



MICROSOFT LABS

APRIL 13, 2018

DYNAMICS 365 DATA TAGGING & OBFUSCATION

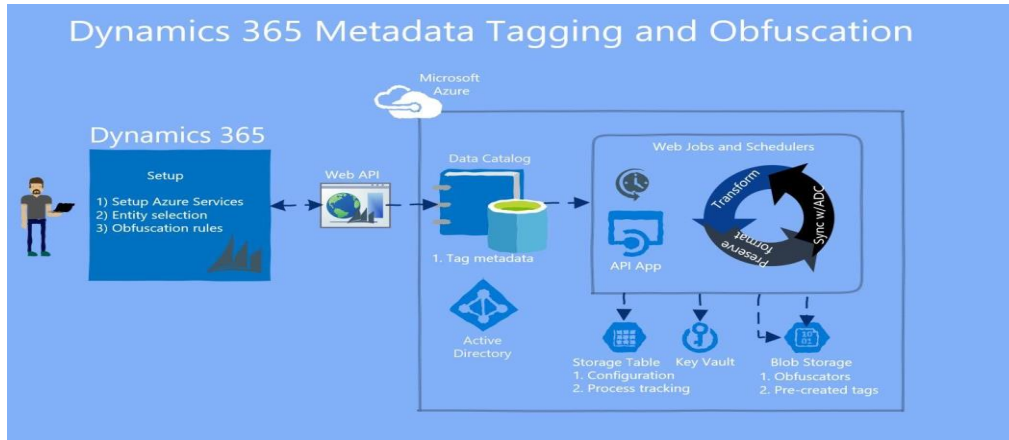
A tool to add entity into CRM, obfuscate the entity and sync Glossary with Azure table storage and give them a weightage.

Contents

Introduction	2
Verify Solution Installation	2
Obfuscation Setup	3
Dynamics 365 Azure setup	3
Template Deployment	7
Generate SAS Token	11
Adding Secrets values to Key Vault	12
Obfuscation Configuration in CRM	16
Add Application User in CRM Org	16
Obfuscation Agents to CRM Org	18
Add New Obfuscation Agent	20
Upload New Agents to Azure Blob	23
CRM Initial Sync and Data Sync	24
Adding Entity for Obfuscation	29
Glossary Term Execution Order	32
Adding a new Glossary – Obfuscation Agent	33
Edit a Glossary term – Obfuscation Agent combination	35
Least Permissions required to access Obfuscation area	36
End User Experience	36

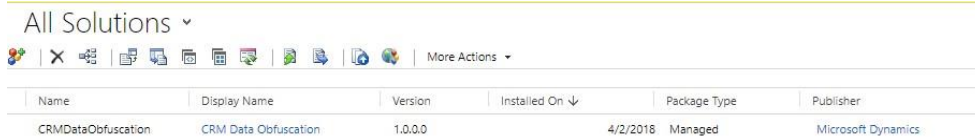
Introduction

Microsoft Dynamics 365 provides several tools for managing data. This tool is for data obfuscation, it look for all available entities in CRM and Obfuscate entity fields based on tagging at Azure Data Catalog and weightage configured in CRM...

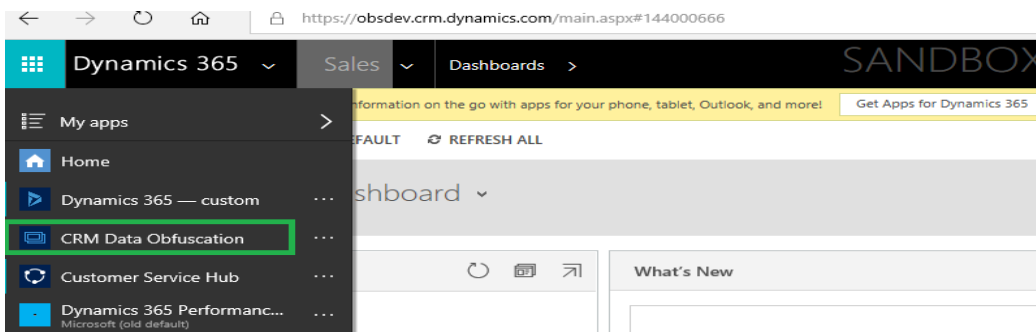


Verify Solution Installation

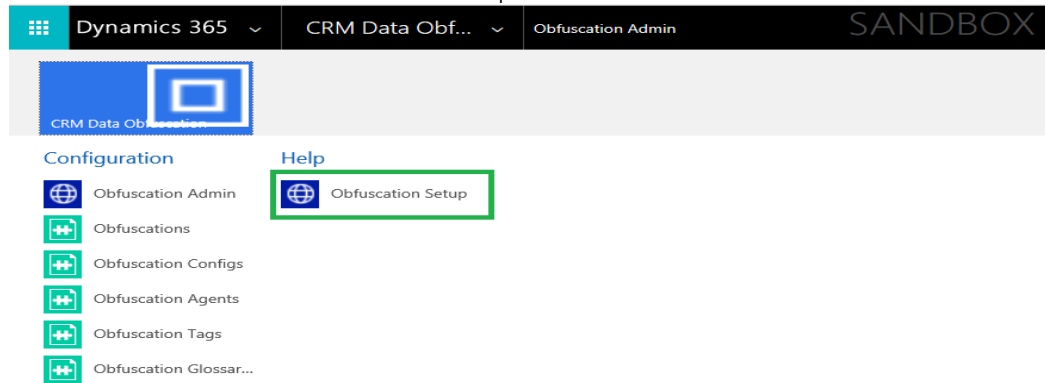
Once install the solution from AppSource. Go to **Settings | Solutions** and Check for the solution.



Look for CRM Data Obfuscation on the left navigation as shown in below picture.



Click on CRM Data Obfuscation → Obfuscation Setup



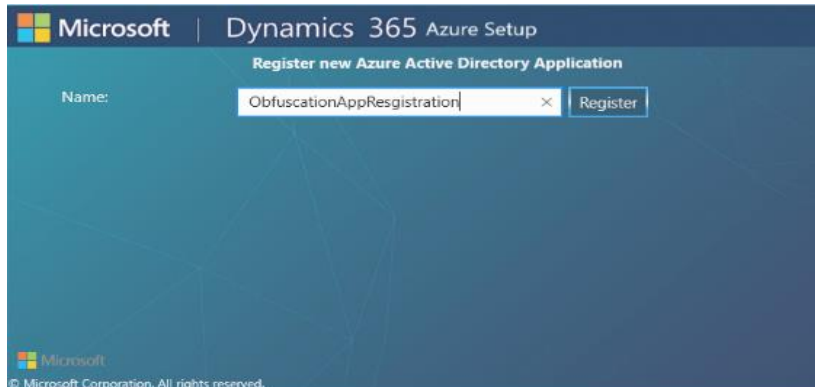
Obfuscation Setup

Dynamics 365 Azure setup

Go to **Obfuscation** | **Obfuscation Setup** | **Dynamics 365 Azure setup**

If you have already registered the applications in Azure Active Directory, you can skip this step.

1. Download and install the Windows Store Application **Dynamics 365 Azure Setup** from [here](#) Once the application is installed, it will show up as a Start menu item.
2. Launch Dynamics 365 Azure Setup app as shown below and enter the required details and save results



After Register the application, below is the snap shot for Keys

Microsoft | Dynamics 365 Azure Setup

Register new Azure Active Directory Application

Name:

Key Vault Application Id:

Secret Key:

Object Id:

Native Application Id:

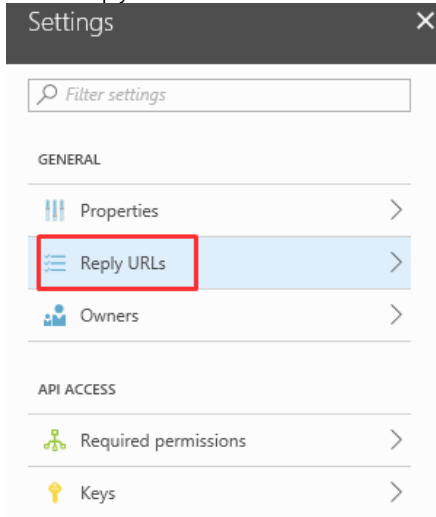
Successfully Registered App, Please note the Appld, Object Id and Secret Key which will be required further

© Microsoft Corporation. All rights reserved.

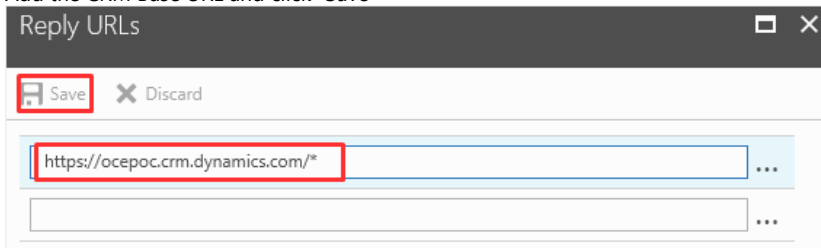
3. Go to Azure Portal -> open the newly created WebApp -> Click Settings

<div><div>⚙ Settings</div><div>✎ Manifest</div><div>🗑 Delete</div></div>	
Display name	Application ID
Obfuscation-Demo-Web-API	fdc44122-10e0-41b8-a0f3-e5b06ec9c274
Application type	Object ID
Web app / API	bbd34358-3f60-4da9-973c-0379dd7d6139
Home page	Managed application in local directory
https://bing.com	Obfuscation-Demo-Web-API

4. Click Reply URLs



5. Add the CRM Base URL and click "Save"



6. Click **Required Permissions** (in 2nd step, under "API ACCESS" section) - > click **+Add** button

- a. **Select an API | Microsoft Azure Data Catalog** | Click on **Select**. In **Select permissions** tick the only available **DELEGATED PERMISSIONS** and click on **Select** and then **Done**.
- b. Follow the above same step to add Permissions to **Azure Key Vault** API
- c. Follow the same instructions given in above step a., to add Permissions to **Windows Azure Active Directory** API. But select only **Sing In and read user profile** Permission as shown in below screen.

Required permissions

+ Add

Grant Permissions

API	APPLICATION PERM...	DELEGATED PERMIS...
Windows Azure Active Directory	0	1
Microsoft Azure Data Catalog	0	1
Azure Key Vault	0	1

Enable Access

Windows Azure Active Directory

Save

Delete

Manage apps that this app creates or owns	Yes
Read and write all applications	Yes
Read and write domains	Yes
DELEGATED PERMISSIONS	
Access the directory as the signed-in user	No
Read directory data	Yes
Read and write directory data	Yes
Read and write all groups	Yes
Read all groups	Yes
Read all users' full profiles	Yes
Read all users' basic profiles	No
Sign in and read user profile	No
Read hidden memberships	Yes

