a data security breach. The overall practice of Data Masking at an organizational level should incorporate processes for the distribution of masked test data subsets.

The application was designed focusing on the following issues:

- Regulatory compliance:

In recent years, new privacy regulations such as the European Union (EU) General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) require companies to evaluate their technical and organizational controls to ensure compliance. Industry-specific standards and regulations such as the Payment Card Industry Data Security Standards (PCI DSS) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) also include strict privacy and security requirements.

Data governance issues can cause significant repercussions for your business, including loss of customer trust and legal consequences, including regulatory fines. GDPR infractions alone can lead to fines of up to 4% of annual global revenues, or \$20 million, whichever is greater.

While production environments are continuously scrutinized for security or privacy leaks, sandbox environments are sometimes lower priority because they're used only for testing and development. However, developers or contractors who are working in sandboxes could have access to data that would otherwise be restricted in production. Mindful of these complex privacy requirements, Mask Sensitive Data app can mask the sensitive data copied from the Production environment to Sandbox.

- Insider threats:

Data breaches initiated from outside the organization get the lion's share of attention, but a 2013 study by the Open Security Foundation found that close to 20% of incidents started inside the organization, and these were responsible for almost 70% of exposed data. While developers, administrators, and QA engineers have a legitimate need for test data, they do not need access to sensitive and confidential information from the live Salesforce environment. Masking live data ensures that those who need access to data can perform their job, without increasing the risk of compromising data during a breach

- External parties:

Outside consultants and service providers play an essential role in many organizations, and it is not uncommon for staff to share data with third parties as part of their daily routine. These transactions have the potential to expose the organization's most sensitive Salesforce data. Data masking is an effective way of mitigating this risk. Masking production data ensures that staff and outside vendors can share access to test data without compromising sensitive and confidential information from the production environment.

The Solution:

'Mask Sensitive Data' application is designed for masking sensitive data field to protect data that is classified as personally identifiable information, sensitive personal data, or commercially sensitive data. It is common to have masking applied to data that is represented outside of a corporate production system, in other words, where data is needed for the purpose of application development, building program extensions and conducting various test cycles. It is common practice in enterprise computing to take data from the production systems to fill the data component, required for these non-production environments, i.e., Sandboxes.

1.2. Warning!

- Please read the user guide and know your Salesforce ORG before using our Application!
- In Sandbox: **Warning!** If you run the Data Masking, your configured data will be Masked and there are no Roll Back options!
- In Sandbox: **Warning!** You need to check your triggers, remote site, process builder, flow, Workflow Actions due to Edit Data Modification Action will be performed in order to Mask your Data!
- In Sandbox: **Warning!** Delete all the Third-Party Production configuration from the Sandbox, this is due to depending on the configuration you have Third Party System will receive the Masked Data! For more information please speak to your Salesforce Developer/Admin to evaluate the risk.
- In Sandbox: **Warning!** If you want to Delete a Records/Object we recommend you Mask the Records/Object first and then re-run with Delete option for this Object, this is due to Salesforce Stores all the Delete records for 15 days**.

You must evaluate your Salesforce Environment before using our Application! this is due to each Salesforce ORG is different.

We will not take any responsibility for your Data Lost!

1.3. General App Information

- * Our app will not "Start" (Mask) on Production Environment or delete any Production Data!
- * If you want to "Mask your Data" while creating the Sandbox or when Refreshing your sandbox, you need to install this app on your Production Environment. And when creating the Sandbox you need to assign a APEX Class on the Sandbox template "MaskSensitiveData"
- * This App requires a System Permission "Field History Delete" ENABLE to delete all the Field History from your sandbox. (We recommend you do this on your sandbox every time, so no one delete your production data)
- * This App also requires a Field History Delete Permission Set assigned to the Profile. (We recommend you create this permission set on your sandbox and assign it to the profile every time, as it will only take 5 minutes)
- * If you don't want to Obscure the Data while creating the Sandbox or at Refresh stage, you can run it manually by going to the App and click on "Start"
- * This App needs "Deliverability" turned on Sandbox/Production in order to email the Obscure results.
- * App will work on Full Sandbox, Partial Copy Sandbox, Developer Pro Sandbox and Developer Sandbox
- * Up on completion of the Obscure the Data the System will send an email to the Running users, this is only if you run the script manually.

1.4. Button Actions

Start = If you want to run the Data Masking manually then click here! up on completion email will be sent to the running user.

Delete Field History = If you want to delete the Field History click here! Up on completion an email will be sent to the running user.

Masking Settings = Here you will be able to see all the Data Masking Objects and Fields

Create/Edit Config = If you want to Create/Edit the Masking Objects and fields you will be able to do it here

Data Type Config = You will be able to see all the Data type the "Mask Sensitive Data" App can do and also you will be able to edit some Data type.

Edit Data Type = You will be able to edit the Data types settings here!

Mask Sensitive Data Objects = Here you will be able to Create/Edit the Masking Objects (STEP View)

Mask Sensitive Data Object Config = Details of Masking Objects and Fields (STEP View)

Label = API Name of the Object that you want to mask

Mask Sensitive Data Object Name = We are not using this fields in our CODE, this fields something salesforce put automatically, just make sure it has some unique text, if you are going to put the API name just remove the __C

Mask Fields (API Name) = All the API names of the Fields that you want to mask, the data type will be captured automatically and the field length will be captured automatically.

Fields not to copy (API Name) = If you don't want a one fields to Copy or Masked then you can put that API name here, our Code will delete all the data from that fields. (ie you don't want to Copy the Customer Credit Card details similar sensitive information and you don't want to mask the Data)

Enable Field Masking = In here if you want to Enable Field masking for this object you must tick here, otherwise it will not Mask this Object.

Delete All Records From Object = If you don't want to copy anything from a object, you can just put the API name of the Object and Tick here. The Code will delete everything from this Object (ie if you don't want to copy any Attachments or Notes to the Sandbox for any confidential reason you can add the API here and it will delete all the Attachments/Notes.)

Mask Sensitive Data Types = Here you can edit your Data Type and Settings

Your Email Domain > Domain Name: If you added an Email Data Type fields on the Config and if you want to change your email domain name then you can click here and Edit the "Domain Name" and Save, this will change the email domain name when you click on the "Re-Run Mask Sensitive Data" or when its creating/refreshing the Sandbox .

Your URL Domain > Domain Name: If you added a URL Data Type on the data Masking, and if you want to change all the URL to your own Dummy domain name you can update here.

APEX Class = For Sandbox Creation "MaskSensitiveData"

1.5. Features

- **Edit configuration:** Make use of the custom metadata types provided as part of this application to set up the objects in their fields that needs to be masked
- **Manually start masking in Sandbox:** You can start the masking process in the sandbox environment by just click of a button
- **Mask while creating/refreshing of Sandbox:** You can also use our class named "MaskSensitiveData" while creating or refreshing sandbox to mask the records (the field history may not be deleted in that case, you might want to delete it manually in the sandbox)
- **Field History Deletion:** Our app will even delete the field history related information for the records, if field history tracking is enabled on any object
- **Do not work in Production, only in sandbox:** Our application will not run in the production environment so one cannot accidentally mask the production sensitive data. It'll only run in a sandbox environment.
- **Supports all Data Types:** Our application can support all data types and mask everything possible
- **Control the masking pattern:** You can control the masking character types for certain fields like Text, Text-Area, Text-Area (Long), Text-Area (Rich) and Text (Encrypted) to alphabets (lower or upper or both), alphanumeric (lower or upper or both) or with our without special character in between
- **Control the masking character length:** For certain fields you can also control the masking length of the masked data. You can set it up to original data length (except for Text-Area (Long) and Text-Area (Rich))
- **Abort the process:** You can abort the process in between by just click of a button on our app
- **Get Detailed Report:** You'll get the detailed report for the process and the errors during the process and also the fields that couldn't be masked and the id's of the records failed, so you can manually mask them later
- **Get Email Alerts:** Post process completion, users will get the result on your email
- **Separate app for masking any csv/excel file:** You can also ad-hoc mask any csv file by using 'Data Mask Generator' tab
- **Separate app for masking entered text:** You can also mask any random text by using 'Data Mask Generator' tab

At OQCT we are here to simplify users issue related to Salesforce, please email us the problems you have with data issue we love to build a solution for you in our app.

