DESelect Engage
Security Fact Sheet

v1.0 - 14 Jun 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 Engage platform.

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

1. High-level architecture

DESelect Engage 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.

DESelect Engage

This Installed Package contains the following elements:

API integration of type Web App

This allows for oAuth2 authentication when users open the DESelect Engage Marketing Cloud app, so that API calls to SFMC can be made during the active user session given the scope of the permissions.

The standard oAuth2 flow provided by SFMC is implemented here. More info on how this works in detail can be found here.

The scope contains the following permissions:

- Data Extensions: Read, Write
- Automations: Read, Write, Execute

Marketing Cloud App

This is the UI that is shown inside an iFrame as a Marketing Cloud app available under the AppExchange menu. This is the app users use to plan and prioritize campaigns, and define the saturation control rules DESelect Engage needs to enforce.

Access to this app is managed by SFMC admins in SFMC on the Access tab of the Installed Package.

Journey Builder custom activity

This is a custom Journey Builder activity of type Flow Control that marketers can add to their journeys to make sending decisions based on the saturation levels of recipients.

Access to this Journey Builder custom activity is managed by SFMC admins in SFMC on the Access tab of the Installed Package.

DESelect Engage S2S

API integration of type Server-to-Server

This allows for connecting to SFMC without an active user session, which is required for all scheduled processing, e.g. starting an automation.

More info on the access tokens in a server-to-server authorization flow here.

The scope contains the following permissions:

- Automations: Read, Write, Execute
- Journeys: Read, Write
- Data Extensions: Read, Write
- File Locations: Read, Write

2. Security Measures

Data view / data extension ingestion

To ingest data from SFMC into DESelect Engage, automations are used that retrieve only the required columns from the data views / data extensions and prepare a CSV. This CSV is then compressed, encrypted and file transferred using the native and secure Google Cloud Platform file transfer feature in SFMC.
Upon ingestion into the DESelect Engage databases, fields that may contain PII, like the contact key, are stored encrypted.

Only campaigns for which the audience and the send date are known need to be extracted. Concretely, this would be campaigns sent out through a journey for which the entry source is a data extension. In case of multiple sends within one campaign, only the first data extension needs to be ingested, if the timing or audience of the following sends can be changed in the journey.

For more information on which data is being ingested, see section 'Data ingestion' of this document.

Encryption

Encryption of data at rest

All systems processing or storing data are equipped with disk level encryption. Next to this, all personal or sensitive data is encrypted at application level using AES-192 (this includes the database).

Encryption of data in transit

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

Trusted cloud computing provider

For hosting of the database and business logic, DESelect Engage works with Google Cloud Platform, which has SOC 2 compliance (and much more). The cloud environment for Engage is fully segregated from DESelect's office network and other products. Access to the environment is strictly restricted to authorized personnel.

Secure API endpoints

The DESelect Engage API endpoints for the Marketing Cloud app are only accessible for logged-in users of the DESelect Engage Marketing Cloud App, and the API endpoint for the Journey Builder endpoint verifies that the call is actually made from the right SFMC environment.
All endpoints are secured by both HTTP headers and a JWT token.

ISO-27001 certification

DESelect as an organization is ISO-27001 certified, which means an external auditing institution has confirmed DESelect implements a set of security best practices. This includes having a dedicated security officer, applying the principle of security by design and development and release management best practices.

Penetration testing

DESelect works with Intigriti to host continuously ongoing bug bounty campaigns on its products. DESelect Engage will be subjected to ongoing security reviews (by internal personnel) and to penetration testing (by an independent external party).

Salesforce security review

DESelect Engage is subject to the Salesforce Security Review, which is a prerequisite to be listed on the App Exchange. This means a thorough assessment of the security of the application is being done. Besides the initial assessment, Salesforce performs additional checks at random intervals. Next to Salesforce, DESelect Engage also performs penetration tests on a regular basis.

3. Data ingestion

The following data is ingested from SFMC into the DESelect Engage platform:

Data View: _Sent

Contains information about emails sent through SFMC.

Field	Description	Encrypted
SubscriberKey	Identifier of a contact	yes
Date	Datetime when the email sent took place	

Data View: _SMSMessageTracking

Contains information about text messages sent through SFMC.

Field	Description	Encrypted
SubscriberKey	Identifier of a contact	yes
ActionDateTime	Datetime when the email sent took place	

Data View: _Job

Contains information about sending Jobs in SFMC.

Field	Description	Encrypted
JobID	Identifier of the job	yes
AccountID	Business Unit Id	
TriggererSendDefinitionObjectID	Link to the journey element responsible for the sending	

MobilePush Report

Contains information about mobile push messages sent through SFMC.

Field	Description	Encrypted
ContactKey	Identifier of a contact	yes
DateTimeSend	Datetime when the email sent took place	

While we only ingest the data listed in the table above, please note that when creating the MobilePush Extract in Automation Studio, the report contains the following fields: *AppName, MessageName, MessageID, Campaigns, DeviceId, DateTimeSend, MessageContent, MessageOpened, OpenDate, TimeInApp, Platform, PlatformVersion, Status, ServiceResponse, GeofenceName, Template, Format, PageName, PushJobId, SystemToken, InboxMessageDownloaded, InboxMessageOpened, IosMediaUrl, AndroidMediaUrl, MediaAlt, ContactKey, RequestId.* These all contain system information, though a field like the MessageName or MessageContent could contain personal information.

Unfortunately there is no way in Marketing Cloud to have the report only contain the fields we need. We do copy this report file to our servers where we process only the columns listed in the table above, and then delete the report file.

Campaign Members Data Extensions

One Data Extension per planned campaign, containing the audience that will receive the campaign.

Field	Description	Encrypted
SubscriberKey	Identifier of a contact	yes

All Contacts Data Extension

One Data Extension per Business Unit, containing all the contacts for which DESelect Engage needs to manage saturation control. Each contact can have one or multiple Contact Categories. In case of multiple Contact Categories, the contact will have multiple rows.

Field	**Description**	**Encrypted**
SubscriberKey	Identifier of a contact	yes
ContactCategory	Name of the Contact Category a Contact belongs too.	

4. Compliance

DESelect Engage is GDPR-compliant. Some examples:

- Any data that can potentially be PII is encrypted
- Data stored is limited in both scope and duration to what's strictly necessary
- Functionality to remove a contact from any table to conform with removal requests

5. SLA's

- Uptime: 99.5%
- RPO (Recovery Point Objective) for the service is set to 1 hour: we make hourly backups of the production databases 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
- Security or privacy breach notification is set to 24 hours: we are committed to inform our customers within 24 hours of identifying an incident.

6. Contact

For any other questions regarding the security or architecture of DESelect Engage, please reach out to our head of engineering at **security@deselect.com**