7. Click "Settings" -> Click Manifest

Settings

Manifest

Delete

Display name

Obfuscation-Demo-Web-API

Application type

Web app / API

Home page

<https://bing.com>

Application ID

fdc44122-10e0-41b8-a0f3-e5b06ec9c274

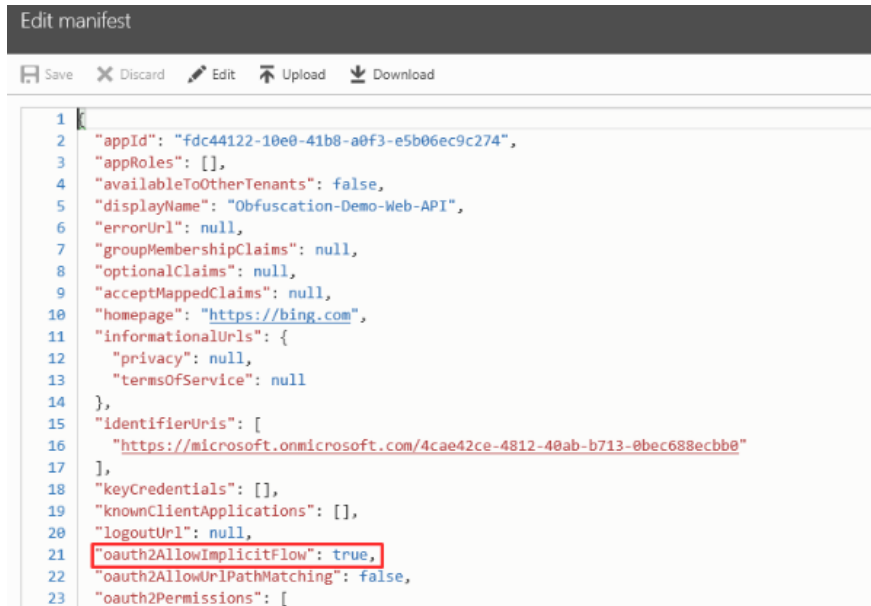
Object ID

bbd34358-3f60-4da9-973c-0379dd7d6139

Managed application in local directory

Obfuscation-Demo-Web-API

8. Change the "oauth2AllowImplicitFlow" to true and Save.



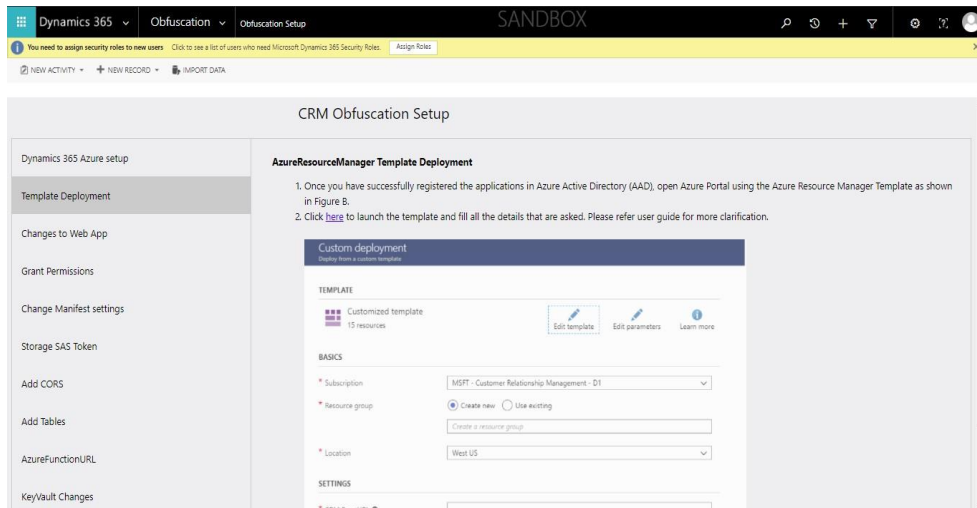
```
1
2 "appId": "fdc44122-10e0-41b8-a0f3-e5b06ec9c274",
3 "appRoles": [],
4 "availableToOtherTenants": false,
5 "displayName": "Obfuscation-Demo-Web-API",
6 "errorUrl": null,
7 "groupMembershipClaims": null,
8 "optionalClaims": null,
9 "acceptMappedClaims": null,
10 "homepage": "https://bing.com",
11 "informationalUrls": {
12   "privacy": null,
13   "termsOfService": null
14 },
15 "identifierUri": [
16   "https://microsoft.onmicrosoft.com/4cae42ce-4812-40ab-b713-0bec688ecbbe"
17 ],
18 "keyCredentials": [],
19 "knownClientApplications": [],
20 "logoutUrl": null,
21 "oauth2AllowImplicitFlow": true,
22 "oauth2AllowUrlPathMatching": false,
23 "oauth2Permissions": [
```

Template Deployment

Go to **Obfuscation** | **Obfuscation Setup** | **Template Deployment**

1. Once you have successfully registered the applications in Azure Active Directory (AAD), open Azure Portal using the Azure Resource Manager Template as shown in Figure B.
2. Click [here](#) to launch the template and fill all the details that are asked. Please refer user guide for more clarification.

High Important***:** Always select West US Location to deploy Azure Resources. Complete the form and deploy to Azure, then navigate to Azure Portal Resource Group. Make a note of all azure resource's names provided in the template.



Filling Custom Deployment Template:

Launch the custom deployment template and fill the details:

BASICS	
* Subscription	MSFT - CUSTOMER RELATIONSHIP MANAGEMENT - D3
* Resource group	<input checked="" type="radio"/> Create new <input type="radio"/> Use existing <input type="text" value="Create a resource group"/>
* Location	Central US
SETTINGS	
* CRM Base URL ⓘ	https://ocepoc.crm.dynamics.com ✓
* CRM Username ⓘ	***** ✓
* CRM Password ⓘ	***** ✓
* Web API Client Id ⓘ	<input type="text"/>
* Web API Secret ⓘ	<input type="text"/>

* Web API Object Id ⓘ

* Native Client Id ⓘ

* Data Catalog Client Id ⓘ

* Data Catalog Name ⓘ

* Data Catalog Secret ⓘ

* Data Catalog Tenant Id ⓘ

* Stakeholder Object Ids ⓘ

* Stakeholder Upns ⓘ

Web Site Name ⓘ

ObfuscationWebApp

Key Vault Name ⓘ

obskeyvault

Storage Account Name ⓘ

obfuscationstorageacc

Storage Account Type ⓘ

Standard_LRS

Function App Name ⓘ

ObfuscationFunctionApp

Hosting Plan Name ⓘ

ObfuscationAppServicePlan

Sku Name ⓘ

S3

Sku Capacity ⓘ

1

CRMAPI Version ⓘ

v8.2

TERMS AND CONDITIONS

[Azure Marketplace Terms](#) | [Azure Marketplace](#)

By clicking "Purchase," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with the publisher of that offering.

☐ I agree to the terms and conditions stated above

☐ Pin to dashboard

Purchase

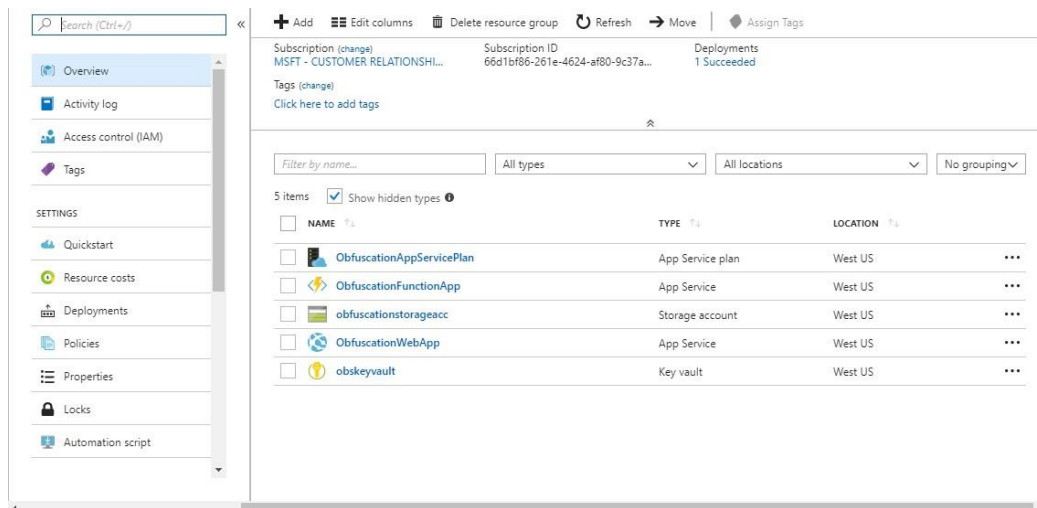
Azure Resource Manager Template Properties

- **Subscription:** Select the correct subscription from the dropdown list.

- **Resource Group:** Please note the following option choices...
 - **First Time setup:** Be sure to select **Create new** option and add a unique resource group name. **Important:** Save the resource group name for future references.
 - **for any upgrades:** Select the **Use existing** option to use the existing resource group name.
- **Location:** Select the correct location from the dropdown list.
- **CRM Base URL:** CRM instance URL
- **CRM Username:** Use the CRM logged in user name (email address) with Admin privileges.
- **CRM Password:** Implied.
- **Web API Client Id:** Paste the existing Key Vault Application Id
- **Web API Secret Id:** Paste the existing Secret Id
- **Web API Object Id:** Paste the existing Object Id
- **Native Client Id:** Paste the existing Native Application Client Id
- **Data Catalog Client Id:** Get the Data Client Id from Azure Data catalog
- **Data Catalog Name:** Get from Azure data catalog
- **Data Catalog Secret:** Get from Azure data catalog
- **Data Catalog Tenant Id:** Get from Azure data catalog
- **Stake Holder Object Id:** Get from Azure data catalog
- **Stake Holder Upns:** Get from Azure data catalog
- **Web Site Name:** Any unique website name with contiguous characters.
- **Key Vault Name:** Any unique KV name. **Important:** Please use contiguous lowercase letters only.
- **Database Account Name:** Alphanumeric Cosmos account name.
- **Storage Account Name:** Alphanumeric storage account name.
- **Storage account Type:** Select the correct value from the dropdown list.
- **Function App Name:**
- **Hosting Plan Name:** Use only unique contiguous lowercase characters.
- **Sku Name:** Select the correct value from the dropdown list.
- **Sku Capacity:** Suggest using the Default value of 1.
- **CRM Web API Version:** Select the correct value from the dropdown list.
-

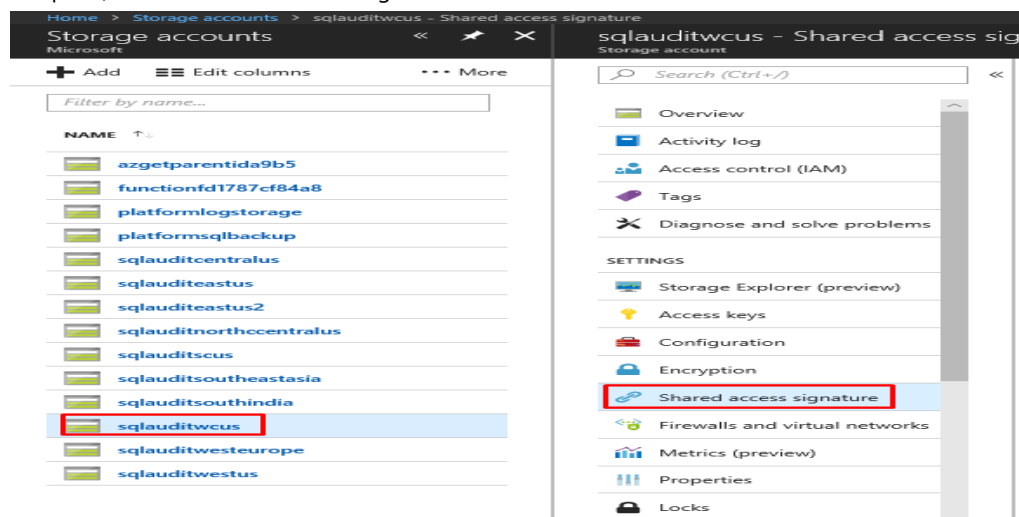
Agree the **Terms and Conditions** and click on the **Purchase** button.

Once the deployment Completed Below are the Azure components



Generate SAS Token

Go to Azure Portal -> Choose the corresponding Storage Account (created using above ARM template) -> click "Shared Access Signature"



1. Choose the following "Allowed Services" – "Blob", "Table"
2. Choose the following "Allowed Resource Types" – "Service", "Container" and "Object"
3. Choose the appropriate Start and End Date Time, try to give start date one day prior to current date and end date as later than an year.
4. Click "Generate SAS and connection string"
5. Copy the "SAS Token" and add as Secret "StorageSASToken" in "KeyVault" ([Reference](#))

A shared access signature (SAS) is a URI that grants restricted access rights to Azure Storage resources. You can provide a shared access signature to clients who should not be trusted with your storage account key but whom you wish to deleg. By distributing a shared access signature URI to these clients, you grant them access to a resource for a specified period of time.

