Field-Level Encryption and Encrypted Data Sending Implementation Guide

Salesforce, Spring ’24

@salesforcedocs

Last updated: November 9, 2023

CONTENTS

FIELD-LEVEL ENCRYPTION IMPLEMENTATION GUIDE

Field-Level Encryption stores encrypted data at rest in a data extension. You can mark text or email-address fields in a data extension as encrypted. This feature allows you to store sensitive data in Marketing Cloud databases using an encrypted format. Data shown in Marketing Cloud's user interface is shown as encrypted data, even to Marketing Cloud users. Marketing Cloud decrypts the data only at send time for use in email message– and landing-page personalization.

Who This Guide Is For

This guide is for Marketing Cloud admins, partners, and developers to implement Field-Level Encryption and Encrypted Data Sending and to configure specific features.

Before You Start

Field-Level Encryption must be enabled for your account. Field-Level Encryption is available only for new accounts, and it functions with any account type. This feature requires a subscriber key value for each contact. You can use Field-Level Encryption with data encrypted at rest. Field-Level Encryption works only with text and email-address fields.

Field-Level Encryption doesn't function with:

- Data obfuscation
- Data masking
- Tokenized Sending
- SMS messages
- Push messages
- List-based sending
- Data added or updated in a customer profile center
- Audience Builder segments, filters, and queries

Set Up Field-Level Encryption

Review this information and follow these steps to set up Field-Level Encryption in your Marketing Cloud account.

Field-Level Encryption Data Imports

With Field-Level Encryption turned on, import data into the Marketing Cloud using one of these methods:

Method	Option
Imports	None
API Call	CreateRow
	UpdateRow

Method	Option
Triggered Send	None
Data Extension AMPscript Functions	Lookup
	InsertDE
	UpsertDE

You can also input data directly into the data extension by adding individual records. This method encrypts data as well. The Marketing Cloud builds a message using encrypted data, then converts that data to plain text using a symmetric key at send time. The system then sends the message from our mail transfer agent (MTA). The Marketing Cloud stores all tracking and deliverability information as identified by the corresponding subscriber key values.

Field-Level Encryption Data Exports

With Field-Level Encryption turned on, export data from the Marketing Cloud using one of these methods:

- FTP export of a data extension from Contact Builder
- File download of a data extension via browser from Contact Builder
- Extract via Interactions - this method exports data as encrypted data only
- API retrieval of a data extension

Encryption Configuration Options

When enabling Field-Level Encryption in Marketing Cloud Security and Encryption products, you can encrypt and import data into your Marketing Cloud account. You can also import plain text into your Marketing Cloud account and encrypt the data as part of the import process. You can also choose the method to display the data, which is also encrypted by default.

Choose one of these options when enabling Field-Level Encryption for your account:

- You can encrypt your data yourself and import it into your Marketing Cloud. Any extracted or exported data remains in the same encrypted format used before the import process.
- You import plain text data into your Marketing Cloud account. Marketing Cloud encrypts that data as part of the import process. Marketing Cloud then decrypts any extracted or exported data. Marketing Cloud exports any data using a data extension export to an FTP location as unencrypted data.
- You choose to display data in Preview, landing pages, View as Webpage, Forward to a Friend, platform apps, and Send Logging in unencrypted text. By default, the Marketing Cloud encrypts this data.

Implement Field-Level Encryption

Follow these steps to implement Field-Level Encryption in your Marketing Cloud account.

To enable Field-Level Encryption for your new Marketing Cloud account, contact your Marketing Cloud account representative or Partner Success Services. Implementation for this feature requires the purchase and completion of a Marketing Cloud Services engagement before performing any configuration in your Marketing Cloud account. Ensure that you understand the prerequisites and account changes for this product before proceeding. Log in to your Marketing Cloud account as an administrative user to perform this implementation.

1. Open **Key Management** under Data Management in the Setup section of your account.

2. To create a symmetric key, provide the required information. Generate the key value for the pre-shared key field using a cryptographically secure random number generator. Marketing Cloud supports AES 256 encryption. Use a 64-character hexadecimal string for the key. Your internal team can provide information for obtaining the key.
3. Save your key and return to the Key Management page.
4. To create an initialization vector (IV), provide the required information. Use a 32-character hexadecimal string for the IV value.
5. Save your IV.

After you use this key value to encrypt data, you can't change the key value. After the Services engagement for this feature completes, you can mark fields in a data extension for encryption. In Contact Builder, a checkbox that enables encryption appears next to text and email address data extension fields.

Salesforce Shield and Field-Level Encryption Compatibility

You can use Salesforce Shield and Field-Level Encryption with Sales and Service Clouds.

- Event Monitoring
- Audit Trail
- Platform Encryption

The Marketing Cloud does not offer Audit Trail or Event Monitoring via the Marketing Cloud app. However, Field-Level Encryption does encrypt data at rest and can support Platform Encryption users. The Marketing Cloud can import data automatically from the Sales and Service Clouds using the Marketing Cloud Connector. This process decrypts the data from these clouds and transmits that data over a secure communication channel to Marketing Cloud. As the data arrives in Marketing Cloud, those fields are encrypted use Field-Level Encryption. The connector establishes a relationship between a Salesforce org and a Marketing Cloud account.

You can accomplish this process using one of the following four methods.

