

Data Masking

Quick Start with DBSync Replication Data Masking

Whenever there is a need to copy the data from one Salesforce account to another, the user might want to mask the data for specific objects to safeguard the sensitive information.

With this feature, the user can mask the necessary objects before copying the data to another. Use DBSync Replication with source app Salesforce to connect a database.

(Note: Source App includes only Salesforce CRM Application)

The DBSync replication is offering you to connect the source app like Salesforce with different databases like MySQL, SQL Server, Oracle, DB2, PostgreSQL, Cassandra, Redshift, Sybase, Snowflakes, and MongoDB.

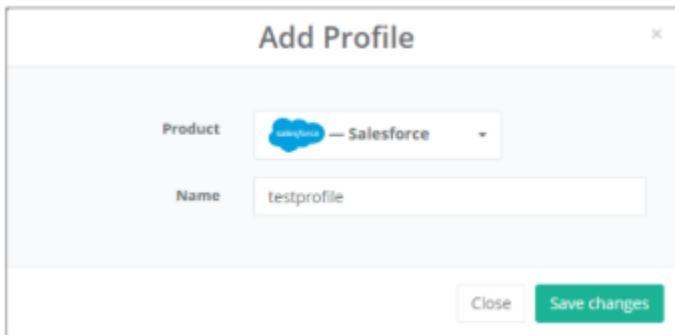
Log in to the DBSync replication portal

Sign in to the [DBSync Replication portal](#).

Steps to Follow

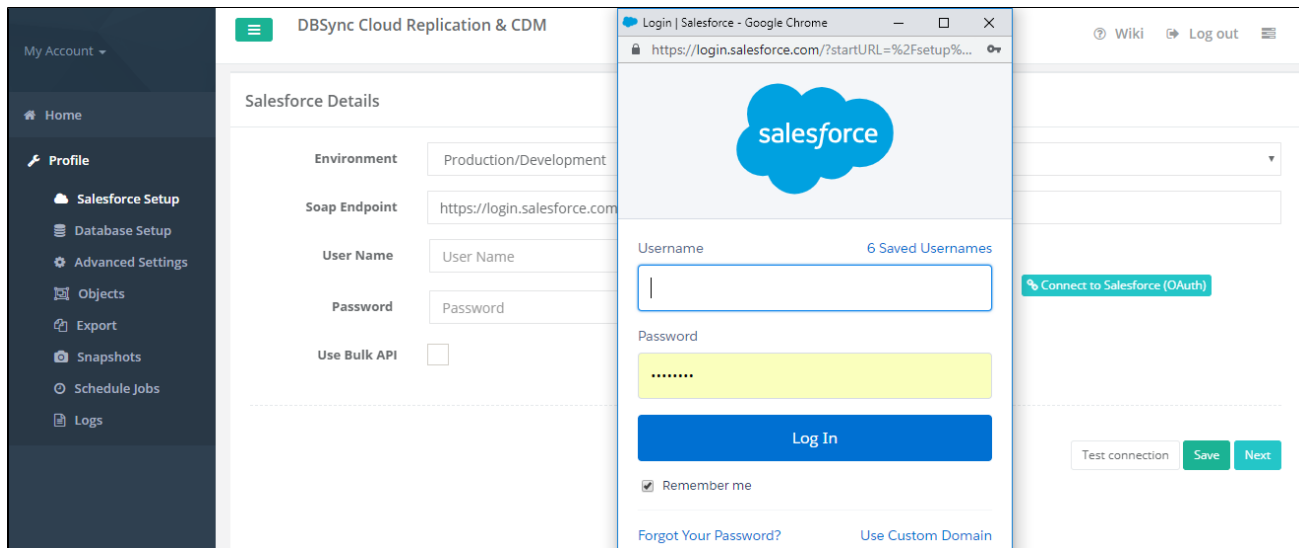
Here are some steps that you have to follow to start the Data Masking. Once you have a login to the DBSync replication portal you have to follow these below steps.