An account-level SAS can delegate access to multiple storage services (i.e. blob, file, queue, table). Note that stored access policies are currently not supported for an account-level SAS.

[Learn more](#)

Allowed services

☒ Blob ☐ File ☐ Queue ☒ Table

Allowed resource types

☒ Service ☒ Container ☒ Object

Allowed permissions

☒ Read ☒ Write ☒ Delete ☒ List ☒ Add ☒ Create ☒ Update ☐ Process

Start and expiry date/time

Start

Expiry

(UTC-07:00) --- Current Timezone ---

Allowed IP addresses

For example, 168.1.5.65 or 168.1.5.65-168.1.5.70

Allowed protocols

☒ HTTPS only ☐ HTTPS and HTTP

Signing key

key1

[Generate SAS and connection string](#)

Connection string

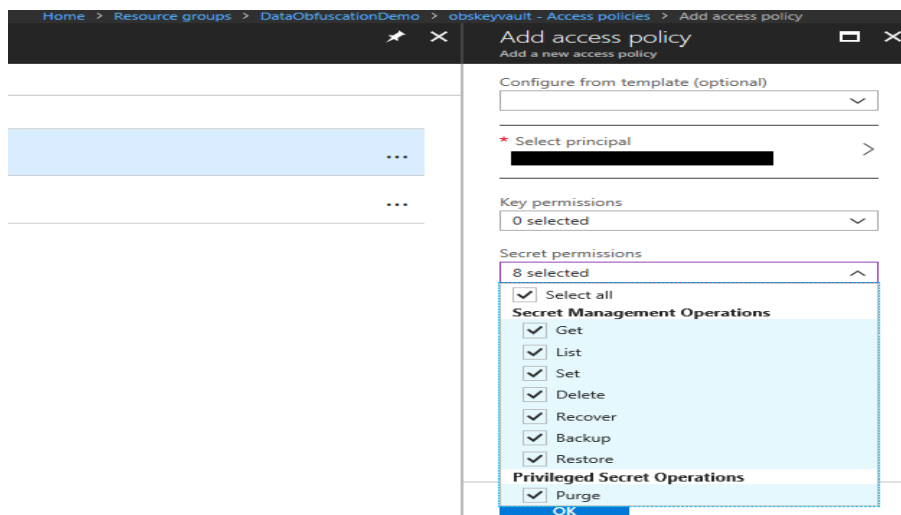
DefaultEndpointsProtocol=https;AccountName=sqclouditwus;AccountKey=t6nxb/+n8c8hp5Hb3Qo257P+/jXOMfzrP90JJZICw45455E/666rq567v801/no8mqaz27QXdcJULIADG8kLQ=;EndpointSuffix=core.windows.net

SAS token

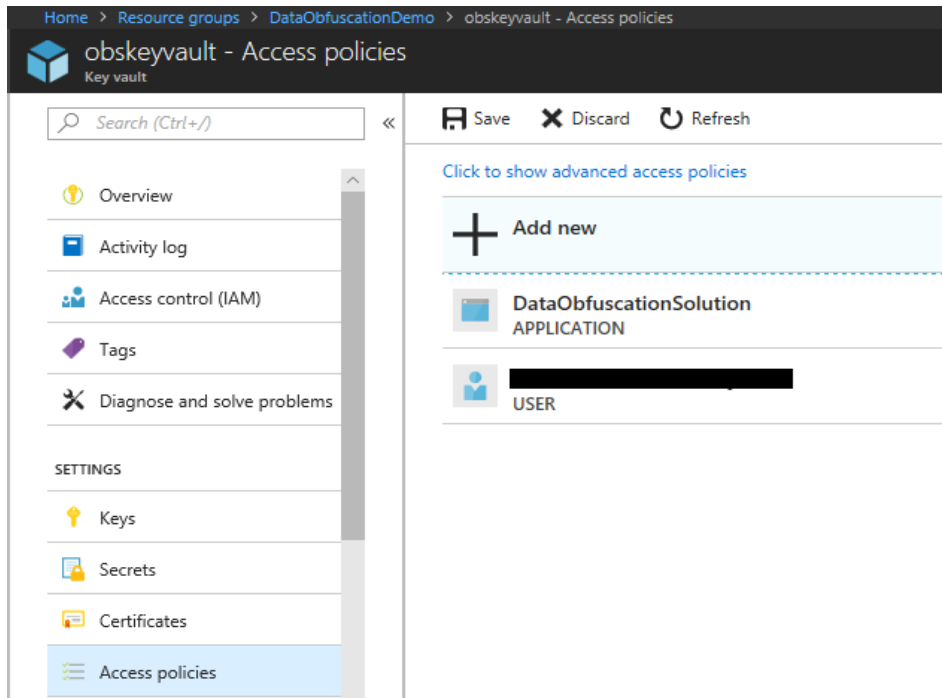
tsv=2017-07-29&ss=bt&sr=sco&sp=rndlacu&se=2019-01-01T08:00:00Z&st=2018-03-25T07:00:00Z&spr=https&sig=PTXh5eqduPmgzWCzKbNsQTD3zfi8dVoiWWFXu6rLY9JD

Adding Secrets values to Key Vault

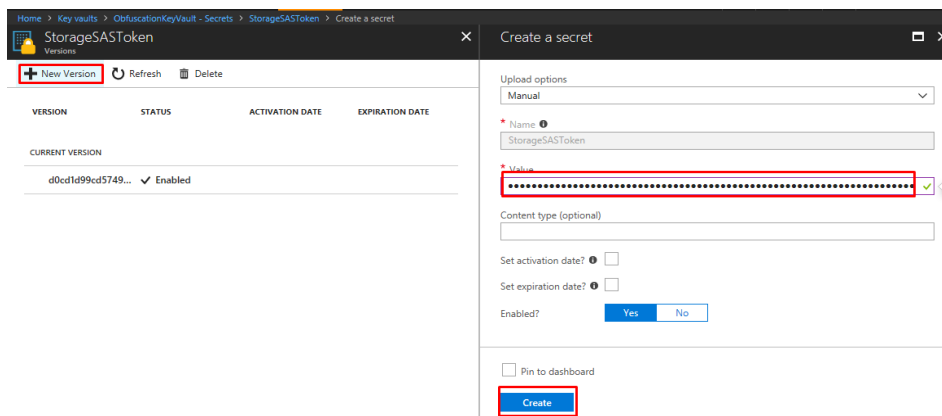
1. Go to Azure Portal -> Choose corresponding Key Vault -> Choose "Access Policies" then click "+Add New"
2. Click on Add -> Select Principal -> Select the User (who performs all these operations) -> Click on Select
3. Select all Secret Permissions and click on OK button



4. save Access Policies



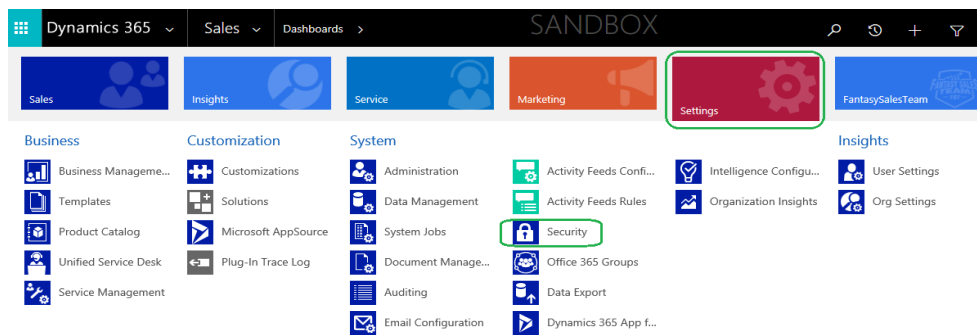
5. Choose the Secret "StorageSASToken" and click "New Version" and paste the SAS Token value in the "Value" textbox and click "Create" button.



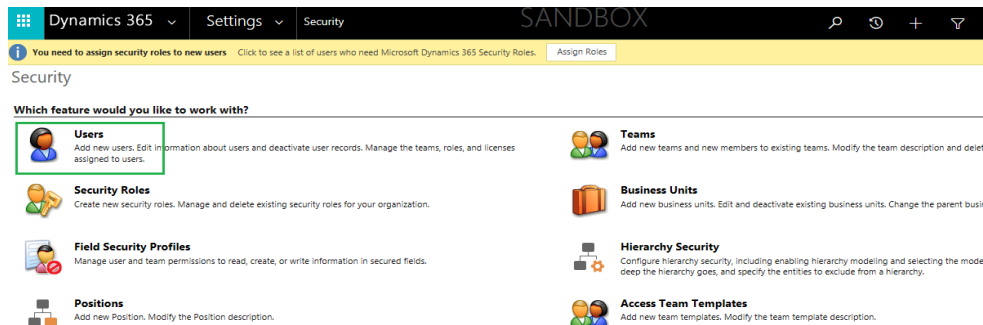
Obfuscation Configuration in CRM

Add Application User in CRM Org

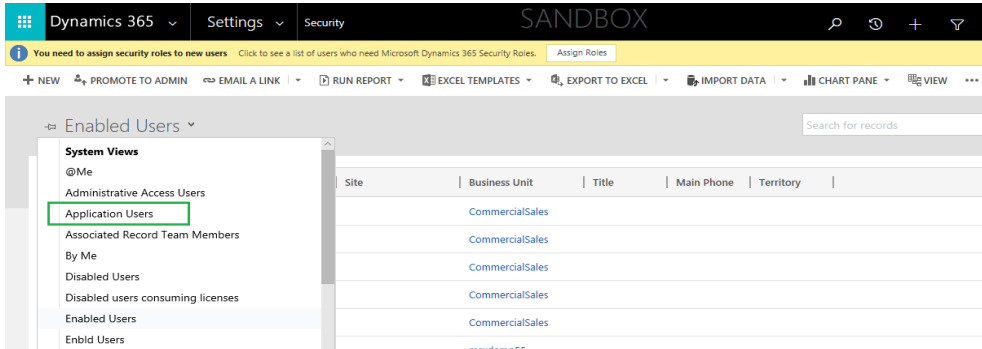
1. Login to CRM Org with a user who has **system admin role**
2. Click on **Settings** - > **Security** as shown in below image.