1.6. Requirement

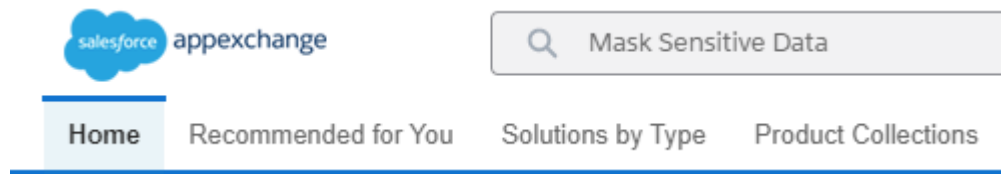
Salesforce Edition:

Professional
Enterprise
Unlimited
Developer

Support: Salesforce Classic & Salesforce Lightning

2. Install Instructions

1. Go to Salesforce App Exchange website "<https://appexchange.salesforce.com>"
2. Search for "**Mask Sensitive Data**"



3. Install the App on your Sandbox Environment or Production Environment
4. Select the Group you would like to install the App, and click "Install"



Install Mask Sensitive Data

By OQCT



☒ Install for Admins Only



☐ Install for All Users



☐ Install for Specific Profiles...



You're installing a Non-Salesforce Application that is not authorized for distribution as part of Salesforce's AppExchange Partner Program. 

☒ I acknowledge that I'm installing a Non-Salesforce Application that is not authorized for distribution as part of Salesforce's AppExchange Partner Program.

Install
 Cancel

App Name	Publisher	Version Name	Version Number
Mask Sensitive Data	OQCT	MaSeDa Spring 2020	2.4 Release Notes

Description

Mask sensitive data while creating/refreshing a Sandbox or you can mask data from within the Sandbox itself. The app is fully customizable to control the objects and fields that need to be masked. It provides detailed reports at the end of the masking.

Additional Details [View Components](#)

5. Please allow few minutes for the App to install it to your ORG



Install Mask Sensitive Data

By OQCT



Installing and granting access to admins Only...

App Name	Publisher	Version Name	Version Number
Mask Sensitive Data	OQCT	MaSeDa Spring 2020	2.4 Release Notes

Description

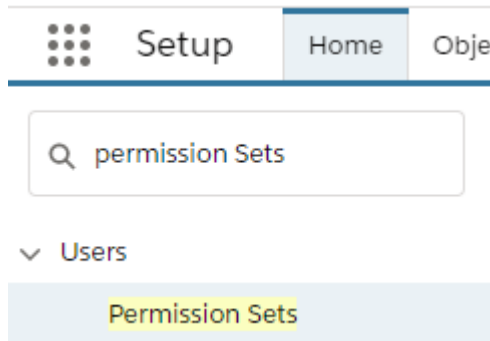
Mask sensitive data while creating/refreshing a Sandbox or you can mask data from within the Sandbox itself. The app is fully customizable to control the objects and fields that need to be masked. It provides detailed reports at the end of the masking.

Additional Details [View Components](#)

2.1. Step-1: Assign Permission Set

You need to assign a permission set to the users of the application (which usually would be admins of the org). Follow these steps:

- a) Under Setup, search for 'Permission Set'

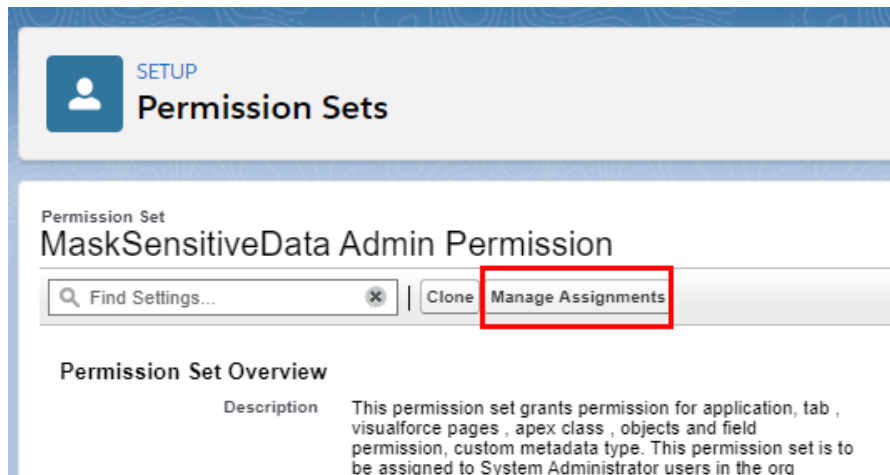


- b) Click the permission set named 'MaskSensitiveData Admin Permission'

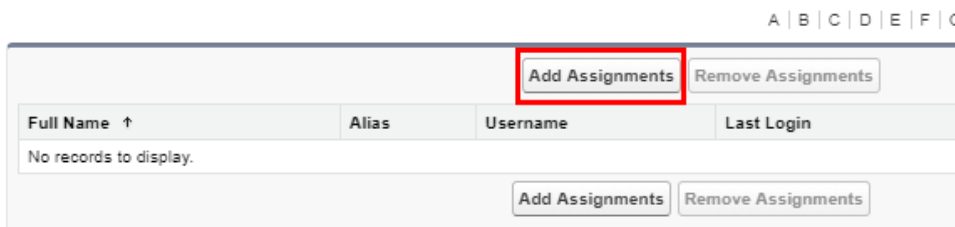
MaskSensitiveData Admin Permission

This permission set grants permission for application...

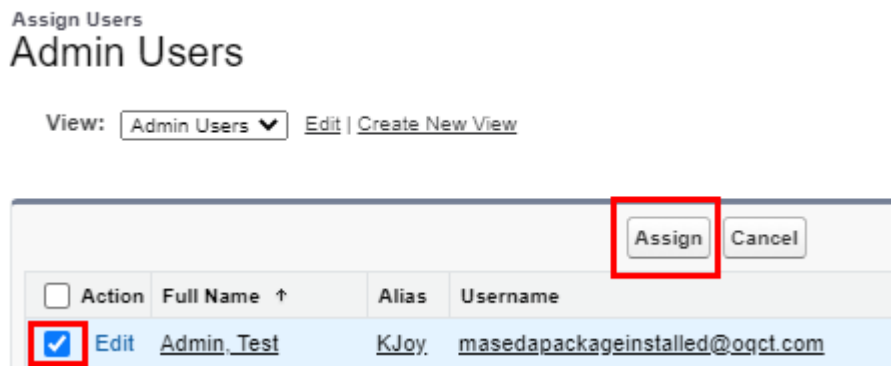
- c) Click on 'Manage Assignments'



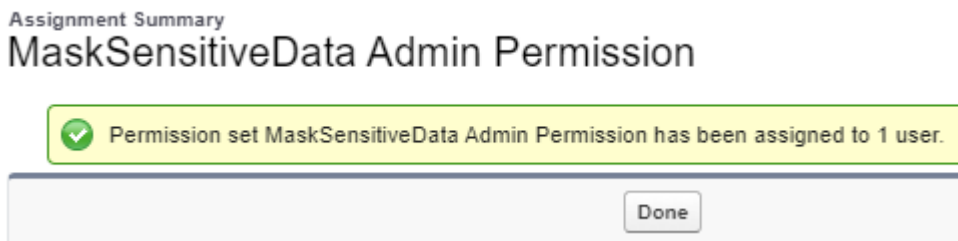
- d) Click on 'Add Assignment'



- e) Select the users you want to assign the permission for application 'Mask Sensitive Data' and click 'Assign'



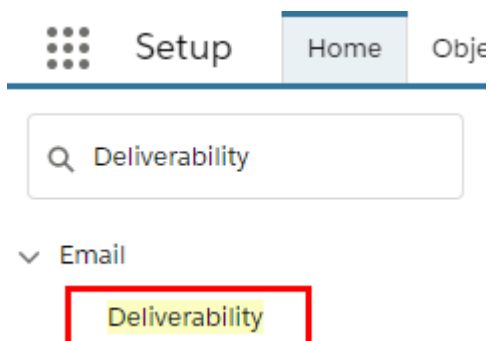
- f) Click on Done



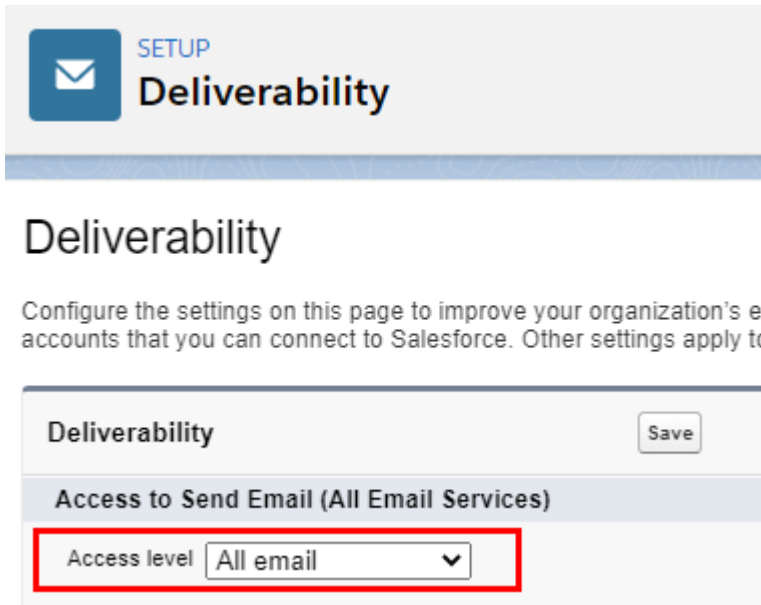
2.2. Step-2: Deliverability

The application will send emails after the Masking process and for this make sure that your org's Email Deliverability Access Level settings is set to 'All Emails'. Follow these steps:

- a) Under setup, search for 'Deliverability'



- b) Make sure the access level is set to 'All Emails'



SETUP
Deliverability

Deliverability

Configure the settings on this page to improve your organization's email accounts that you can connect to Salesforce. Other settings apply to

Deliverability

Save

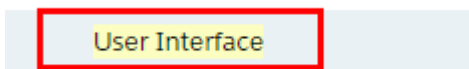
Access to Send Email (All Email Services)

Access level All email

2.3. Step-3: (Recommended in Sandbox)

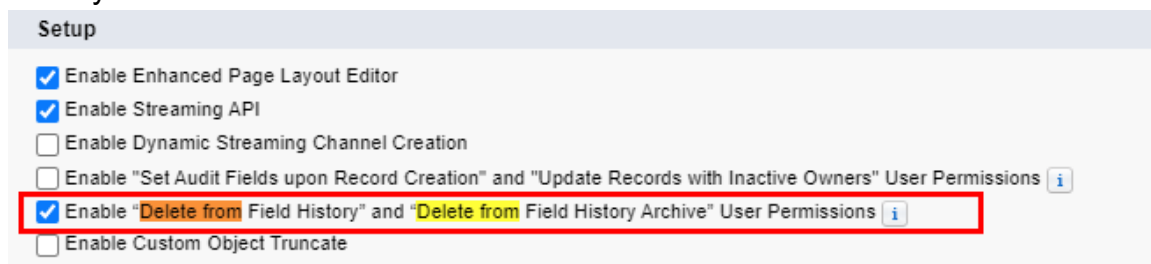
The application can also delete the field history tracking information for the masked records. For that, you need to do some configuration. **Also, in order to delete files uploaded by other users, admin needs 'Query All Files' permission Follow these steps:**

- a) From Setup Search for 'User Interface'



User Interface

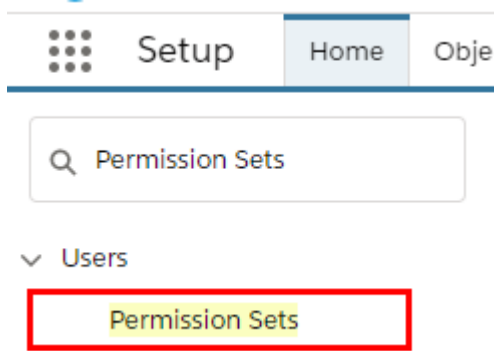
- b) Select the option named: Enable "Delete from Field History" and "Delete from Field History Archive" User Permission



Setup

- ☒ Enable Enhanced Page Layout Editor
- ☒ Enable Streaming API
- ☐ Enable Dynamic Streaming Channel Creation
- ☐ Enable "Set Audit Fields upon Record Creation" and "Update Records with Inactive Owners" User Permissions [i](#)
- ☒ Enable "Delete from Field History" and "Delete from Field History Archive" User Permissions [i](#)
- ☐ Enable Custom Object Truncate

c) Search for 'Permission Sets' in setup.



d) Create a new Permission set with following details (You can use any name for the permission set):

Label: **MaskSensitiveData FieldHistoryDelete and QueryAllFiles Permission**

Name: **MaskSensitiveData_FieldHistoryDelete_and_QueryAllFiles_Permission**

Description: **The permission set grants admin access to delete field history information if field history tracking is enabled on that object. This permission set also allows admin to view/delete files uploaded by other users**

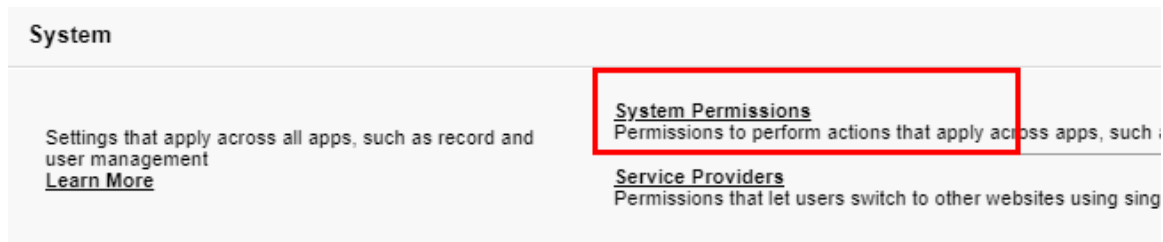
Session Activation Required: **False (Leave the checkbox unchecked)**

License: **None**

Permission Set
Create

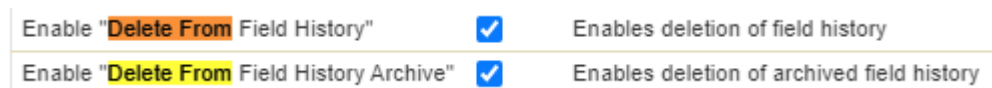
A screenshot of the 'Create Permission Set' form in Salesforce. The form is titled 'Enter permission set information' and contains several fields: 'Label' with the value 'MaskSensitiveData FieldHistoryDelete and QueryAllFiles Permission', 'API Name' with the value 'MaskSensitiveData_FieldHistoryDelete_and_QueryAllFiles_Permission', and 'Description' with the text 'The permission set grants admin access to delete field history information if field history tracking is enabled on that object. This permission set also allows admin to view/delete files uploaded by other users'. There is an unchecked checkbox for 'Session Activation Required'. Below this section is a section titled 'Select the type of users who will use this permission set' which includes instructions and a dropdown menu for 'License' set to '--None--'. At the bottom of the form, there are 'Save' and 'Cancel' buttons, with the 'Save' button highlighted by a red rectangular box.

- e) Go to 'System Permissions' on the 'New Permission Set' and Click 'Edit'



- f) Select the two options:

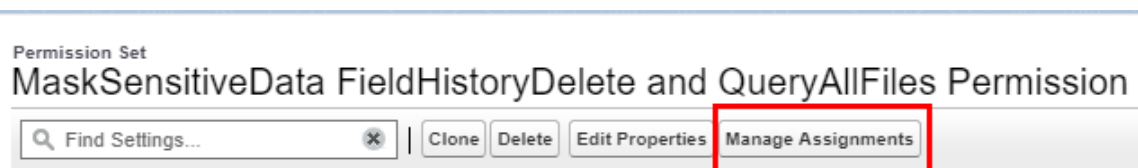
- Enable "Delete From Field History"
- Enable "Delete From Field History Archive"
- And click 'Save'



- g) For giving 'Query All' Permission, go to 'App Permissions' on the New Profile.
- h) Edit the permission and under 'Content' section, give permission on 'Query All Files' and save the changes

▼ Content		
Permission Name	Enabled	Description
Manage Content Permissions	☐	Create, edit, and delete library permissions in Salesforce CRM Content.
Manage Content Properties	☐ ⓘ	Create, edit, and delete custom fields in Salesforce CRM Content.
Manage record types and layouts for Files	☐ ⓘ	Create, edit, and delete content types in Salesforce CRM Content..
Manage Salesforce CRM Content	☐ ⓘ	Create, edit, and delete libraries and library memberships.
Query All Files	☒ ⓘ	Allows View All Data users to SOQL query all files in the org.
View Content in Portals	☐	View Salesforce CRM Content from a portal.

- i) Click on 'Manage Assignments' and assign the permission set to the admin users in the org



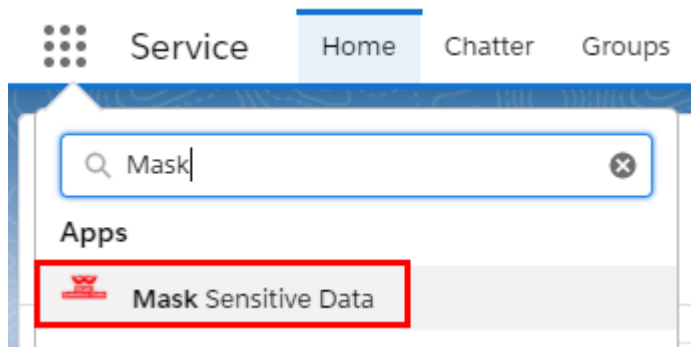
Note: If you want to create two separate permission sets for giving 'Field history delete' permission and 'Query All' Files permission, you can do so.