1. Click to "**add profile**" in the right-hand corner of the profiles section of the DBSync replication portal.
2. Select, the required **source name application** from the **drop-down menu** under the **product header**.
3. Next, **enter the name of the profile** like "test profile" under the name section.
4. **Click on save changes button to create a new replication profile.**

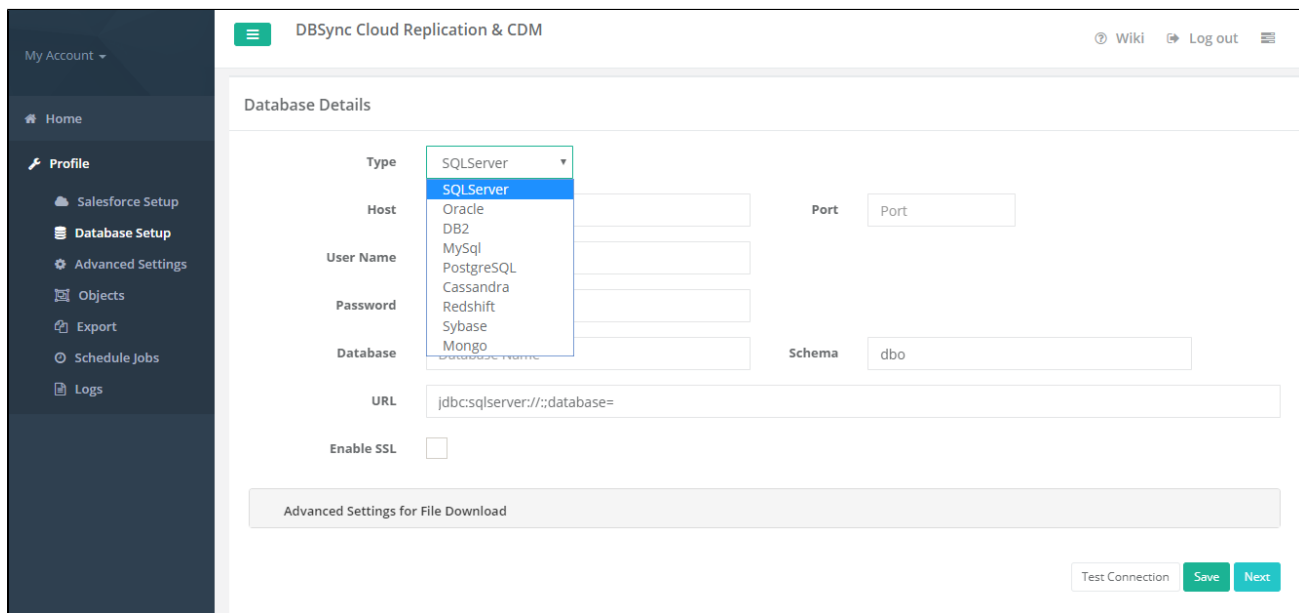


The screenshot shows a modal window titled "Add Profile". Inside, there is a "Product" label followed by a dropdown menu currently displaying "Salesforce". Below this is a "Name" label followed by a text input field containing the text "testprofile". At the bottom right of the modal, there are two buttons: a "Close" button and a green "Save changes" button.

5. Click to "**Salesforce setup tab**" on the left-hand corner in the profiles section of the DBSync Replication portal.
6. Don't change the "**environment and soap end details**", all these details are pre-filled.
7. Next, enter the "**username**" and "**password**" **credentials for Salesforce**.



8. Once completed, click on the next button to proceed to the database setup tab.
9. Click to "database" setup tab on the left-hand corner in the profiles section of the DBSync replication portal.
10. Select, the required "type name" from the drop-down menu options like "MySQL, SQL Server, Oracle, DB, PostgreSQL, Cassandra, Redshift, Sybase, Snowflakes, AWS S3 and MongoDB" under the "database setup" section.
11. To start with database credentials user has to enter all the configuration details like **host, port, username, password, database name, and schema**.



