DESelect Search
Security Fact Sheet

v1.1 - February 25th, 2022

About this document

At DESelect, we place a high value on security. Trust is one of our core values.

This document aims to provide a high-level overview of the different security aspects and inner workings of the DESelect Search application.

More details can be found on our **website** or our **Security Portal**.

1. Functionality / Architecture Overview

DESelect Search provides a UI that is rendered in an iFrame in Marketing Cloud.

This UI consists of a search bar, where users indicate the type of object he's searching for and the search term.

Upon submitting this form, an Api call is made to the DESelect servers, which make an API call to Marketing Cloud, handle the responses properly, and return the results in a formatted way back to the front end so the search results can be shown to the user.
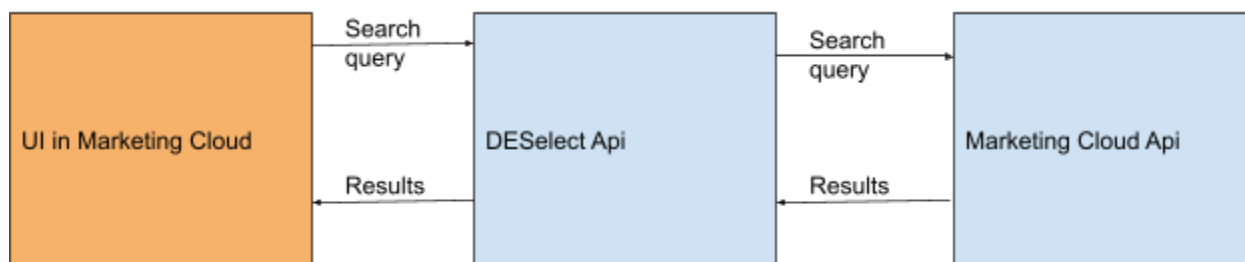
2. High-level architecture

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

2.1. 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 Search*.

When a user clicks on the DESelect Search item under AppExchange in the Marketing Cloud menu, the oAuth2 authentication process starts, as documented on top of the **DESelect Search Architecture diagram**. Once the user is authenticated, the frontend of the DESelect Search application is rendered within an iFrame, and all interactions of DESelect Search with Marketing Cloud happen through the Marketing Cloud APIs. When a user switches to another Marketing Cloud application, the logout flow is triggered (as documented on the

bottom of the **DESelect Search Architecture diagram**) and the user's session with DESelect Search is terminated.

2.2.   API Integration

The DESelect Search 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 Search is allowed to do through the API. The scope required for DESelect Search is minimal, with only the permissions listed below. Note that the installed package already comes with these permissions, you don't need to take any additional steps.

For this installed package to work, we just need Read permissions on the objects users want to search for. The permissions scope for this Installed Package is:
- Email: Read
- Documents and Images: Read
- Saved Content: Read
- Automations: Read
- Journeys: Read
- Data Extensions: Read

2.3.   Access to the DESelect Search Installed Package

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

3. User permissions

DESelect Search is limited to Make sure Marketing Cloud users' permissions. For example, if a user does not have access to view automations, (s)he won't be able to search for automations using DESelect Search.

4. Security Measures

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

4.1. HTTPS / SSL

All communication between the Salesforce Marketing Cloud App and the DESelect Search API, as well as the communication between the DESelect Search backend and the Salesforce Marketing Cloud API, happens over HTTPS through TLS 1.3. This means nobody can intercept or modify any messages sent.

4.2. Secure API Endpoints

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

4.3. Authenticated Users

When users perform actions in DESelect Search, 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 Search, 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 Search and also a Salesforce best practice when building packages for Salesforce Marketing Cloud. More details on this authentication flow can be found **here**.

4.3.1. How session tokens and refresh tokens work

When a user opens DESelect Search in Marketing Cloud, authentication happens through oAuth2, and DESelect Search is provided with a session token and a refresh token. This

session token allows DESelect Search to make API calls to Salesforce Marketing Cloud in the name of the user. This session token has a scope limited to the permissions defined in the Installed Package as described in section 1.2 of this document. This session token has a limited lifetime of 20 minutes. With the refresh token that was provided upon authentication, a new session token is requested with SFMC before the old one expires. Both access and refresh tokens are stored encrypted on DESelect Search servers.

When the user logs out of Salesforce Marketing Cloud, or switches to another studio inside of SFMC, (s)he is logged out of DESelect Search, and the session token and refresh token become invalid.

When a user just closes his/her browser, the tokens remain valid until they expire. So for the session token this is after 20 minutes, for the refresh token this is after the period described in the next section of this document.

Note that DESelect Search can only be used by a Salesforce Marketing Cloud user when (s)he is logged in.

4.4.   Safe Hardware

DESelect Search 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 and Frankfurt, managed by DigitalOcean, with ISO-27001:2013, SOC I and II, and PSI-DSS **certifications**. A DPA is in place between DESelect Search and DigitalOcean and they are GDPR compliant.

4.5.   Security Review

DESelect Search has passed the Salesforce Security Review, which is a prerequisite to be listed on the AppExchange. This means a thorough assessment of the security of the application has been done. Besides the initial assessment, Salesforce performs additional checks at random intervals.

Next to Salesforce, DESelect Search also performs penetration tests on a regular basis.

5. Data Protection

5.1. Processing of data

DESelect Search 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 Search.

DESelect does not access any other of your Salesforce Marketing Cloud data. It just passes along a request to the Salesforce Marketing Cloud api, which allows for searching in a different way than in the UI. For example: if a user searches for a data extension with a certain name, DESelect just passes along the search term to Marketing Cloud, and retrieves a list of matching data extensions which are shown to the user. DESelect Search is not able to look at the content of these data extensions.

5.2. Subprocessors

DESelect Search has one subprocessor, **DigitalOcean**, which hosts the application.

NAME	COMPANY BUSINESS REG. NO.	ADDRESS AND LOCATION OF THE PERSONAL DATA	DESCRIPTION OF PROCESSING
DigitalOcean LLC	101 Avenue of the Americas 10th Floor New York, NY 10013, United States	DigitalOcean datacenter AMS3, Science Park 610, 1098 XH Amsterdam, The Netherlands	Contains database of the application with user details and selection metadata.

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

5.3. Termination of Contract

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

- 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.

6. SLA's
- Uptime: 99.5%

7. Further Reading

For more information check out **the Security Portal**, which explains all aspects of the DESelect organisation security in detail.

8. Contact

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