# DESelect Segment Security Fact Sheet

v2.0 - July 27th, 2023

# About this document

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

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

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

# 1. High-level architecture

DESelect Segment is installed through 2 Installed Packages inside your Salesforce Marketing Cloud instance. The details of these Installed Packages will be explained in the next 2 sections.

For a detailed understanding of how DESelect Segment works together with Marketing Cloud to deliver its functionalities, please check **this DESelect Segment Segmentation Architecture diagram**.

# 2. Installed Package: DESelect Segment

## 1. Architecture Overview

For a detailed understanding of how DESelect Segment works together with Marketing Cloud to deliver its functionalities, please check **this DESelect Segment Segmentation Architecture diagram**.

## 2. Components

This Installed Package has 2 components:

### 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 Segment*.

When a user clicks on the DESelect Segment item under AppExchange in the Marketing Cloud menu, the oAuth2 authentication process starts, as documented on top of the **DESelect Segment Architecture diagram**. Once the user is authenticated, the frontend of the DESelect Segment application is rendered within an iFrame, and all interactions of DESelect Segment 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 Segment Architecture diagram**) and the user's session with DESelect Segment is terminated.

## API Integration

The DESelect Segment UI provided in the iFrame connects to the DESelect Segment 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 Segment is allowed to do through the API. The scope required for DESelect Segment 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.

**Offline Access: 60 days**

DESelect Segment 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 deduplication query, even if the user has signed off

This offline access is possible through this setting in the Installed Package that keeps the users' refresh token valid for 60 days. We're working on changing this setting in the future so this offline access is limited to a few hours.
For more information on how this Offline Access works and how the 60 days can be reduced, please see section 6.3.2.

**Automations: Read, Write, Execute**

DESelect Segment needs to be able to:

- Create and update SQL queries
- Schedule executions of selections

**Journeys: Read, Write, Execute, Activate/Stop/Pause/Resume/Send/Schedule, Delete**

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

**Data Extensions: Read, Write**

DESelect Segment 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

## 3. Access to the DESelect Segment Installed Package

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

# 3. Installed Package: DESelect Automations

### What is it?

DESelect has an additional Installed Package called DESelect Automations. This package has been security reviewed by Salesforce and uses **Server-to-Server authentication** which allows DESelect Segment to use the SFMC api outside of a user's context.

The DESelect Automations installed package will enable the following features:
- Scheduled selections and scheduled waterfall selections: allows users to schedule the execution of a selection at a certain time in the future, or set a selection to be executed on a recurring schedule.
- Picklist auto-refresh: checks the values available for a field in a data extension and updates the picklist values definition based on this.

### Installation

It's highly recommended that the installation of DESelect Automations is handled by us during the installation of DESelect Segment. The scope of this installed package is the same as the api permisions explained in section 2 of this document.

### Access to the installed package

Any Salesforce Marketing Cloud administrator can manage the licenses for the DESelect Automations S2S installed package. Since this application is not visible to end users, access is not granted on a user level, but on a business unit level. Within this package, the business units needs to be enabled in which DESelect Segment is being used.

# 4. User permissions

Please check the **Salesforce Marketing Cloud required user permissions** article on the DESelect Segment support portal for more information on the permissions required for Salesforce Marketing Cloud users to use DESelect Segment.

# 5. Folders

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

## 5.1. Data Extensions folder

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

## 5.2. Query Activities folder

DESelect Segment 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 Segment creates, with one query activity for each selection in DESelect Segment. 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.

# 6. Security Measures

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

## 6.1. HTTPS / SSL

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

## 6.2. Secure API Endpoints

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

## 6.3. Authenticated Users

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

### 6.3.1. How session tokens and refresh tokens work

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

session token allows DESelect Segment 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 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 Segment 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 Segment, 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 Segment can only be used by a Salesforce Marketing Cloud user when (s)he is logged in.

### 6.3.2. Considerations regarding the refresh token lifetime

**Changing the refresh token lifetime**

In the permissions of the standard DESelect Segment installed package, there is a permission called *Offline Access*, which by default is set to 60 days. This means that the refresh token described above remains valid for 60 days after the user has logged out of DESelect Segment.

DESelect Segment needs this to be able to complete certain tasks that may be ongoing after the user has left the application. For example, when a user clicks on the Run button to run a selection, and then leaves DESelect Segment, the application needs to be able to continue following up on the completion of the query until it has completed.

Originally, this refresh token lifetime has been set to 60 days, so DESelect Segment can handle multiple tasks while users are offline, like auto-refreshing picklist values.

Companies who are not comfortable with a refresh token lifespan of 60 days can opt to have a custom DESelect Segment Installed Package, which allows us to modify the refresh token lifetime.

The refresh token lifetime can be reduced to 2 hours. A minimum of 2 hours is required to make sure that complex selections that use prio deduplication can be completed (deduplication requires 2 queries to run).

## 6.4. Safe Hardware

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

## 6.5. Security Review

DESelect Segment 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 Segment also performs penetration tests on a regular basis.

# 7. Data Protection

## 7.1. Metadata Processing

DESelect Segment 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 Segment. This information is updated automatically every time a user opens DESelect Segment.
- Metadata about the selections a user creates in DESelect Segment.

## 7.2. Data Processing

### 7.2.1. How DESelect Segment processes data

Note that DESelect Segment does not store any of your data on its own databases. That means we are rather “lightweight” from a data processing point of view, as we do not store your actual customer data.

When building a selection, DESelect Segment pulls in the metadata of your data extensions. This means DESelect Segment only looks at the fields available in the data extensions, not the data. DESelect Segment 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 Segment 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 Segment servers.

The data access level for DESelect Segment is limited to the permissions defined in section 2. Concretely, this means DESelect Segment 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 Segment than he has access to in Marketing Cloud directly. Within DESelect Segment all actions are taken as a user, so DESelect Segment could never access data a user cannot access.

For every Marketing Cloud user that opens DESelect Segment, a user record is created in the DESelect Segment 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 Segment does not copy any Subscriber/Contact data.

### 7.2.2. Subprocessors

DESelect Segment 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. |
| OpenAI OpCo, LLC | 180 18th Street, San Francisco, CA, United States | United States | Enabling AI capabilities for selection creation. |

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

## 7.3. Termination of Contract

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

- 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.

## 8. SLA's

- Uptime: 99.5%
- RPO (Recovery Point Objective) for the service is set to 1 hour: we make hourly backups of the production database so we'll never lose more than 1 hour of work.
- RTO (Recovery Time Objective) is set to 24 hours: we can roll back to a data backup within 24 hours of an incident

## 9. Further Reading

For more information, check out our security page, which explains all aspects of the DESelect Segment security in detail.

## 10. Contact

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