12. Once, this is done click on the save button and test the connection.
13. Click on the **next button** to redirect to the object page, their user has to select the particular **Object** which he/she wants to do the **Data Masking**.
14. Once, you have selected the **Object- Account** then click on the **Run button** to select any **command like Cleancopy** and wait for the sync.
15. Once, the **Sync is complete** then the user has to go back to **Export Tab**, select the **Object** from the **Schema** and click on the run **button** and select the column in which you want to change.
16. After the selection of the column **click on the Add Data Mask button**.

Account

Search Column...

Mask Enabled	Column	Mask Type
☐ OFF	AccountNumber : VARCHAR	None
☐ OFF	AccountSource : VARCHAR	None
☐ OFF	Active__c : VARCHAR	None
☐ OFF	AnnualRevenue : DECIMAL	None
☐ OFF	asxscftusar__c : VARCHAR	None
☐ OFF	AVSFNS__NS_Entity_Id__c : VARCHAR	None

Showing 1 to 72 of 72 entries

Previous1Next

Show100entries

Close

Save changes

17. As you can see on the above image **Account object** is showing on the **top left corner** and other options like **Mask Enabled (Toggle buttons)**, **Column**, and **Mask Type**.
18. **Enabled** mask for any field like **Phone** and select the **Mask Type** from the list. See the below image for the reference.

Account

phone

Mask Enabled	Column	Mask Type
☒ ON	Phone : VARCHAR	None Date/Time Mask (1900-01-01 00:00:00) Phone Mask (XXXXX12345) Email Mask (axxb.pxxq@gxxl.com) Default Mask (ABCD1234) Random Mask (vchkj45632) Credit Card Mask (XXXXXXXXXXXX1234)

Showing 1 to 1 of 1 entries (filtered from 72 total entries)

previous1Next

Show100entries

Close

Save changes

19. Here, I have selected the **Phone Column** and **enabled the mask**. On the right side, you will see the **drop-down menu** to select **the mask type**.
20. These are the six **Mask type** we support for data maskings like **Date/Time**, **Phone Mask**, **Email Mask**, **Default Mask**, **Rando Mask**, and **Credit Card Mask**.
21. After the selection of a **Phone mask from the mask type** then click on the **Save changes** button.

Data Masking

Account ▼

phone

Mask Enabled	Column	Mask Type
ON ☐	Phone : VARCHAR	Phone Mask (XXXXX12345) ▼

Showing 1 to 1 of 1 entries (filtered from 72 total entries)

Show 100 ▼ entries

Previous

1

Next

Close

Save changes

- After the changes click on the **Export Tab** to move further.
- Once you have clicked on the export button it will pop-up a **Source Metadata window**. Select the Object - **Account** and click on the **Next** button.
- It will redirect to the **Target Profile pop-up**, their user has to select the **existing profile or create a profile section** in which the user has to give the **target Salesforce credentials**.
- Once it is connected with the **Target Salesforce** then click on next to validate the data and finish the export task.
- In the final step, you have to go back to your **Target Salesforce** and check in the **Account section** all the **phone numbers** have mentioned in the **records** were **masked by the Data Masking** functionality. Check the below **image** for your reference.

Recent Accounts			New	Recently Created ▼
Account Name	Billing City	Phone		
MONGO DBSSS 12		XXXXX42206		
John SNOW SFDBZZZZZ		555555		
SFS3QRCL12DBSSSSS				
MONGO DBSSS 12		XXXXX42206		
John SNOW SFDBZZZZZ		555555		
United Oil & Gas UK V		+XX XXX XX56203		
test07				

- As you can see on the above image **first 5 digits** have been masked and the **last 5 digits** are visible only. This means data was **masked successfully**.