3. App Configuration

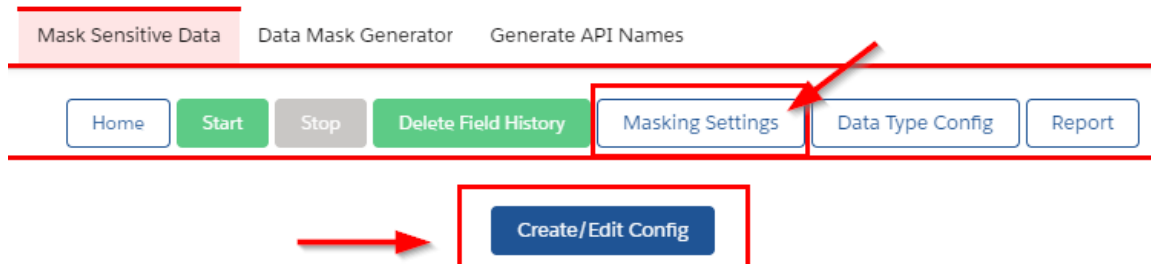
3.1. Step-4: Configure the Metadata

You can configure the Metadata types before starting the process to include/exclude any object and fields of those objects whose records need to be masked. Follow these steps:

- a) On Salesforce Apps Search for "Mask Sensitive Data" and Select it



- b) Click "Masking Settings" and Click "Create/Edit Config"



- c) Click 'New' to add records, "Mask Sensitive Data Object".

Mask Sensitive Data Objects

View: All Create New View

			New
Action	Label ↓	Mask Sensitive Data Object Name	
Edit Del	testobject_c	testobject_c	
Edit Del	test_obj_c	test_obj_c	
Edit Del	test_delete_record_c	test_delete_record_c	
Edit Del	NotFoundObject_C	NotFoundObject_C	
Edit Del	contentversion	contentversion	
Edit Del	attachment	attachment	

d) Enter the details as following:

Label: [API Name of the object that needs to be masked]

Mask Sensitive Data Object Name: [Leave default]

Mask Fields (API Name): [API Names of the fields that needs to be masked **comma-space-separated** (,[space])]

E.g.: MyField1__c, MyField2__c, MyField3__c

Fields not to copy (API Name): [API Names of the fields that must be set blank **comma-space-separated** (,[space])]

E.g.: MyField4__c, MyField5__c, MyField6__c

Enable Field Masking: ['Checked' if the object if you want to mask this object's records]

Delete All Records From Object: ['Checked' if the object if you want to delete this object's records]

Protected: [Leave Unchecked]

Mask Sensitive Data Object

Mask Sensitive Data Object Edit

Save Save & New Cancel

Mask Sensitive Data Object Config

Label Account

Mask Sensitive Data Object Name Account *i*

Mask Fields (API Name) *i* Name, Phone, Website

Fields not to copy (API Name) *i* Fax, AnnualRevenue, Description

Enable Field Masking *i* ☒

Delete All Records From Object *i* ☐

e) Click "Save" to save the metadata record

f) Now if you go back to the App and click on the "Mask Settings" you will be able to see: Which Object will be Masked, Fields that will be Masked, Fields that will be Blanked (No Data), if its "Enable" for Masking or to Delete All the records from the Objects!



All

Search...








Mask Sensitive Data
Mask Sensitive Data
Data Mask Generator
Generate API Names
Recently Viewed | Accou...
Recently Viewed

Home

Start

Stop

Delete Field History

Masking Settings

Data Type Config

Report

Create/Edit Config

Show 25 entries
Search:

Object API Name	Mask Fields (API Name)	Fields not to copy (API Name)	Enable Field Masking	Delete All Records From Object
Account	Name, Phone, Website	Fax, AnnualRevenue, Description	☒	☐
attachment			☐	☒
contentversion			☐	☒
NotFoundObject__C	asdjkhask__c		☐	☐
test_delete_record__c			☐	☐
test_obj__c	region__c, country__c, item_type__c, sales_channel__c, order_priority__c, order_id__c, units_sold__c, unit_price__c, unit_cost__c, total_revenue__c, total_cost__c, NotFoundMask__c	total_profit__c, NotFoundDelete__c	☐	☐
testobject__c	emp_id__c, first_name__c, last_name__c, e_mail__c, father_s_name__c, mother_s_name__c, mother_s_maiden_name__c, age_in_yrs__c, year_of_joining__c, currency__c, telephone_number__c, checkbox__c, date__c, geolocation__latitude__s, geolocation__longitude__s, geolocation__c, percent__c, text_encrypted__c, text_area_rich__c, text_area_long__c, text_area__c, url__c, FieldnotMaskFieldNotFound__c	first_name__c, FieldnottocopyNotFound__c	☐	☐

Showing 1 to 7 of 7 entries

Previous
1
Next

3.2. Step-5: Email and URL Format

You can choose the way the Email and URL fields will be masked by providing the domain name that you wish to put which will be used with masked data for these types of fields. Follow these steps:

- On the "Mask Sensitive Data" App Click on "Data Type Config"

Data Type Config

- Click "Edit" Icon on the "Email"

 EMAIL	80	asjk41@oqct.com	[Random Alphanumeric String]@[Your Email Domain]
---	----	-----------------	--

- Click "Edit" beside "Your Email Domain" and change the "Domain Name" to the one you like and Save

Mask Sensitive Data Type - Domain (Managed)

 This Mask Sensitive Data Type - Domain is managed, meaning that you may only edit certain attributes. [Display More Information](#)

Mask Sensitive Data Type - Domain Edit Save Save & New Cancel

Data Type Config

Domain Name 

Not Required

Label	Your Email Domain	Namespace Prefix	OQCT_MaSeDa
Mask Sensitive Data Type - Domain Name	Your_Email_Domain 		

d) Now when Masking the Email Field, the Masked Data will be looked like this:
"[asjk41@oqct.com](#)" ([Random Alphanumeric String]@[Your Email Domain])

e) In order to change the "URL" format, go back to the App and Click on the URL Edit Icon

 URL	255	www.sjh45.oqct.com	www.[Random Alphanumeric String].[Your URL Domain]
---	-----	------------------------------------	--

f) Click "Edit" beside "Your URL Domain" and change the "Domain Name" to the one you like and Save

Mask Sensitive Data Type - Domain (Managed)

 This Mask Sensitive Data Type - Domain is managed, meaning that you may only edit certain attributes. [Display More Information](#)

Mask Sensitive Data Type - Domain Edit Save Save & New Cancel

Data Type Config

Domain Name 

Not Required

Label	Your URL Domain	Namespace Prefix	OQCT_MaSeDa
Mask Sensitive Data Type - Domain Name	Your_URL_Domain 		

Save Save & New Cancel

3.3. Step-6: Phone Data Type Format

You can choose the way the Phone data type field will be masked, i.e. the length of the data to produce when masking record. Follow these steps:

- a) On the "Mask Sensitive Data" App Click on "Data Type Config"

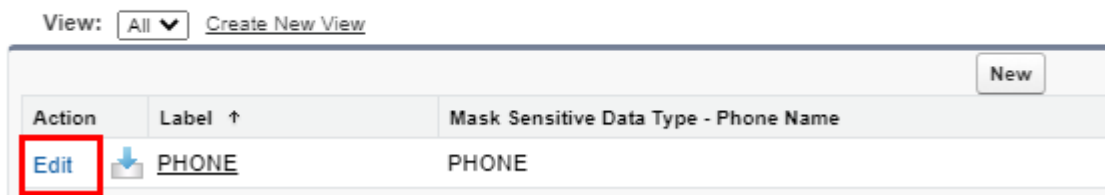


- b) Click "Edit" Icon on the "Phone"

 PHONE	40	02081333880	Match Records Data Length - [Random Number]
---	----	-------------	---

- c) Again Click "Edit" on the Data Type

Mask Sensitive Data Type - Phones

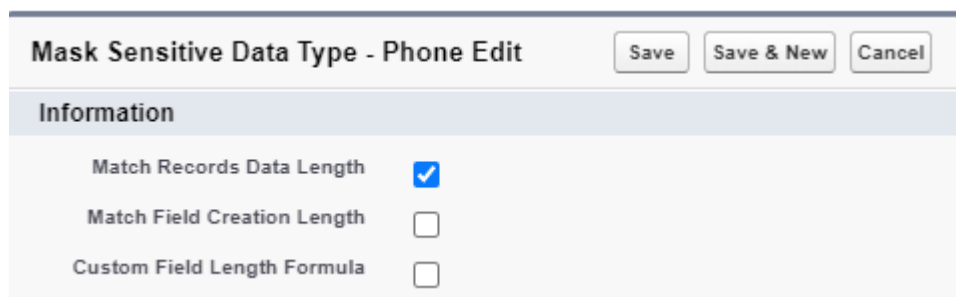


- d) Choose between the three checkboxes:

Match Records Data Length: [Select this if you want the length of the data generated should match the original data in that field]

Match Field Creation Length: [Select this if you want the length of the data generated should match the length entered when the field was created, i.e. the maximum length of that field]

Custom Field Length Formula: [Select this if you want the length of the data generated should depend on your formula (See point (e))]

A form titled "Mask Sensitive Data Type - Phone Edit" with "Save", "Save & New", and "Cancel" buttons. Under the "Information" section, there are three checkboxes: "Match Records Data Length" (checked), "Match Field Creation Length" (unchecked), and "Custom Field Length Formula" (unchecked).