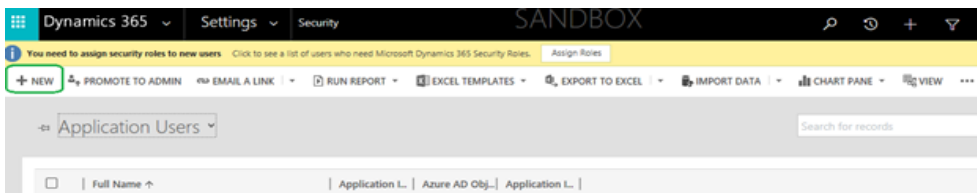
3. Click on **Users** as shown in below image



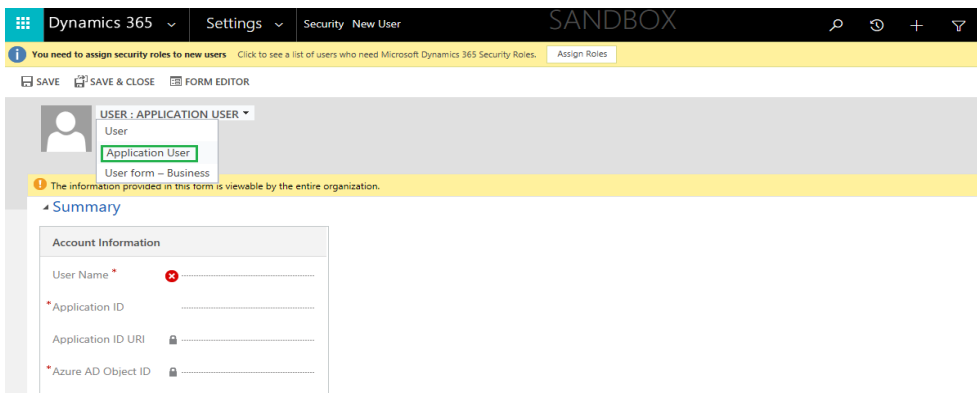
4. Select **Application Users** from the dropdown as shown in below image



5. Click on + **New** as shown in below image



6. Select **Application User View** from the View Selector (if it is not already selected) as shown in below image.



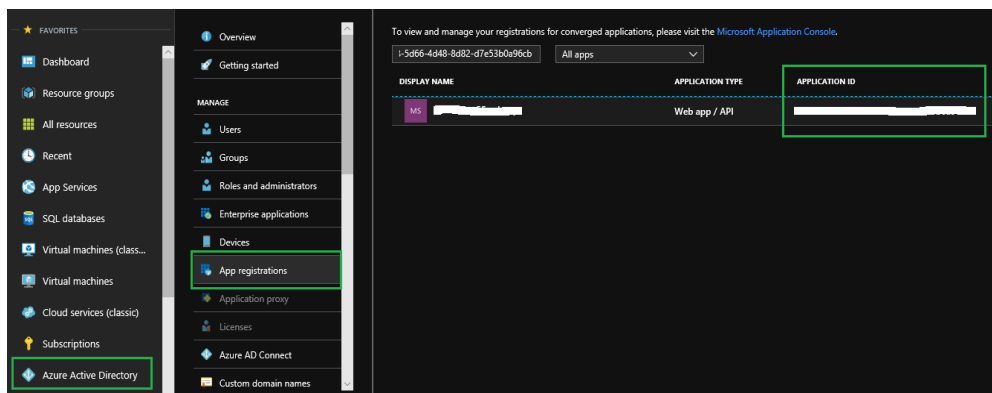
7. Provide details as mentioned below and Save the details

- **Application ID:** Azure Active Directory Web Application ID (Application ID generated for AAD Web App, refer below screen shot).
- **Full Name:** Any valid full name. For ex: First Name: **Obfuscation** & Last Name: **Admin**
- **Primary Email:** Any valid email. For ex: dummy@dummy.com
 *Above email address will not be using in obfuscation process to send any emails.

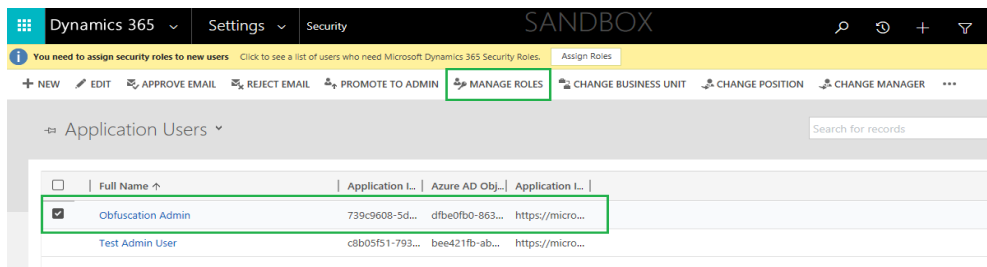
Note: User Name, Application ID URI & Azure AD Object ID will get created when user is saved.

Commented [PKK1]: Add Azure screen shot representing web app ID extraction.

Commented [CG(L2R1)]: Done



8. Select the newly created Application User.
Click on Manage Roles
and grant System Admin role.s

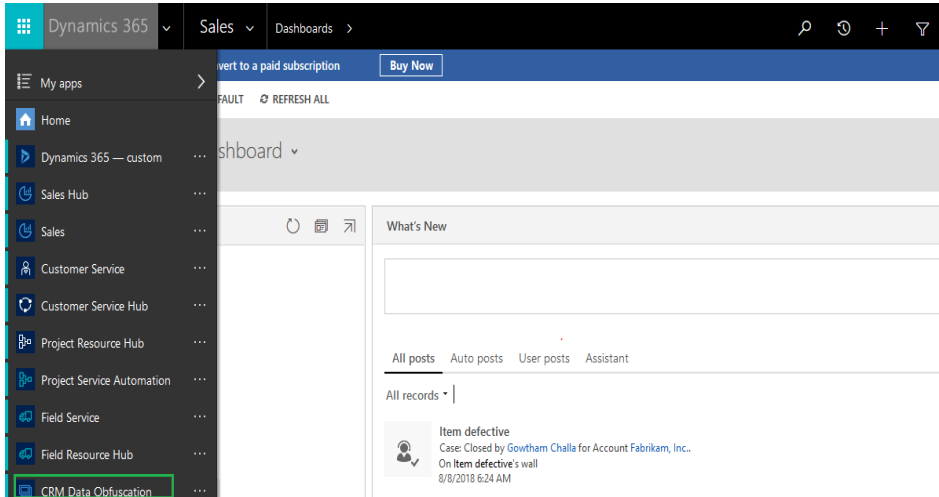


Obfuscation Agents to CRM Org

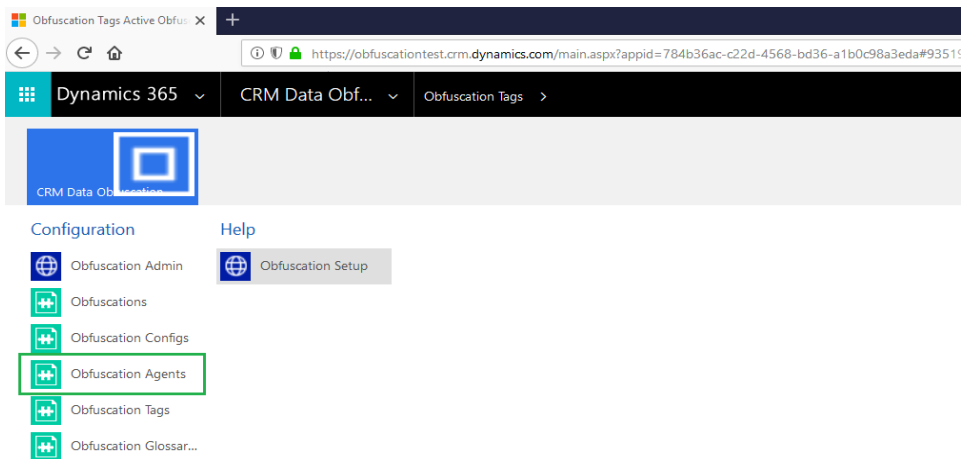
CRM Org -> CRM Data Obfuscation (available in left navigation view)

Commented [PKK3]: Put appropriate screen shot

Commented [CG(L4R3)]: Done

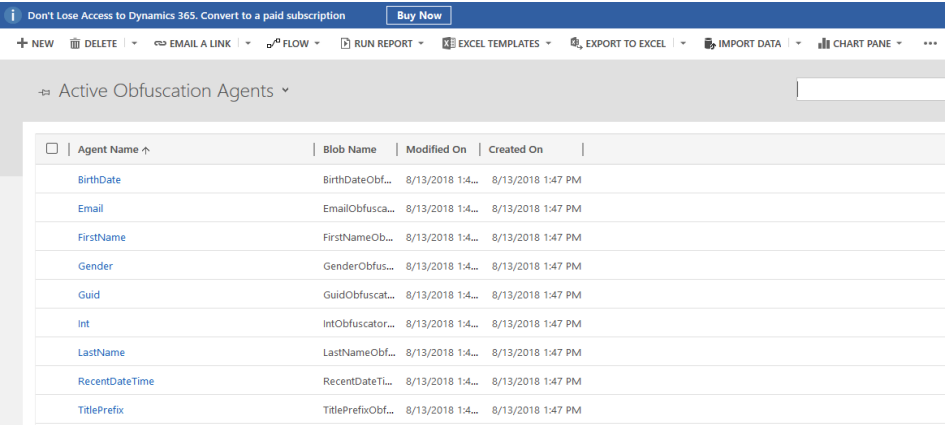
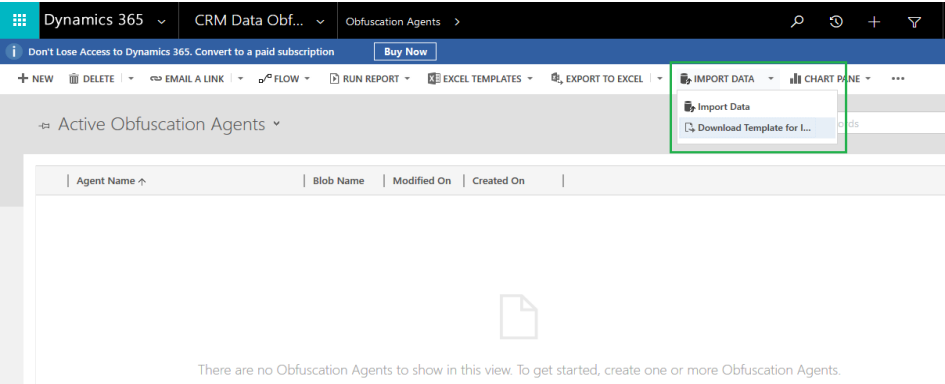


Select obfuscation Agents entity as shown in below image.



Agents are available in [location](#). Download all available agents and Upload them using IMPORT DATA option as shown below.

Note: these agents are sample agents which comes by default with the solution. Refer section **(Add New Obfuscation Agent)** to add new obfuscation agent and configuring into the system.

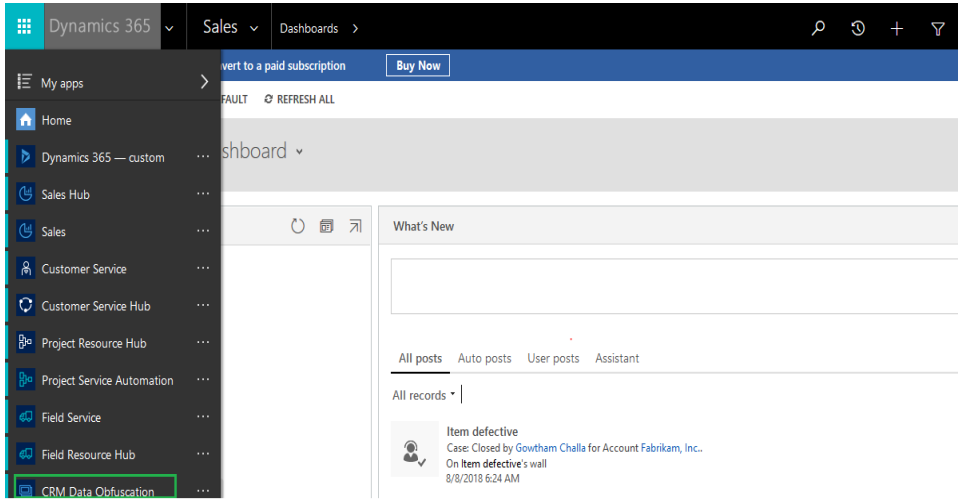


Add New Obfuscation Agent

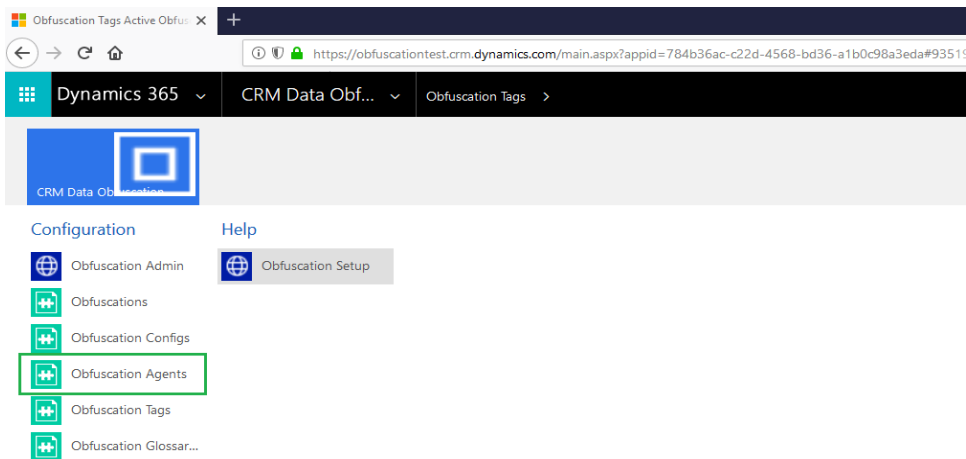
CRM Org -> CRM Data Obfuscation (available in left navigation view)

Commented [PKK5]: Put appropriate screen shot

Commented [CG(L6R5)]: Done



Select obfuscation Agents entity as shown in below image.