Synchronized Data Sources

Synchronized Data Sources supports Platform Encryption. This feature synchronizes data from your Salesforce org at specified time intervals, including data schema and relationships previously established in your Salesforce CRM account. The Marketing Cloud encrypts fields identified as encrypted using Platform Encryption. An enabled user views encrypted data in the Sales or Service Cloud. They can also select fields for synchronization in the Marketing Cloud, which imports and stores this data in Synchronized Data Extensions. The Marketing Cloud re-encrypts this data using the Field-Level Encryption symmetric key upon import.

Reports and Campaign Sends

Reports and Campaign Sends supports Platform Encryption. After installing the Marketing Cloud Connector, you can send to Reports and Campaigns directly from your Sales Cloud account. A Marketing Cloud account enabled with Field-Level Encryption encrypts data identified as encrypted from the Sales or Service Cloud.

Journey Builder Events

Journey Builder Events do not support Platform Encryption. The Marketing Cloud does not re-encrypt data imported via events. Journey Builder lets you create an entry event to power a journey based on Sales and Service Cloud data. Journey Builder then creates associated data extensions as it creates the entry events. The Marketing Cloud does not encrypt data taken from the Sales and Service Clouds as part of these entry events currently. You can use Journey Builder with Field-Level Encryption and implement Synchronized Data Extensions instead of data imports to maintain encryption.

Automation Studio Imports

Automation Studio imports do not support Platform Encryption. Automation Studio permits you to create an import activity that can import Sales and Service Cloud data into the Marketing Cloud. The Marketing Cloud does not encrypt this data once imported. You can synchronize encrypted Salesforce Objects data using Synchronized Data Extensions.

Field-Level Encryption Use Cases for Implementation and Testing

These use cases demonstrate effective processes to set up and test Field-Level Encryption in your Marketing Cloud account.

Create an Encryption Key

Create an encryption key in Marketing Cloud for use with Field-Level Encryption. This use cases places a symmetric key and IV value in your Marketing Cloud account.

This use cases requires the Marketing Cloud Admin role or the Key Admin permission in Data Management under Admin.

1. In Setup, click **Key Management**.
2. Select **Symmetric**.
3. Enter a name and external key value for your key.
4. Enter a 256-bit key value for your pre-shared key value. This value requires 64 hex characters.
5. Copy the 256-bit key value and enter the value again.
6. Click **Save**.
7. Click **Create**.
8. Select your initialization vector (IV) value. This value requires 32 hex characters.
9. Enter the IV value in the **IV** field.
10. Click **Save**.

Create a Data Extension with Encryption Fields

Create a data extension with encrypted fields in Marketing Cloud for use with Field-Level Encryption. Use this information to encrypt text and email address type fields.

This use case requires Field-Level Encryption enablement for your account. You must create an encryption key for this use case.

1. In Contact Builder, click **Data Extensions**.
2. Click **Create**.
3. Enter the information for your data extension, and click **Next**.
4. Implement your data retention policy, and click **Next**.
5. Add the fields to your data extension. For each field to encrypt, select **Encrypt Data**. This feature supports only text and email fields.
6. Click **Complete**.
7. Click **Import**.
8. Click **Create**.
9. Perform the steps to import data into your new data extension.

In Contact Builder, the data extension displays ciphertext for encrypted fields. The All Subscribers list shows an "Email_Unavailable_SubscriberID" format value for encrypted email addresses.

Field-Level Encryption Best Practices and Limitations

This information helps you understand Field-Level Encryption limitations and how to best manage your encrypted data.

Field-Level Encryption Limitations

These limitations apply when working with Field-Level Encryption in Marketing Cloud's Security and Encryption products.

Note: Implementation for this feature requires the purchase and completion of a Marketing Cloud Services engagement prior to performing any configuration in your Marketing Cloud account. This requirement includes the creation of any new business units. To enable Field-Level Encryption for your new Marketing Cloud account, contact your Marketing Cloud account representative or Partner Success Services.

- Use only data extensions created specifically for Field-Level Encryption with this feature.
- Configure Field-Level Encryption before configuring any data synchronization with Sales or Service Clouds.
- Field-Level Encryption doesn't support segmenting, filtering, or querying encrypted fields.
- Encrypted data appears encrypted on Discover and standard reports. The send-to domain appears as @exct.net.
- Field-Level Encryption doesn't support auto-suppression lists. Instead, create a list with only the subscriber key values to suppress and assign that list for use in your account.
- You can't add or update encrypted data via Marketing Cloud. Use imports, AMPscript, triggered sends, or API calls, or manually add records into a data extension using Contact Builder.
- Field-Level Encryption doesn't support encryption of a mobile number used as a subscriber key value.
- Field-Level Encryption doesn't support encryption for primary key fields or subscriber key values.
- You can use MobileConnect and MobilePush in accounts using Field-Level Encryption, but messages can't include any encrypted fields.
- You can't turn off Field-Level Encryption after you enable it.
- Field-Level Encryption doesn't support list-based sending.
- Accounts enabled for Field-Level Encryption don't support data filters. Use query activities instead.
- Use queries instead of data relationships with Field-Level Encryption. Data relationships don't support Field-Level Encryption.
- Encrypted fields don't support default values in data extensions.
- API-based triggered sends support encryption only for email addresses. Triggered sends can't decrypt non-email-address information and send the encrypted string instead.
- If you include the emailaddr personalization string in your email messages, any sendlog used contains the unencrypted email address.
- Field-Level Encryption doesn't support Marketing Cloud's Transactional Messaging API.