- e) For "Custom Field Length Formula", you can write your formula, On the left side you have the field length in your org, i.e. the length you entered at the time of field creation

or the maximum character allowed in that field and on right side you'll have to enter the masked data length. You can include up to 10 such pairs

E.g.: If your ORG's Phone field Length is 12, Mask Sensitive Data Generate 10

Phone Formula Config

If your ORG's Phone field Length is	12	Mask Sensitive Data Generate	10
If your ORG's Phone field Length is	10	Mask Sensitive Data Generate	10
If your ORG's Phone field Length is	9	Mask Sensitive Data Generate	9
If your ORG's Phone field Length is	40	Mask Sensitive Data Generate	10
If your ORG's Phone field Length is		Mask Sensitive Data Generate	
If your ORG's Phone field Length is		Mask Sensitive Data Generate	

3.4. Step-7: TEXT Data Type Format

You can choose the way the Text, Text-Area, Text-Area (Long), Text-Area (Rich), Text (Encrypted) data type field will be masked, i.e. the length of the data to produce when masking record. Follow these steps:

- a) On the "Mask Sensitive Data" App Click on "Data Type Config"



- b) Click "Edit" Icon on the "Text"

 TEXT	255	HJVFRAGFR	Match Records Data Length - [Alphabets(Upper Case Only)]
--	-----	-----------	--

- c) Click "Edit" beside "TEXT"

Mask Sensitive Data Type - Text

View: All [Create New View](#)

Action	Label ↑	Mask Sensitive Data Type - Text Name
Edit	 TEXT	TEXT
Edit	 TEXT(Encrypted)	TEXT_Encrypted
Edit	 TEXTAREA	TEXTAREA
Edit	 TEXTAREA(Long)	TEXTAREA_Long
Edit	 TEXTAREA(Rich)	TEXTAREA_Rich

- d) Choose between the three check boxes:

Match Records Data Length: [Select this if you want the length of the data generated should match the original data in that field]

Match Field Creation Length: [Select this if you want the length of the data generated should match the length entered when the field was created, i.e. the maximum length of that field]

Custom Field Length Formula: [Select this if you want the length of the data generated should depend on your formula (See point (e))]

Mask Sensitive Data Type - Text (Managed)

 This Mask Sensitive Data Type - Text is managed, meaning that you may only edit certain attributes. [Display](#)

Mask Sensitive Data Type - Text Edit

Save Save & New Cancel

Information

Match Records Data Length

☒

Match Field Creation Length

☐

Custom Field Length Formula

☐

Type

Alphabets(Upper Case Only)

▼

- e) For "Custom Field Length Formula", you can write your formula, On the left side you have the field length in your org, i.e. the length you entered at the time of field creation or the maximum character allowed in that field and on right side you'll have to enter the masked data length. You can include up to 20 such pairs

E.g.: If your ORG's Text field Length is 255, Mask Sensitive Data Generate 50

Text Formula Config

If your ORG's Text field Length is	255	Mask Sensitive Data Generate	50
If your ORG's Text field Length is	200	Mask Sensitive Data Generate	50
If your ORG's Text field Length is	150	Mask Sensitive Data Generate	50
If your ORG's Text field Length is	100	Mask Sensitive Data Generate	50
If your ORG's Text field Length is	50	Mask Sensitive Data Generate	50
If your ORG's Text field Length is	20	Mask Sensitive Data Generate	20
If your ORG's Text field Length is		Mask Sensitive Data Generate	
If your ORG's Text field Length is		Mask Sensitive Data Generate	

- f) You can also select the type of pattern for the generated data for these type of fields, i.e. Alphabets(Lower Case Only), Alphabets(Upper Case Only), Alphabets(Upper Case And Lower Case Mix), AlphaNumeric(Lower Case Only), AlphaNumeric(Upper Case Only), AlphaNumeric(Lower Case-Upper Case-Special Characters)

Type

- g) Repeat the same for Text-Area, Text-Area (Long), Text-Area (Rich), Text (Encrypted)

Mask Sensitive Data Type - Text

View: [Create New View](#)

Action	Label ↑	Mask Sensitive Data Type - Text Name
Edit	TEXT	TEXT
Edit	TEXT(Encrypted)	TEXT_Encrypted
Edit	TEXTAREA	TEXTAREA
Edit	TEXTAREA(Long)	TEXTAREA_Long
Edit	TEXTAREA(Rich)	TEXTAREA_Rich

[New](#)

3.5. Step-8: Number, Currency, Percent Data Type Format

You can choose the way the Number, Currency, Percent data type field will be masked, i.e. the length of the data to produce when masking record. Follow these steps:

- a) On the "Mask Sensitive Data" App Click on "Data Type Config"

[Data Type Config](#)

- b) Click "Edit" Icon on the "Number"



- c) Click "Edit" beside "NUMBER"

Mask Sensitive Data Type – Numbers

View: All [Create New View](#)

Action	Label ↑	Mask Sensitive Data Type – Number Name
Edit	Number	Number

- d) Choose between the three checkboxes:

Mask Sensitive Data Type – Number Edit Save Save & New Cancel

Information

Match Records Data Length ☒

Match Field Creation Length ☐

Custom Field Length Formula ☐

Match Records Data Length: [Select this if you want the length of the data generated should match the original data in that field]

Match Field Creation Length: [Select this if you want the length of the data generated should match the length entered when the field was created, i.e. the maximum length of that field]

Custom Field Length Formula: [Select this if you want the length of the data generated should depend on your formula (See point (e))]

- e) For "Custom Field Length Formula", you can write your formula, On the left side you have the field length in your org, i.e. the length you entered at the time of field creation or the maximum character allowed in that field and on right side you'll have to enter the masked data length. You can include up to 10 such pairs

E.g.: If your ORG's Number field Length is 16, Mask Sensitive Data Generate 10

If your ORG's Number field Length is	10	Mask Sensitive Data Generate	5
If your ORG's Number field Length is	15	Mask Sensitive Data Generate	10
If your ORG's Number field Length is	18	Mask Sensitive Data Generate	15
If your ORG's Number field Length is		Mask Sensitive Data Generate	
If your ORG's Number field Length is		Mask Sensitive Data Generate	
If your ORG's Number field Length is		Mask Sensitive Data Generate	

- f) To Configure Currency, Percent do the same!

If you have any issue please contact our email: support@oqct.com

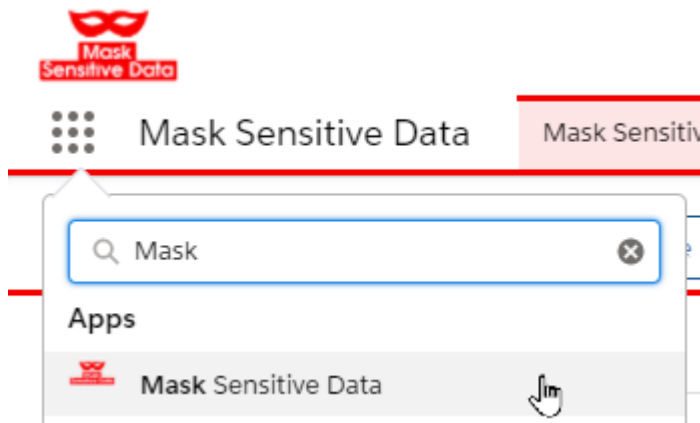
4. How to ?

4.1. How to Mask Manually?

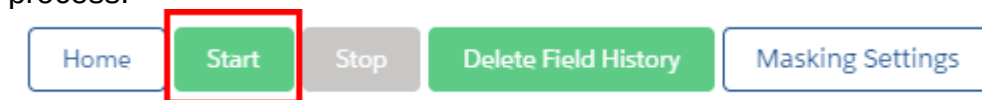
Info:

Our App will only Mask Data from Sandbox, before starting the process please make sure you have configured the "Mask Sensitive Data" App.