Click on Obfuscation Agents to see all available agents as shown in below image.

Don't Lose Access to Dynamics 365. Convert to a paid subscription [Buy Now](#)

[+ NEW](#)
[DELETE](#)
[EMAIL A LINK](#)
[FLOW](#)
[RUN REPORT](#)
[EXCEL TEMPLATES](#)
[EXPORT TO EXCEL](#)
[IMPORT DATA](#)
[CHART PANE](#)

Active Obfuscation Agents

<input type="checkbox"/>	Agent Name ↑	Blob Name	Modified On	Created On
	BirthDate	BirthDateObf...	8/13/2018 1:4...	8/13/2018 1:47 PM
	Email	EmailObfusca...	8/13/2018 1:4...	8/13/2018 1:47 PM
	FirstName	FirstNameOb...	8/13/2018 1:4...	8/13/2018 1:47 PM
	Gender	GenderObfus...	8/13/2018 1:4...	8/13/2018 1:47 PM
	Guid	GuidObfuscat...	8/13/2018 1:4...	8/13/2018 1:47 PM
	Int	IntObfuscator...	8/13/2018 1:4...	8/13/2018 1:47 PM
	LastName	LastNameObf...	8/13/2018 1:4...	8/13/2018 1:47 PM
	RecentDateTime	RecentDateTL...	8/13/2018 1:4...	8/13/2018 1:47 PM
	TitlePrefix	TitlePrefixObf...	8/13/2018 1:4...	8/13/2018 1:47 PM

Click on +New button as shown in below image to add new agents

Don't Lose Access to Dynamics 365. Convert to a paid subscription [Buy Now](#)

[+ NEW](#)
[DELETE](#)
[EMAIL A LINK](#)
[FLOW](#)
[RUN REPORT](#)
[EXCEL TEMPLATES](#)
[EXPORT TO EXCEL](#)
[IMPORT DATA](#)
[CHART PANE](#)

Active Obfuscation Agents

<input type="checkbox"/>	Agent Name ↑	Blob Name	Modified On	Created On
	BirthDate	BirthDateObf...	8/13/2018 1:4...	8/13/2018 1:47 PM
	Email	EmailObfusca...	8/13/2018 1:4...	8/13/2018 1:47 PM
	FirstName	FirstNameOb...	8/13/2018 1:4...	8/13/2018 1:47 PM
	Gender	GenderObfus...	8/13/2018 1:4...	8/13/2018 1:47 PM
	Guid	GuidObfuscat...	8/13/2018 1:4...	8/13/2018 1:47 PM
	Int	IntObfuscator...	8/13/2018 1:4...	8/13/2018 1:47 PM
	LastName	LastNameObf...	8/13/2018 1:4...	8/13/2018 1:47 PM
	RecentDateTime	RecentDateTL...	8/13/2018 1:4...	8/13/2018 1:47 PM
	TitlePrefix	TitlePrefixObf...	8/13/2018 1:4...	8/13/2018 1:47 PM

Provide Agent name and click on SAVE & CLOSE button as shown in below image.
Note: Blob Name will be auto generated.

Dynamics 365 CRM Data Obf... Obfuscation Agents > New Obfuscation Ag... **SANDBOX**

You need to assign security roles to new users Click to see a list of users who need Microsoft Dynamics 365 Security Roles. Assign Roles

SAVE SAVE & CLOSE + NEW FORM EDITOR

OBFUSCATION AGENT : INFORMATION
New Obfuscation Agent

General

Agent Name * NewAgent

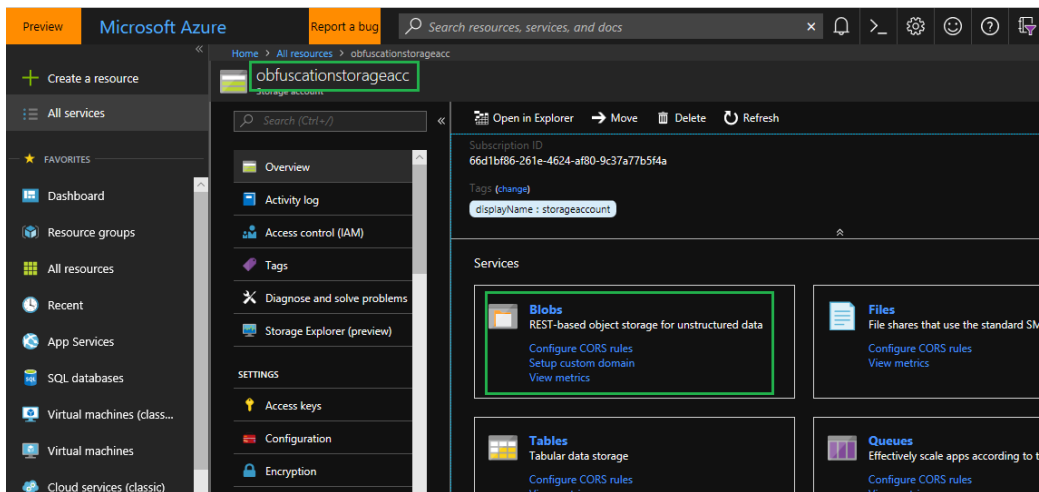
Blob Name * NewAgentObfuscator.cs

Owner * Next Gen Sales Dev Account *

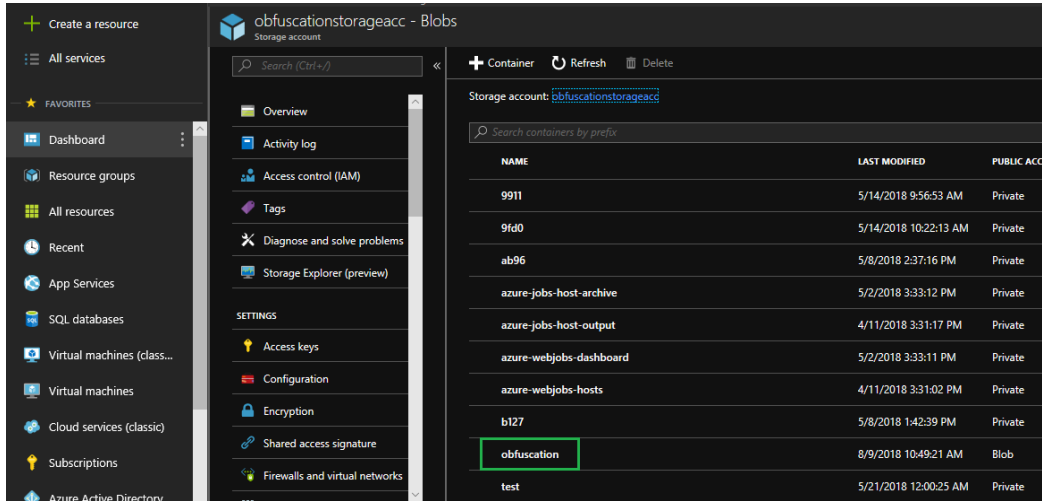
Note: Obfuscation Agents need to be added to Azure blob Refer section (**Upload New Agents to Azure Blob**) before adding an agent detail here.

Upload New Agents to Azure Blob

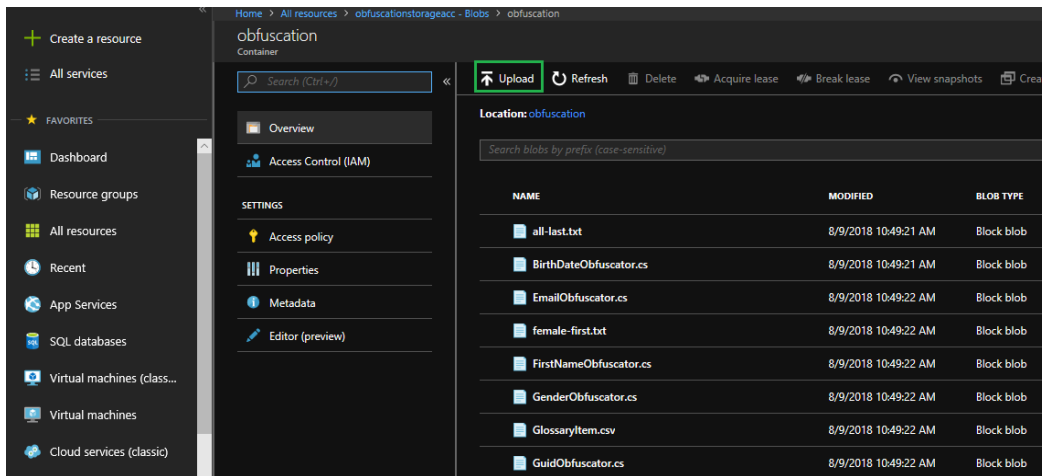
Go to Azure Portal -> Choose the corresponding Storage Account (created using above ARM template) -> click blobs, as shown in below images.



Click on Container obfuscation.



Use Upload button to upload new Agents.



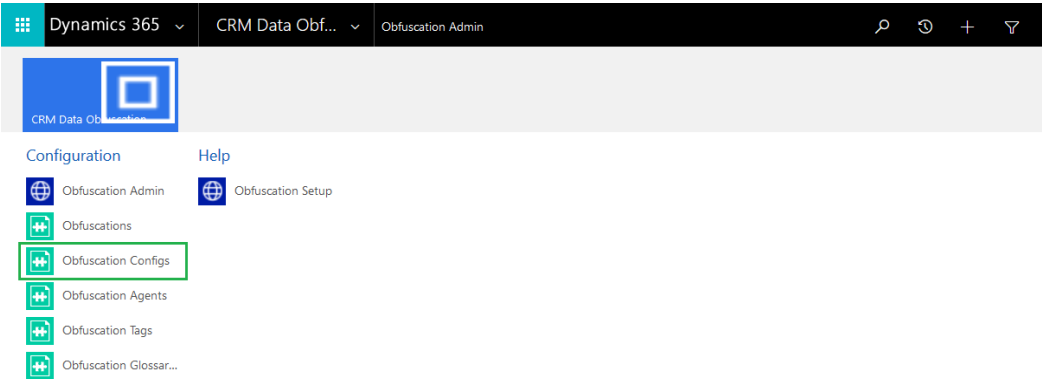
CRM Initial Sync and Data Sync

CRM Initial Sync:

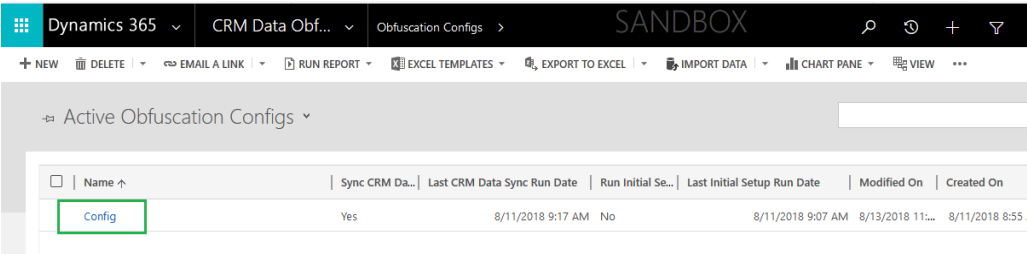
This should run only once after ARM Template deployment.

