DESelect

DESelect - Security Documentation

v1.2.0 - April 15th, 2020

DESelect

1. High-level architecture

DESelect is installed as an Installed Package inside your Salesforce Marketing Cloud instance. This Installed Package has 2 components:

1.1. Marketing Cloud App

The Marketing Cloud App component allows us to show an iFrame within Salesforce Marketing Cloud. This way we can provide additional functionality to marketers within the platform. The Marketing Cloud App is available for users by clicking 'AppExchange > DESelect'.

1.2. API Integration

The DESelect UI provided in the iFrame connects to the DESelect servers, on which a combination of custom logic and calls to the Salesforce Marketing Cloud provide the functionality to support the front end.

During the setup of the API integration, a scope needs to be defined. The scope determines what DESelect is allowed to do through the API. The scope required for DESelect is minimal, with only the following permissions:

1.2.1. Offline Access: 60 days

DESelect needs to be able to:

- Follow up on the progress of SQL queries (query activities) a user has started, even if the user has signed off
- Start a new query to count the number of results of an SQL query a user has started, even if the user has signed off

1.2.2. Automations: Read, Write, Execute

DESelect needs to be able to:

- Create and update SQL queries
- Schedule executions of selections

1.2.3. Journeys: Read, Write, Execute

Required for features planned to be released in the near future.

1.2.4. Data Extensions: Read, Write

DESelect needs to be able to:

- Show a list of all data extensions
- Get the fields of a data extension
- Create new data extensions to write results of SQL queries to
- Write the results of a query to a data extension

1.2.5. Access to the DESelect Installed Package

Any Salesforce Marketing Cloud administrator can manage the licenses for the DESelect installed package. Access can be granted per individual user and per business unit and can be revoked at any time.

2. Folders

DESelect needs a few folders to store the data extensions and query activities DESelect generates.

2.1. Data Extensions folder

Under Data Extensions, DESelect creates a folder called *DESelect*, which contains the data extensions created to write the preview results to.
This folder may not be deleted.

2.2. Query Activities folder

DESelect creates a folder called *DESelect* under Query Activities → All SQL Query → Query.
This folder has 2 subfolders: *Selections* and *System*.
Selections contain the SQL queries DESelect creates, with one query activity for each selection in DESelect. These query activities can be used in automations.
System contains other query activities necessary to generate the previews and count the number of records in the preview and the final query. These query activities should not be used directly by users.
None of these folders may be deleted.

2.3. Automations folder

Under Automations, DESelect creates a folder called *DESelect*, which contains the automations created to deduplicate results.
This folder may not be deleted.

3. Security Measures

The following security measures are in place in DESelect to assure the safety of your data:

3.1. HTTPS / SSL

All communication between the Salesforce Marketing Cloud App and the DESelect API, as well as the communication between the DESelect backend and the Salesforce Marketing Cloud API, happens over HTTPS with an SSL certificate. This means nobody can intercept or modify any messages sent.

3.2. Secure API Endpoints

The DESelect API endpoints are only accessible for logged in users of the DESelect Marketing Cloud App. Our endpoints are secured by both HTTP headers and a session token.

3.3. Authenticated Users

When users perform actions in DESelect, they do so in their own name. That way you maintain full visibility and accountability on the data processing by users. For example, when a user creates a new Data Extension in DESelect, the 'Created By' of this Data Extension will show the user's name.

Authentication happens through oAuth2, which is the industry standard safe way of authentication without sharing any passwords with DESelect and also a Salesforce best practice when building packages for Salesforce Marketing Cloud.

Note that DESelect can only be used by a Salesforce Marketing Cloud user when (s)he is logged in. When the user logs out of Salesforce Marketing Cloud, (s)he is logged out of DESelect as well.

3.4. Safe Hardware

DESelect runs on servers of DigitalOcean, a market leader in infrastructure as a service, with an additional security layer by Cloudflare, which protects it from attacks.
Our servers are in secure data centers in Amsterdam, managed by DigitalOcean, with ISO-27001:2013, SOC I and II, and PSI-DSS certifications.

4. Data Protection

4.1. Metadata Processing

DESelect stores the following metadata:

- Some details about your Salesforce Marketing Cloud instance and the installed package, necessary to authenticate users
- Name, username, and email of every Salesforce Marketing Cloud user that uses DESelect. This information is updated automatically every time a user opens DESelect.
- Metadata about the selections a user creates in DESelect

4.2. Data Processing

4.2.1. How DESelect processes data

Note that DESelect does not store any of your data on its own databases.

When building a selection, DESelect pulls in the metadata of your data extensions. This means DESelect only looks at the fields available in the data extensions, not the data. DESelect only needs to know which fields exist in each data extension, and what the details of those fields are (eg. length of a text field).

The only point in the application where DESelect accesses data in data extensions is when rendering the preview. Here 20 records are queried from the target data extension after the query has run, so a preview of the results can be shown to the user. This preview data is presented in the UI and not stored on the DESelect servers.

The data access level for DESelect is limited to the permissions defined in section 1.2. Concretely, this means DESelect can only query data extensions, query activities and automations.
Furthermore, access is limited to the visibility of each user. A user cannot access more data in DESelect than he has access to in Marketing Cloud directly. Within DESelect all actions are taken as a user, so DESelect could never access data a user cannot access.

For every Marketing Cloud user that opens DESelect, a user record is created in the DESelect database to identify the user, so a user can be an owner of a selection. This user record contains the

username and name of each user.
Note: this paragraph is about SFMC users, not Subscribers or Contacts. DESelect does not copy any Subscriber/Contact data.

4.2.1. Subprocessors

Currently, DESelect does not have any subprocessors.

DESelect informs customers about changes in subprocessors via email 30 days before the agreement with the new subprocessor goes into effect.

4.3. Termination of Contract

Unless agreed otherwise, the following policy applies in case of termination of the customer contract for DESelect:

- The metadata stored for the customer will be maintained for 60 days, in case the customer changes his mind.
- After 60 days, all (meta)data is deleted.

DESelect

Made with ♥ for salesforce marketing cloud

5. Contact

For any other questions regarding the security of DESelect, please reach out to our product team at privacy@deselect.io.