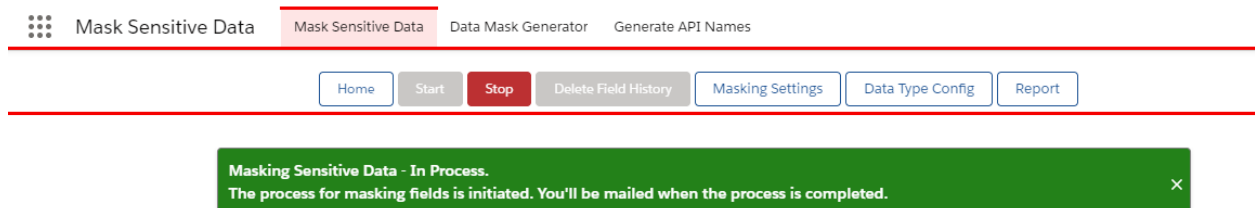
a) Salesforce App Menu > Search / Click "Mask Sensitive Data"



b) Once you have configured the app, just click "Start", this will start the Data Masking process.



c) Once completed you will receive an email.



d) You will be able to track the status of Masking Process if you click "Report"

The screenshot shows the 'Mask Sensitive Data' application interface. At the top, there's a navigation bar with tabs: 'Mask Sensitive Data', 'Data Mask Generator', and 'Generate API Names'. Below this is a sub-navigation bar with buttons: 'Home', 'Start', 'Stop', 'Delete Field History', 'Masking Settings', 'Data Type Config', and 'Report'. The 'Report' button is highlighted with a red box. Below the navigation bar, the title 'Mask Sensitive Data Report' is displayed. A 'Delete' button is visible above the table. The table has columns: 'Job ID', 'Status', 'Job Start', 'Job End', 'Job Start By', 'Job Type', 'Objects Not Found', 'Total Success Records', and 'Total Fail Records'. Two rows of data are shown, both with a status of 'Completed'.

Job ID	Status	Job Start	Job End	Job Start By	Job Type	Objects Not Found	Total Success Records	Total Fail Records
ID-004	Completed	2/20/2020, 11:46 AM	2/20/2020, 11:46 AM	Krrish Joy	Masking Sensitive Data		7	1
ID-003	Completed	2/20/2020, 11:38 AM	2/20/2020, 11:38 AM	Krrish Joy	Masking Sensitive Data		3	1

4.2. How to Mask Data Automatically (While Sandbox refresh)

If you want to mask your Production data while creating the Sandbox for (Full Copy and Partial Copy Sandbox) then You need to create a New Sandbox and on the Sandbox creation: Apex Class use "MaskSensitiveData". Please be aware this is not recommended due to If you have any Trigger, Process Builder, Remote Site, Flow, Workflow run while Record Edit (Configured Objects) the action will be taken (from: Trigger, Process Builder, Remote Site, Flow, Workflow), We advice our customers to Run manually after deactivating the config they don't want to run it while Masking!

a) Configure the "Mask Sensitive Data" App (all the objects and fields that need to be Masked)

b) From Setup Search for 'Sandbox'

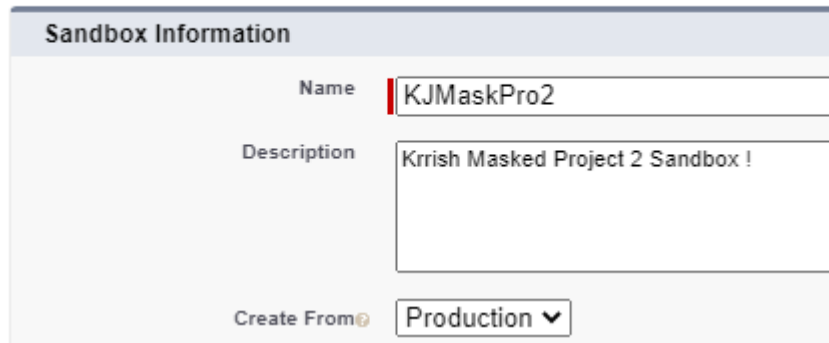
The screenshot shows the Salesforce Setup page. The 'Setup' tab is selected. A search bar contains the text 'Sandbox'. Below the search bar, the 'Sandboxes' option is highlighted under the 'Environments' section.

c) Click "New Sandbox"

The screenshot shows a button labeled 'New Sandbox'.

d) Fill the "Name" and "Description" of the Sandbox and Select the Sandbox you want to create and Click "Next" and the Objects you want to copy (If its Full copy Sandbox or Partial copy Sandbox)

Create Sandbox



Sandbox Information

Name: KJMaskPro2

Description: Krrish Masked Project 2 Sandbox !

Create From: Production

- e) Here you need to enter as it is / Copy& Paste, on the "Apex Class" as **"MaskSensitiveData"** and Click "Create" in order to Create the Sandbox!

Create Sandbox



Sandbox Options

Apex Class: MaskSensitiveData

Back Create Cancel

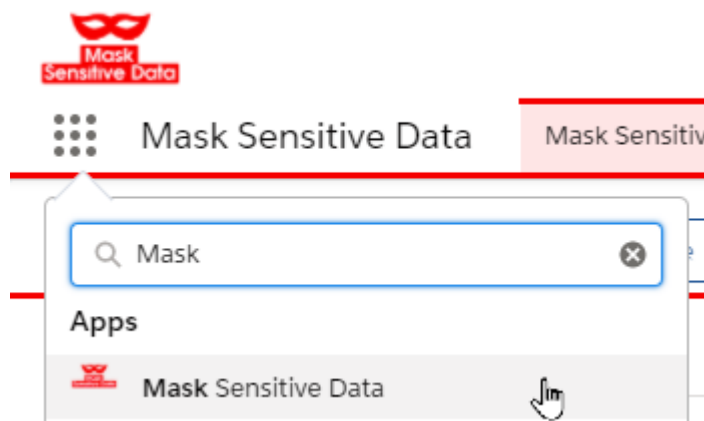
- f) Up on creating the Sandbox, Salesforce will copy your production data to new sandbox and then it will run our program to Mask the Data Automatically!

4.3. How to Delete Field History ?

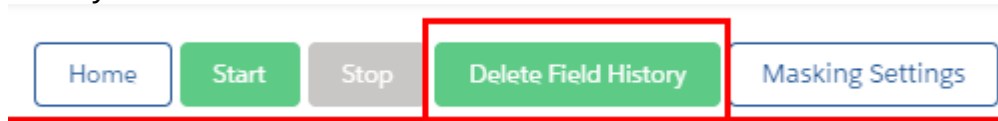
Info:

Our App will only Delete Field History from Sandbox, before starting the process please make sure you have configured the "Mask Sensitive Data" App.

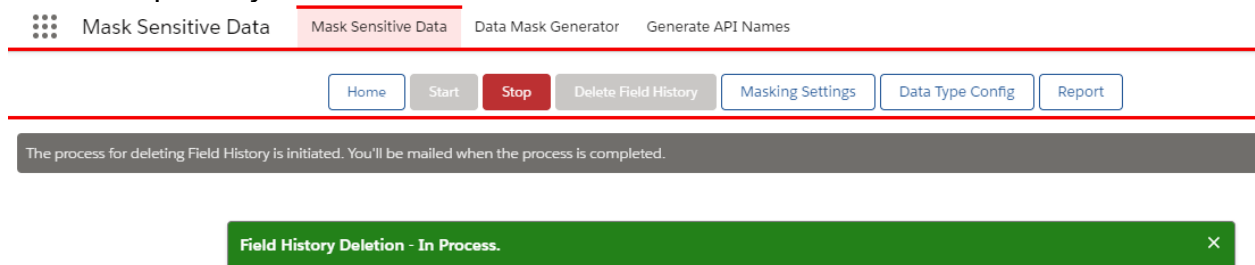
- a) Salesforce App Menu > Search / Click "Mask Sensitive Data"



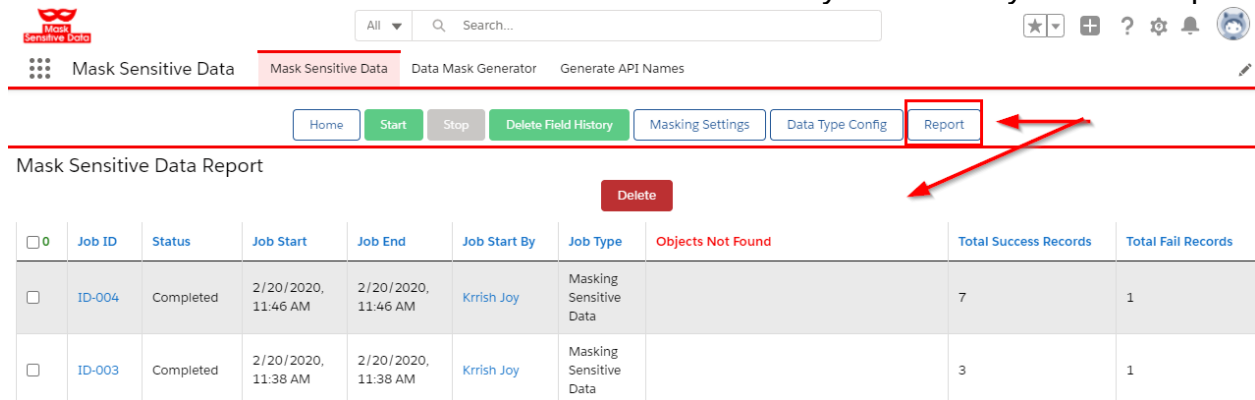
b) Once you have configured the app, click "Delete Field History", this will start Delete Field History.



c) Once completed you will receive an email.



d) You will be able to track the status of "Delete Field History Process" if you click "Report"



4.4. Data Mask Generator - Manual

If you want to Mask Data Manually by copy and pasting the data, use this function! This function will come handy when a developer or project team request for few Data, you can just simply copy the production data and past it here and Mask the data and pass it to the developer! Which makes it easier when its comes to Data Type, Data Size, Data Format etc..