MICROSOFT LABS

CRM Initial Sync option is available in CRM Org -> CRM Data Obfuscation (available in left navigation) -> Obfuscation Configs entity.



Click on Config in Active Obfuscation Configs



Select Run Initial Setup Check box. This is one-time activity, this will be Un-Checked by Web job after successful run. Initial sync takes care of below listed activities,

- Upload initial set of Obfuscator agents and setup files to Azure blob
- Set Storage CORS
- Sync Glossary terms to Azure Data Catalog
- Create Config entity & Obfuscation Agent table

Commented [PKK7]: Add all the activities we are doing in initial sync for user understanding.

Commented [CG(L8R7)]: Done

OBFUSCATION CONFIG : INFORMATION

Config

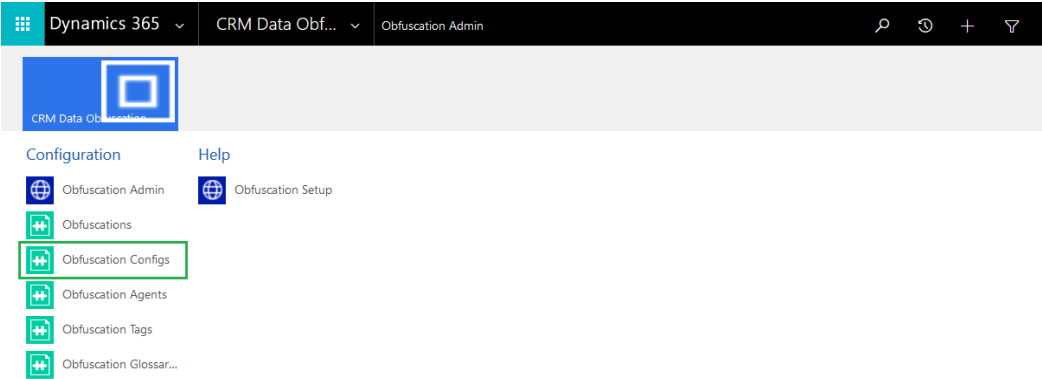
Key Vault Secret	ML38iVg4hzk7oW/bgQL6isxuQ5EvyIq/RH4GbUWpIc=
Key Vault App Name
Name *	Config
Owner *	 Obfuscation Admin

Obfuscation Sync Settings	
Run Initial Setup	<input checked="" type="checkbox"/>
Last Initial Setup Run Date 8/11/2018 9:07 AM	
Sync CRM Data	<input checked="" type="checkbox"/>
Last CRM Data Sync Run Date 8/11/2018 9:17 AM	

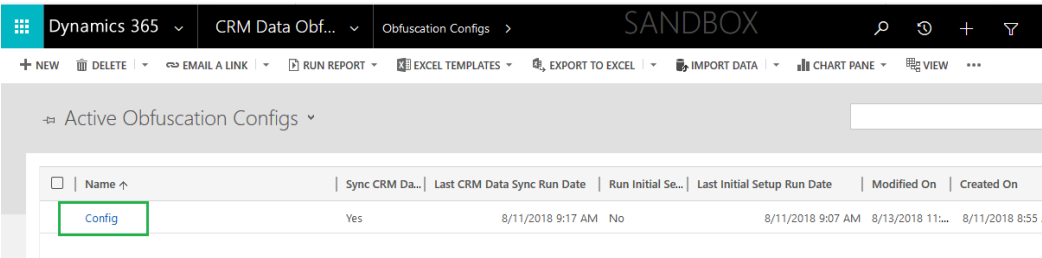
CRM Data Sync:

This should run every time when data need to be synched. This will be taken care by Web job. User need to schedule the Sync Job. If user want to run on-demand, follow below steps.

CRM Data Sync option is available in CRM Org -> CRM Data Obfuscation (available in left navigation) -> Obfuscation Configs entity.



Click on Config in Active Obfuscation Configs



Select Sync CRM Data Check box. Sync job will run based on schedules.

OBFUSCATION CONFIG : INFORMATION

Config

Key Vault Secret

ML38IVg4hzik7oW/bgQL6isxuQ5EvyJq/RH4GbUWplc=

Key Vault App Name

Name

Config

Owner

Obfuscation Admin

Obfuscation Sync Settings

Run Initial Setup

☒

Last Initial Setup Run Date

8/11/2018 9:07 AM

Sync CRM Data

☒

Last CRM Data Sync Run Date

8/11/2018 9:17 AM

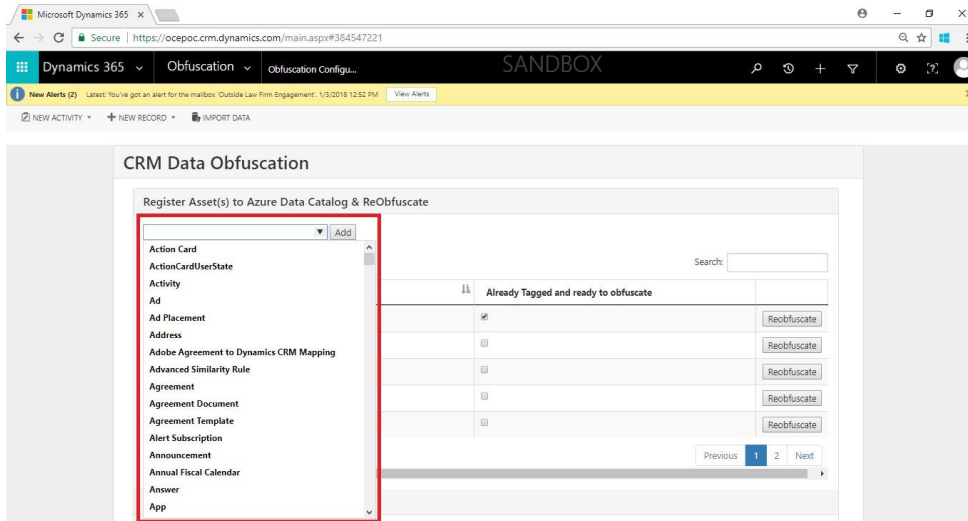
Note: Sync CRM Data Check box will be selected when user make any changes to CRM Data Obfuscation page.

Commented [PKK9]: Its not config page rather any changes made to tags configuration in admin UI

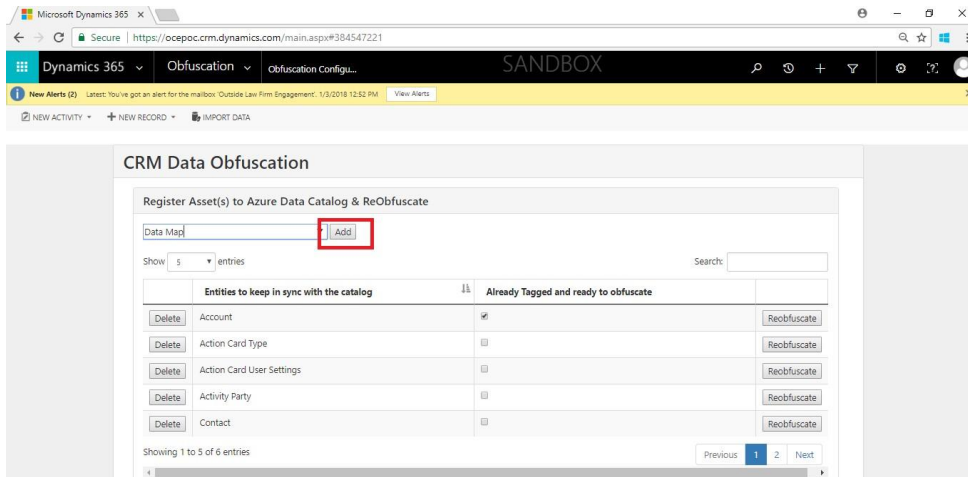
Commented [CG(L10R9)]: Done

Adding Entity for Obfuscation

1. Go to Obfuscation Configuration page and click on the drop down under register Asset(s) to Azure Data Catalog & ReObfuscate. All available entity will appear in the drop down.



2. Click on Entity name which you want to register and Click on Add Button.



3. Selected Entity gets added into the grid. Entity can be deleted or Reobfuscate.

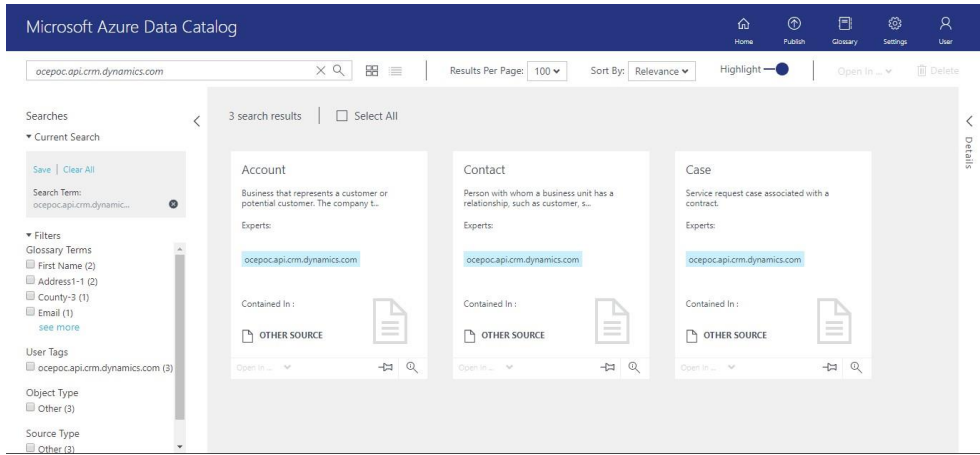
Delete: Deletes the entity from the list

Reobfuscate: Clicking on this button will Re-Obfuscate the previously Obfuscated entities.

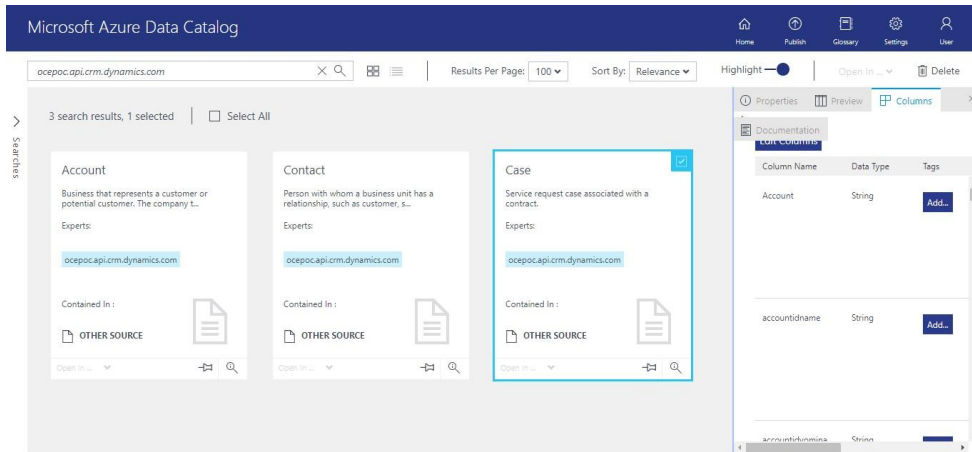
4. Navigate to Azure data catalog to add tags to the Selected entity. Enter the org name in the format of **'org.api.crm.dynamics.com'** to find out the listed entities in Azure Catalog. Pls. note that this entity related information must be pushed by the sync job. **By default, Web Job Sync data between Azure Data Catalog and CRM will run on first minute in every hour and web job Obfuscation starts every 30th minute of every hour.**

This is configurable in Resource groups | Select the Resource Group | Select App Service | Select App Settings | Change Sync Schedule or Obfuscation schedule (chronic expression)

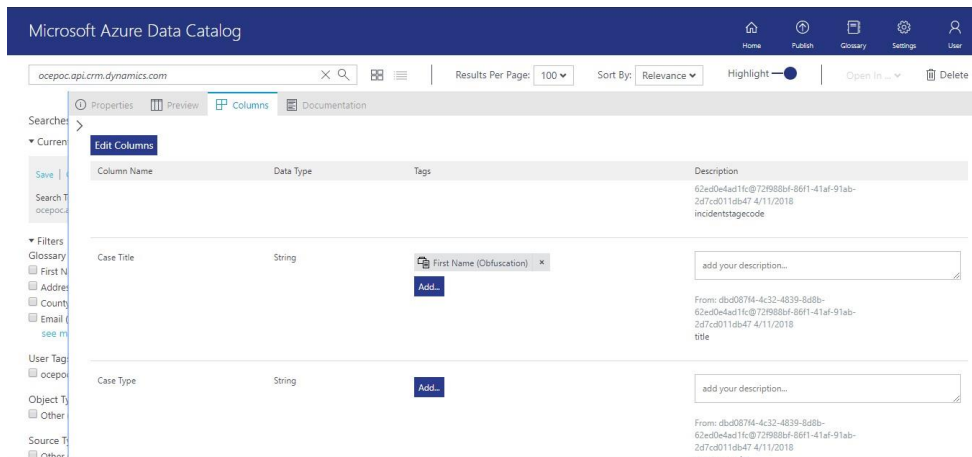
Click on the displayed entity to add the tags



Select the entity and click on right side top 'Columns'

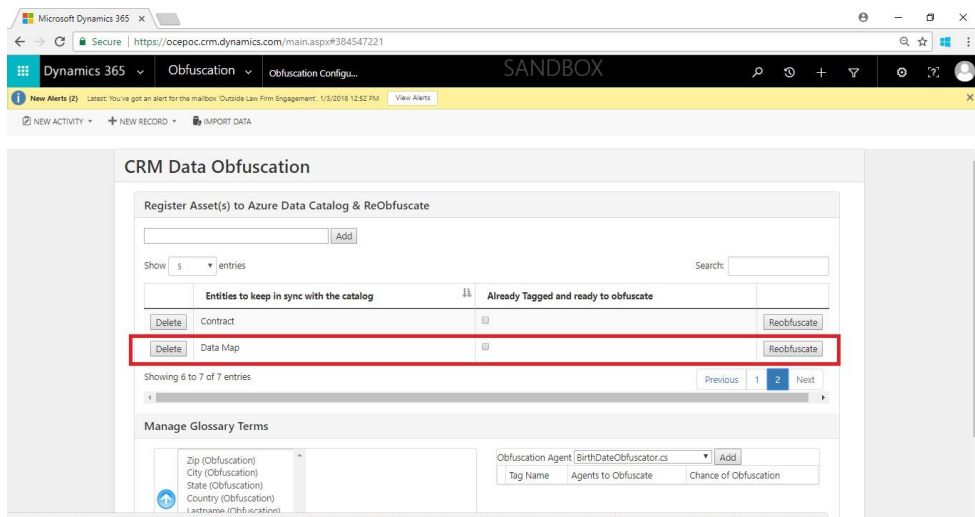


Add the catalog. In the below example We have added First Name Tag to Case Title column of Case entity.

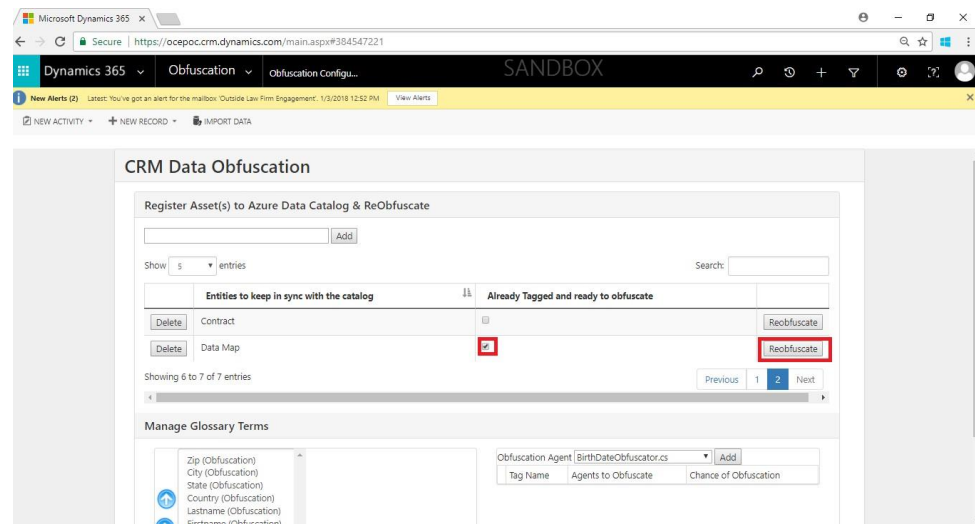


Now Switch back to CRM to select the tag in Manage Glossary Terms.

Agent.Cs : These are the actual agents written in C# to use obfuscation on the selected obfuscator column.

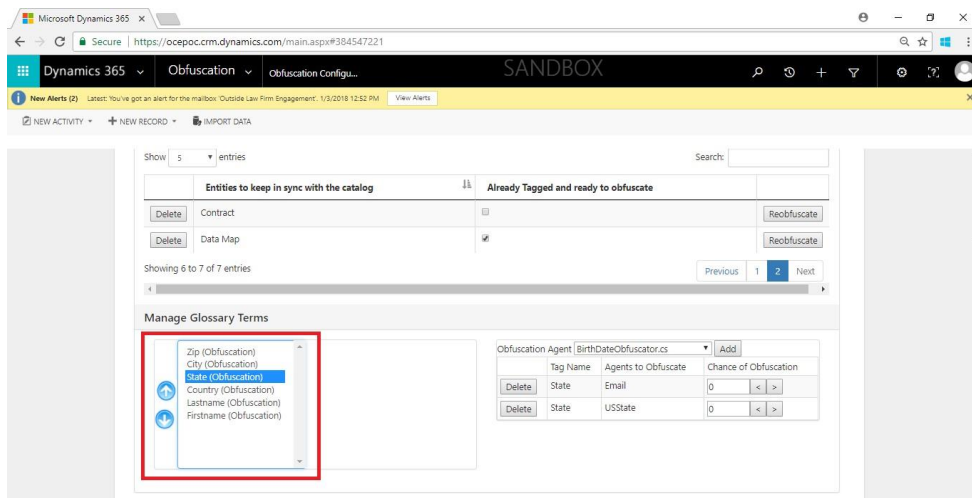


5. For ReOfuscation, checked Already Tagged and ready to obfuscate check box and Click on ReObfuscate button.

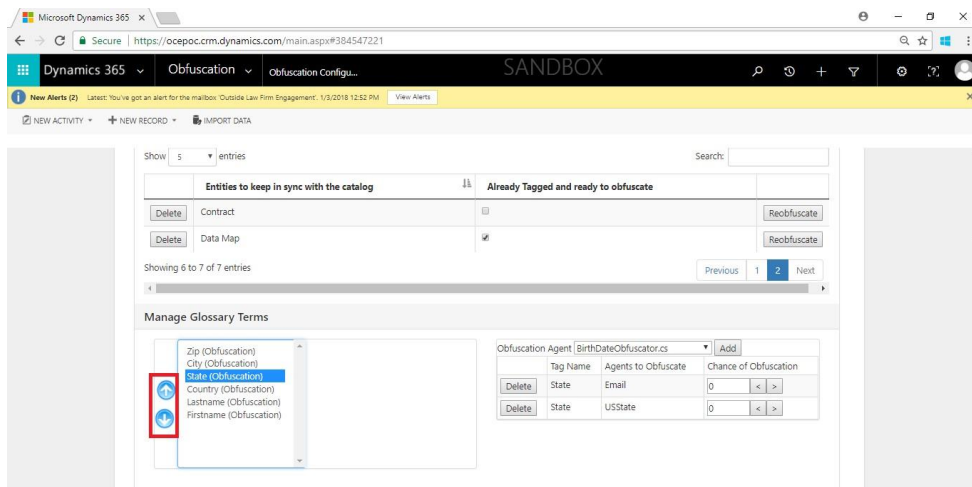


Glossary Term Execution Order

1. Glossary term combo box appearing under Manage Glossary Term can be set with a sequence number by moving it up or down on a specific position.

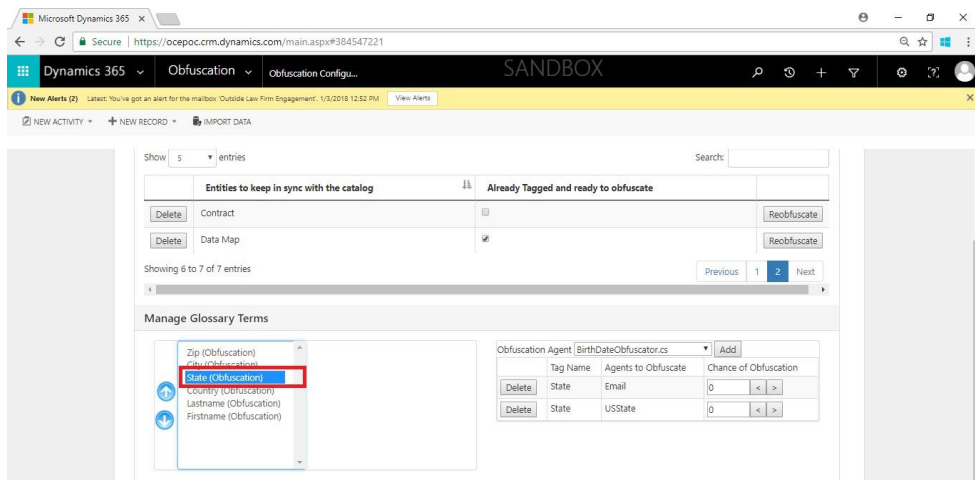


2. Clicking on Move Up or Move down will move up or down the glossary and set the execution order as per the sequence number of combo box.

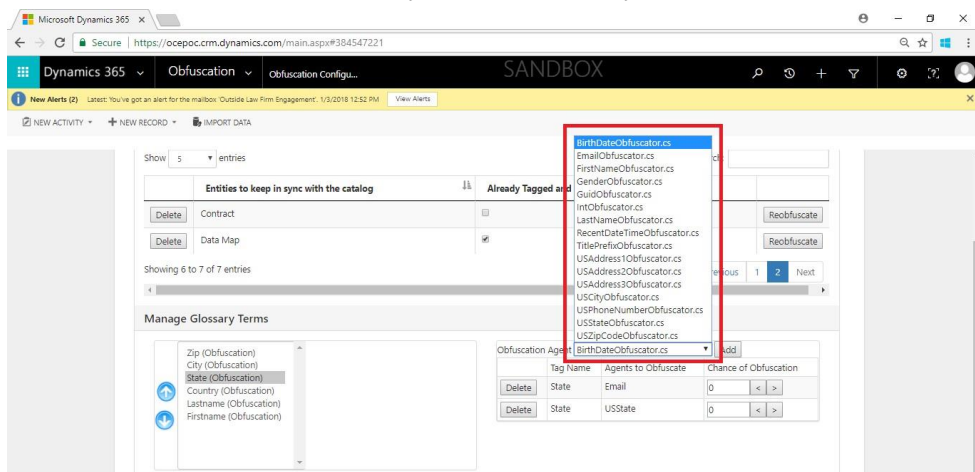


Adding a new Glossary – Obfuscation Agent

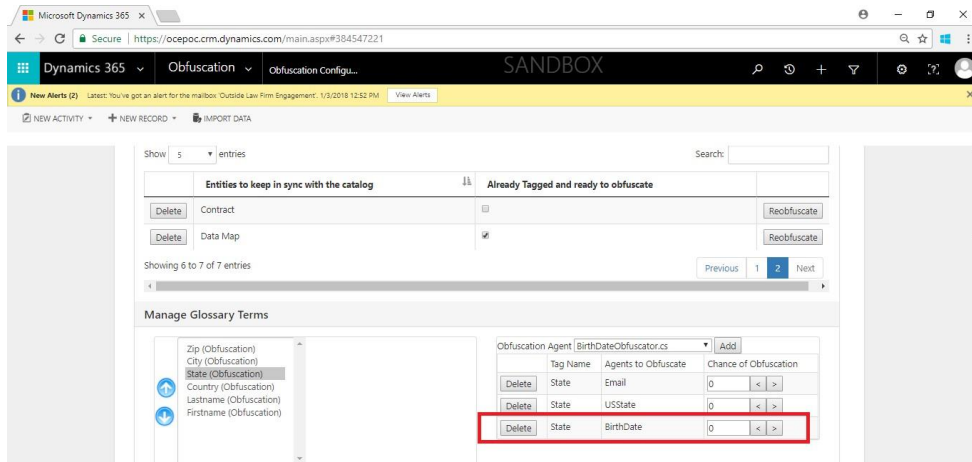
1. Select any Glossary Term.