Manual Data Mask Generator

Enter Data To Mask

Enter your items in the field below, each on a separate line or comma (,) seperated. Items can be numbers, names, email addresses, etc. A maximum of 10,000 characters are allowed.

Hermila Suhr,Todd Suhr,Cathrine Suhr
Antonio,Joy,Clark Joy,Clarisa Joy
Sebastian,Moores,Everette Moores,Sol Moores
Alec,Rittenhouse,Jefferey Rittenhouse,Moir Rittenhouse
Reggie,Doughty,Jerrold Doughty,Crista Doughty

Select Seperator

Comma

Select Category

Text

Select Type

Alphabets (Lower Case only)

Select Masked Data Length

5

Generate

Clear

Select Category: Here you will be able to choose the Data Type you want generate.

Select Type: Here the format

Select Masked Data Length: Here the length of the output.

When generating this example Data you will get the bellow Data!

Masked Data

twqxe,tpmua,xysqb
dmizh,polvf,fvzyr,tockv
fazfw,mascf,nqxfu,pdxhb
mtczt,petyh,fckcl,dovdh
bjenf,lyzbq,bfohq

4.5. Data Mask Generator - CSV

If you want to Mask Data Manually using your Excel file or CSV Data file, use this function! This function will come handy when a developer or project team request for sample Data, you can just simply upload your Data file and Mask the data file and send it to Project team.

- a) Click "Upload File" and upload your Data File

Attachment

Upload File

or Drop File

TestOBJ.csv

Select Masked File Format

excel(xls)

Generate File

CSV XLS

- b) and click "Generate File"
- c) Select the "Data Type" for each column, Masking pattern and the Length and click "Download Masked Data".

Manual Data Mask Generator

CSV Header	Data Type	Masking Pattern	Length	Enable Mask
Emp ID	Number	Without Decimal	Original Data Length	☒
First Name	Text	Alphabets (Lower Case only)	Original Data Length	☒
Last Name	Text	Alphabets (Lower Case only)	Original Data Length	☒
E Mail	Text	Alphabets (Lower Case only)	Original Data Length	☒

- d) Now you Data file will be Masked and you can forward this to your project team.

4.6. Generate API Names

We created an API Names generator for your ORG, so anyone can configure the "Mask Sensitive Data" app and mask the Data without Salesforce Technical Skills.

Simply select the Objects and the Fields you want to mask and the Generator will give you the API names, and you just need to copy and past it on the Config.



Generate API Name

Select object and fields that you would like to copy and paste in the metadata configuration

Select Object

Account

Load All Objects

Copy your Object Label

account

API Name, you need it for the Config

Fields API Names for Masking

Fields API Names for Not to copy

Available Fields

Account ID
Deleted
Master Record ID
Account Type
Parent Account ID
Billing Latitude
Billing Longitude
Billing Geocode Accuracy
Billing Address
Shipping Street
Shipping City
Shipping State/Province
Shipping Zip/Postal Code

Selected Fields

Account Name
Billing Street
Billing City
Billing State/Province
Billing Zip/Postal Code
Billing Country

Generate API Name for Mask Sensitive Data Object

Create/Edit Config

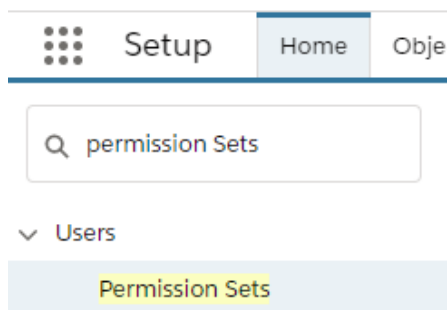
API Names, you need it for the Config

name, billingstreet, billingcity, billingstate, billingpostalcode, billingcountry

4.7. Assign App to New Admin

You need to assign a permission set to the users of the application (which usually would be admins of the org). Follow these steps:

- Under Setup, search for 'Permission Set'



- Click the permission set named 'MaskSensitiveData Admin Permission'

MaskSensitiveData Admin Permission

This permission set grants permission for application...

- c) Click on 'Manage Assignments'

SETUP
Permission Sets

Permission Set
MaskSensitiveData Admin Permission

Find Settings... | Clone | **Manage Assignments**

Permission Set Overview

Description This permission set grants permission for application, tab , visualforce pages , apex class , objects and field permission, custom metadata type. This permission set is to be assigned to System Administrator users in the org

- d) Click on 'Add Assignment'

Assigned Users
MaskSensitiveData Admin Permission
« Back to: Permission Set

A | B | C | D | E | F | G

Add Assignments Remove Assignments

Full Name ↑	Alias	Username	Last Login
No records to display.			

Add Assignments Remove Assignments

- e) Select the users you want to assign the permission for application 'Mask Sensitive Data' and click 'Assign'

Assign Users
Admin Users

View: Admin Users ▼ Edit | Create New View

☐ Action	Full Name ↑	Alias	Username
☒ Edit	Admin_Test	KJoy	masedapackageinstalled@oqct.com

Assign Cancel

- f) Click on Done

Assignment Summary
MaskSensitiveData Admin Permission

✓ Permission set MaskSensitiveData Admin Permission has been assigned to 1 user.

Done

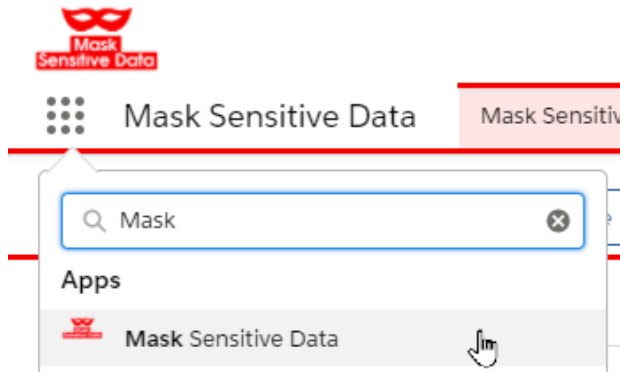
- g) Open "MaskSensitiveData FieldHistoryDelete and QueryAllFiles Permission" and Assign this permission to New Admin also.

☐	Clone	MaskSensitiveData Admin Permission	This permission set grants permission for application...
☐	Del Clone	MaskSensitiveData FieldHistoryDelete and QueryAll...	The permission set grants admin access to delete file ...

- h) Once you assign both permission set the New admin will have the access to "Mask Sensitive Data" App.

4.8. How to find Failed Masking Data

a) Salesforce App Menu > Search / Click "Mask Sensitive Data"



b) Click "Report" on the App Menu



c) Here you will find the basic Information about the Failed and Success Masking and the Objects Not Found

A screenshot of the Mask Sensitive Data Report interface. At the top, there is a navigation bar with the following tabs: 'Mask Sensitive Data', 'Mask Sensitive Data', 'Data Mask Generator', and 'Generate API Names'. Below the navigation bar, there is a row of buttons: 'Home', 'Start', 'Stop', 'Delete Field History', 'Masking Settings', 'Data Type Config', and 'Report'. The 'Report' button is highlighted with a red box. Below the buttons, the title 'Mask Sensitive Data Report' is displayed. To the right of the title, there is a red 'Delete' button. The main content area is a table with the following columns: 'Job ID', 'Status', 'Job Start', 'Job End', 'Job Start By', 'Job Type', 'Objects Not Found', 'Total Success Records', and 'Total Fail Records'. The table contains 8 rows of data. The 'Objects Not Found' column is highlighted with a red box. The 'Total Success Records' and 'Total Fail Records' columns are also highlighted with red boxes. The table data is as follows:

Job ID	Status	Job Start	Job End	Job Start By	Job Type	Objects Not Found	Total Success Records	Total Fail Records
ID-007	Completed	8/19/2020, 10:24 PM	8/19/2020, 10:25 PM	Krrish Joy	Field History Deletion		0	0
ID-006	Completed	8/19/2020, 8:20 PM	8/19/2020, 8:21 PM	Krrish Joy	Field History Deletion		0	0
ID-005	Completed	8/19/2020, 8:18 PM	8/19/2020, 8:19 PM	Krrish Joy	Masking Sensitive Data		996	1
ID-004	Completed	2/20/2020, 11:46 AM	2/20/2020, 11:46 AM	Krrish Joy	Masking Sensitive Data		7	1
ID-003	Completed	2/20/2020, 11:38 AM	2/20/2020, 11:38 AM	Krrish Joy	Masking Sensitive Data		3	1
ID-002	Completed	2/19/2020, 6:33 AM	2/20/2020, 12:10 AM	Krrish Joy	Masking Sensitive Data	NotFoundObject__C	1,648,049	53
ID-001	Completed	2/18/2020, 2:20 PM	2/19/2020, 6:22 AM	Krrish Joy	Masking Sensitive Data	NotFoundObject__C	1,351,168	14
ID-000	Completed	2/17/2020, 8:59 PM	2/18/2020, 7:53 AM	Krrish Joy	Masking Sensitive Data	NotFoundObject__C	1,168,652	10

Page 1 of 1

Previous 25 Next

1 - 8 of 8

d) If you click on the 'Job ID' this will drill down the report more in detail.