2. Select any Obfuscation Agent that is not exist in the grid below to Agent drop down. If you try to add the combination which is already exist, it will not allow you to add the same.

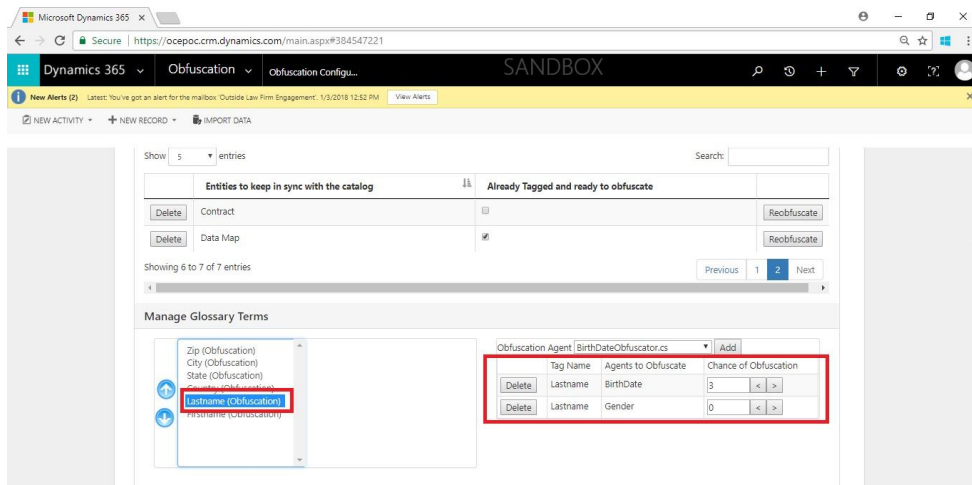


3. Click on the Add button. It will add a new row in the grid with weight as 0.



Edit a Glossary term – Obfuscation Agent combination

1. Select Glossary term and the grid will start showing all Obfuscation Agent with their respective weight.



2. You can update the weight by increase/decrease it or directly entering into weight textbox. The same can be deleted by clicking on Delete button.


This means: User have a choice to increase or decrease the obfuscation of the selected column values in the entity. If 100 selected, the agent will obfuscate all the values in the selected columns.

Least Permissions required to access Obfuscation area

This section describes providing minimal security settings permissions required for users to access **Dynamics 365 Data Tagging & Obfuscation**.

Users should be having **Read Permissions** (Least Permissions) on **ObPrivilege** entity to access Dynamics 365 Data Tagging & Obfuscation area in Sitemap. The steps to provide the minimal security settings needed on the custom entity are:

- 1. Login to CRM and go to **Settings | Security Roles | Select A Role**
- 2. Go to **"Custom Entities"** tab, **ObPrivilege** Entity, and provide Read Permissions.

 **Security Role: Salesperson**

Details	Core Records	Marketing	Sales	Service	Business Management	Service Management	Customization	Missing Entities	Business Process Flows	Custom Entities
ObPrivilege						<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Page						<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Page Alert						<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

End User Experience

In this section will obfuscate the Contact entity - First Name.

- Below are the steps:
- 1. Through Advance Find Query, select the Contact entity – First Name values. This can be used to compare after Obfuscation.

FILE

ADVANCED FIND

Query

Saved Views

Results

New

Save

Save As

Edit Columns

Edit Properties

Clear

Group AND

Group OR

Details

Download Fetch XML

Show

View

Query

Debug

Look for: Contacts

Use Saved View: [new]

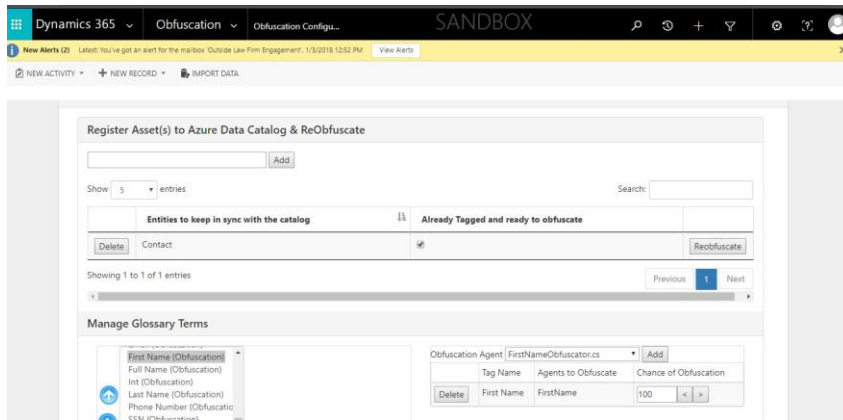
First Name

Contains Data

Select

✓	First Name	Full Name ↑
	Adelaida	Adelaida Easterling
✓	Alden	Alden Kingsberry
	Alden	Alden Lindstedt
	Aleen	Aleen Jest
	Alejandrina	Alejandrina Marchio
	Alfonso	Alfonso Mullahey
	Alfonzo	Alfonzo Denzine
	Ali	Ali Forsell
	Ali	Ali Millard
	Alphonso	Alphonso Schramek
	Amanda	Amanda Buchner
	Amparo	Amparo Kinkade
	Ana	Ana Villamarin
	Andre	Andre Torra
	Angelique	Angelique Malamud
	Anibal	Anibal Vanstrom

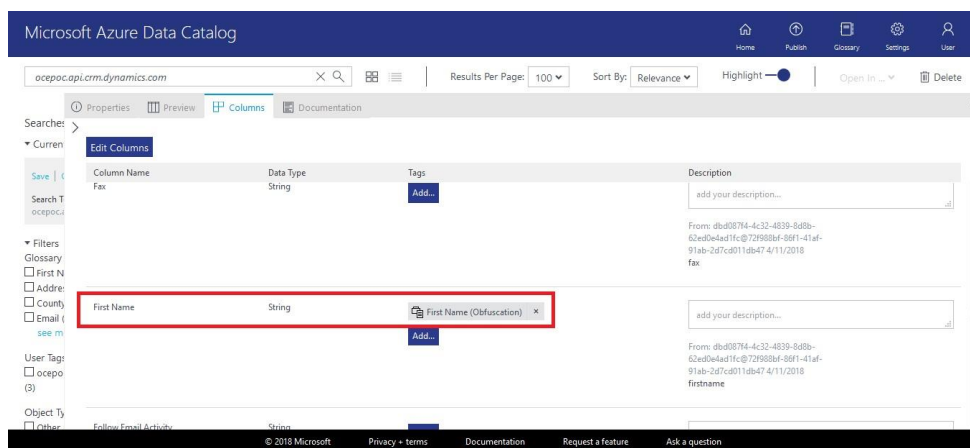
2. Add Contact entity in Obfuscation | Configuration page as shown below



3. Tag Contact entity | First Name field in Azure Data catalog

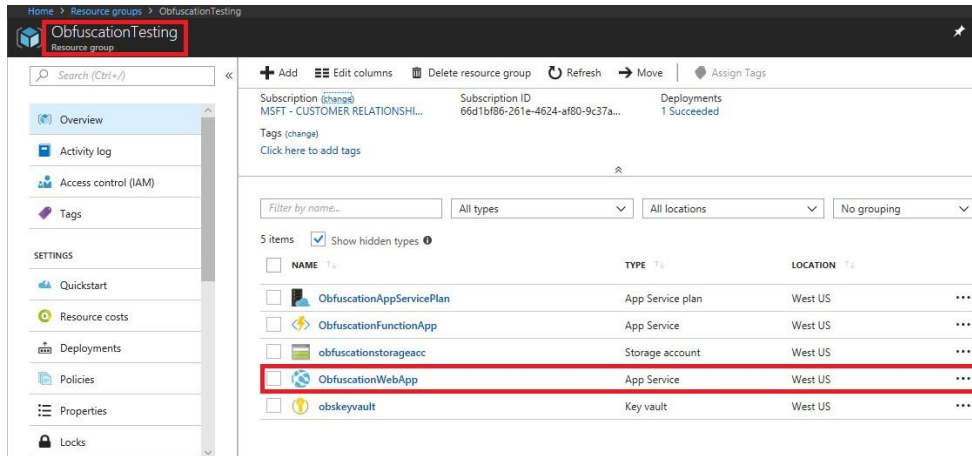
Go to Azure Catalog | Type in Org name | Select the Contact entity | Add the 'First Name(Obfuscation)' to First Name column.

Note: This column tags will be added only when obfuscation web job runs.

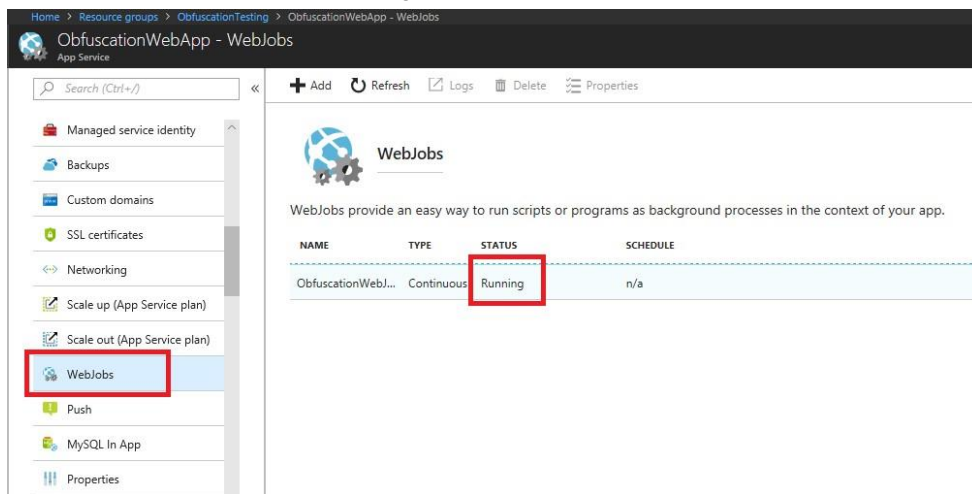


Wait for Obfuscation Web Job to run (Job runs on schedule).

Go to Resource Groups | Select the resource group | Select the Web App



Select Web Job to make sure, Job is running



After running the Web job on its own schedule, below are the results with obfuscated contact entity First Name values

✓	First Name	Full Name ↑
	Abram	Abram Gizewski, Ted M (TEDGI)
	Ada	Ada Botner
	Adalberto	Adalberto Shogren
	Adelia	Adelia Ashburn
	Adriene	Adriene Holman, Heidi L (HEIDIH)
	Afton	Afton Galarza Rosario, Nydia R (NYGALARZ)
	Ai	Ai Boxer
	Aida	Aida Pullano
	Ailene	Ailene Benafield
	Aja	Aja Galligan, John W (JOGALLIG)
	Alan	Alan Haniuk, Kathryn L (KATHAN)
	Alana	Alana Kinkade
	Alejandro	Alejandro Hilliard, Michael R (MIHIL)
	Alessandra	Alessandra Garlington
	Ali	Ali Vivo
	Alicia	Alicia Trybala

End of Document