☐	ID-002	Completed	2/19/2020, 6:33 AM	2/20/2020, 12:10 AM
--------------------------	---------------	-----------	-----------------------	------------------------

e) Here on the Job ID detail you can see "Masking process and the Deletion Process", Field History Deletion Status, Fields Not Found.

Home Start Stop Delete Field History Masking Settings Data Type Config Report						
Mask Sensitive Data Report						
Back Delete						
☐	Object API Name	Masking/Deletion Status	Field History Deletion	Records Succeeded	Records Failed	Fields Not Found
☐	testobject__c	Masking - Completed	Completed	601,747	53	fieldnotmaskfieldnotfound__c, fieldnottocopynotfound__c
☐	test_delete_record__c	Deletion - Completed	Completed	2	0	
☐	test_obj__c	Masking - Completed	Completed	1,046,300	0	notfoundmask__c, notfounddelete__c

Page 1 of 1 << Previous 25 Next >> 1 - 3 of 3

f) When there is a Records Failed to Mask you will be able to click on that Object API Names to find out in more detail. Click on the "testobject__c" hyper link

Object API Name
testobject__c

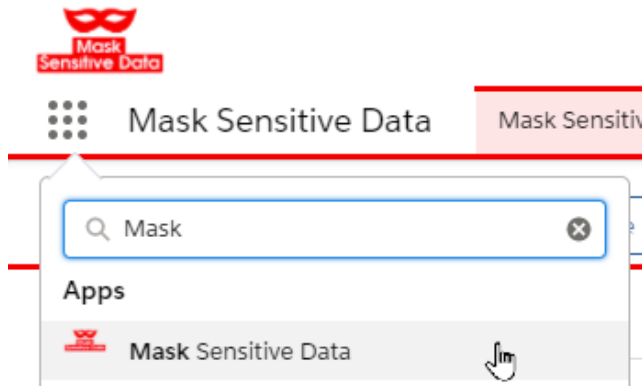
g) Detailed Masking Failed

Home Start Stop Delete Field History Masking Settings Data Type Config Report						
Mask Sensitive Data Fail Records						
Filter Result Back Delete Export All Records Download all in CSV file						
Error Status: --None-- Search Clear						
☐	Object API Name	Masking Error Fields	Masking Validation Error Fields	Salesforce Record Id	Error Status	Error Reason
☐	testobject__c	Year_of_Joining__c		a0363000004hWcoAAE	Partially Failed	
☐	testobject__c	Year_of_Joining__c		a0363000004hY12AAE	Partially Failed	
☐	testobject__c	Year_of_Joining__c		a0363000004igRtAAI	Partially Failed	
☐	testobject__c	Year_of_Joining__c		a0363000004iifPAAQ	Partially Failed	
☐	testobject__c	Year_of_Joining__c			Partially Failed	
☐	testobject__c	Year_of_Joining__c			Partially Failed	
☐	testobject__c	Year_of_Joining__c		a0363000004hvKBAAY	Partially Failed	

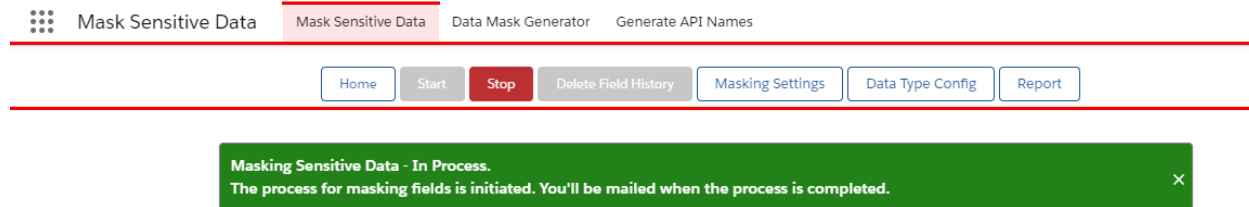
4.9. How to Stop Masking

IMPORTANT STOP DOES NOT UNDO ANY MASKING THAT HAS ALREADY COMPLETED!

a) Salesforce App Menu > Search / Click "Mask Sensitive Data"



b) click "Stop", this will Stop the Data Masking process.

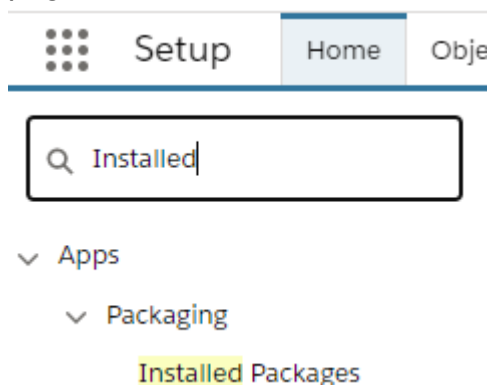


5. App Uninstall

At OQCT we are here to support our customers and partner with Salesforce and our app related issues, or any feature missing from our app.

If you like to Uninstall the "Mask Sensitive Data" app for any reason, please follow this setup:

1. GO to "Setup" and Search for "Installed Packages" and Open the "Installed Packages" page.



2. Find the "Mask Sensitive Data" and Click on "Uninstall" link.

Installed Packages

On AppExchange you can browse, test drive, download, and install pre-built apps and components. [Installing Packages](#).

Apps and components are installed in packages. Any custom apps, tabs, and custom objects are your users. This allows you to test and customize before deploying. You can deploy the component by clicking Deploy.

Depending on the links next to an installed package, you can take different actions from this page.

To remove a package, click Uninstall. To manage your package licenses, click **Manage License**.

Installed Packages			
Action	Package Name	Publisher	Version Number
Uninstall	Salesforce.com CRM Dashboards Description Salesforce.com CRM Dashboards	salesforce.com	1.0
Uninstall	Knowledge Base Dashboards & Reports Description This package provides reports and dashboards that help you monitor	Salesforce Knowledge	1.23
Uninstall Configure	MaskSensitiveData Description This application is for masking data, i.e., the records of the object (t	OQCT Ltd	2.4

3. Review all the changes that will take place in your ORG and click on "Uninstall"

Custom Object Data

Custom Object
Mask Sensitive Data Type - Text
Mask Sensitive Data Type - Number
Mask Sensitive Data Report
Mask Sensitive Data Result Details
Mask Sensitive Data Type - Domain
Mask Sensitive Data Object
Mask Sensitive Data Fail Record
Mask Sensitive Data Type - Phone

☐ Save a copy of this package's data for 48 hours after uninstall

☒ Do not save a copy of this package's data after uninstall

☒ Yes, I want to uninstall this package and permanently delete all associated components

[Uninstall](#)

6. Contact us



Company: OQCT Limited

Tel: +44 208 133 3880

Website: www.oqct.com

Email: support@oqct.com

A

About Application · 6
App Config - Assign Permission Set · 14
App Config - Deliverability · 16
App Configuration · 20
App Uninstall · 45
App Warning · 7
Assign App to New Admin · 39

B

Button Actions · 9

C

Configure the Metadata · 20
Contact us · 47

D

Data Mask Generator · 35
Data Mask Generator CSV · 37
Delete Field History · 34

E

Email and URL Format · 23

F

Failed Masking Data · 42
Features · 10

G

General App Information · 8
Generate API Names · 38

H

How to ? · 31
How to Mask Data Automatically (While
Sandbox refresh) · 32
How to Mask Manually · 31

I

Install Instructions · 12

N

Number, Currency, Percent Data Type
Format · 29

P

Phone Data Type Format · 25

R

Requirement · 12

S

Stop Masking · 44

T

TEXT Data Type Format · 26