ReachFive

CIAM integration for salesforce commerce cloud SFRA storefronts

Version 20.4.0

Table of Contents

1. Summary

ReachFive is a CIAM (Customer Idendity and Access Management), providing social media and full authentication features.
With ReachFive, customers can simplify their authentication process and improve their customer identity management.
Currently, more than 30 social networks authentications are managed by ReachFive but the number of social networks supported is continuously growing.

As described in the ReachFive website (https://www.reach5.co/), ReachFive provide the following functionalities:
- Single Sign On: sets of API and widget to allow the user to signup, login, manage social account profiles
- Social Login: allows merchants to integrate OAuth providers registering and login functionalities, manage
social account profiles

This component integrates SFCC with the ReachFive platform.
Using this cartridge, merchants and solution partners do not need to do anything to integrate new providers when they become available in the ReachFive platform (except activating these new providers in the ReachFive back office, as everything related to the connection is managed by ReachFive).

Merchants willing to use this component to connect to the ReachFive platform will be required to subscribe to the ReachFive service.

This component requires the generic **int_reachfive** and **int_reachfive_sfra** cartridges to be included in the code source of the merchant Salesforce Commerce Cloud sites. The merchants will also have to set specific Site Preferences in order for the service to work properly, as described in this documentation.

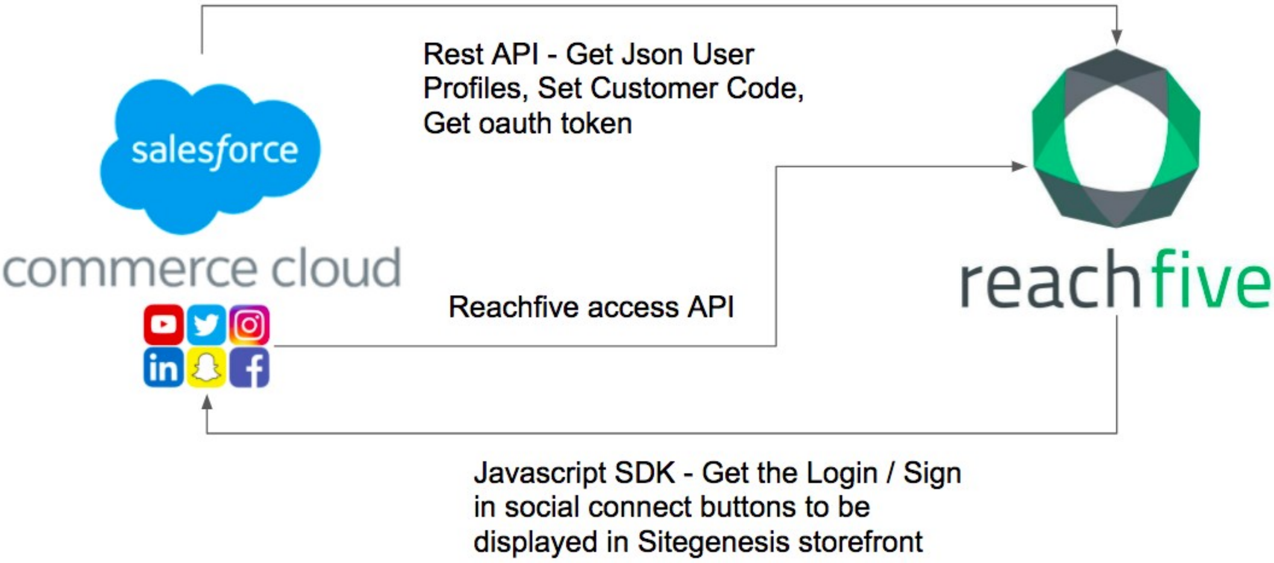
The merchant's storefronts will be slightly modified, to include the Reach Five SSO widget or social connect buttons, as described in this documentation.

The development of this cartridge is based on SFRA version 6.3.0.

2. Component Overview

2.1 Functional Overview

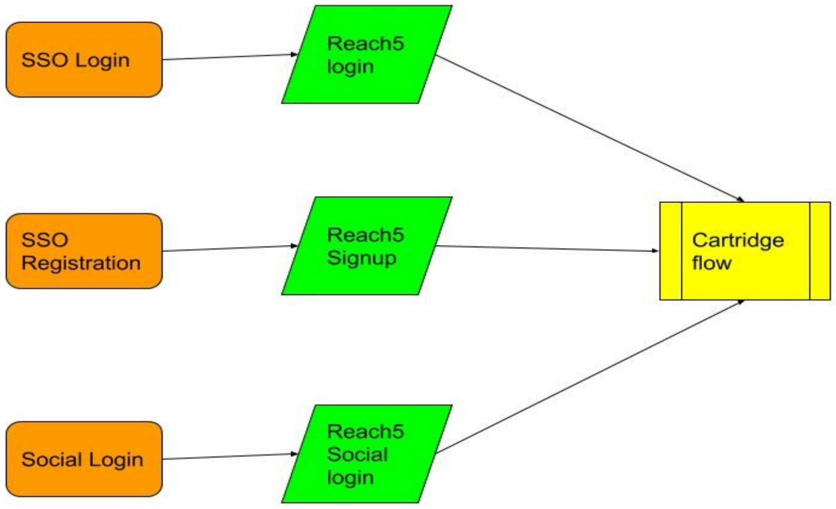
The **int_reachfive** and **int_reachfive_sfra** cartridges makes use of the Javascript SDK and the REST API provided by ReachFive to exchange data between the Salesforce Commerce Cloud instance and the ReachFive platform.


Rest API - Get Json User Profiles, Set Customer Code, Get oauth token
salesforce
commerce cloud
Reachfive access API
reachfive
Javascript SDK - Get the Login / Sign in social connect buttons to be displayed in Sitegenesis storefront

The Javascript SDK provides widget and API to integrate SFCC with ReachFive, in details:

- SSO: widget to manage login, signup, change password are included in the SFRA login page, registration page, my account pages, checkout pages.
- Social Login: buttons for social login are added to the login page, registration page, my account page, checkout pages.

The following diagrams illustrate the Login and Registration Process



In the SSO scenario, a customer access to the SSO Login / Signup widget from:

- Login/Registration Page
- Checkout Page

In these pages, a widget is presented instead of the standard SFRA related form.

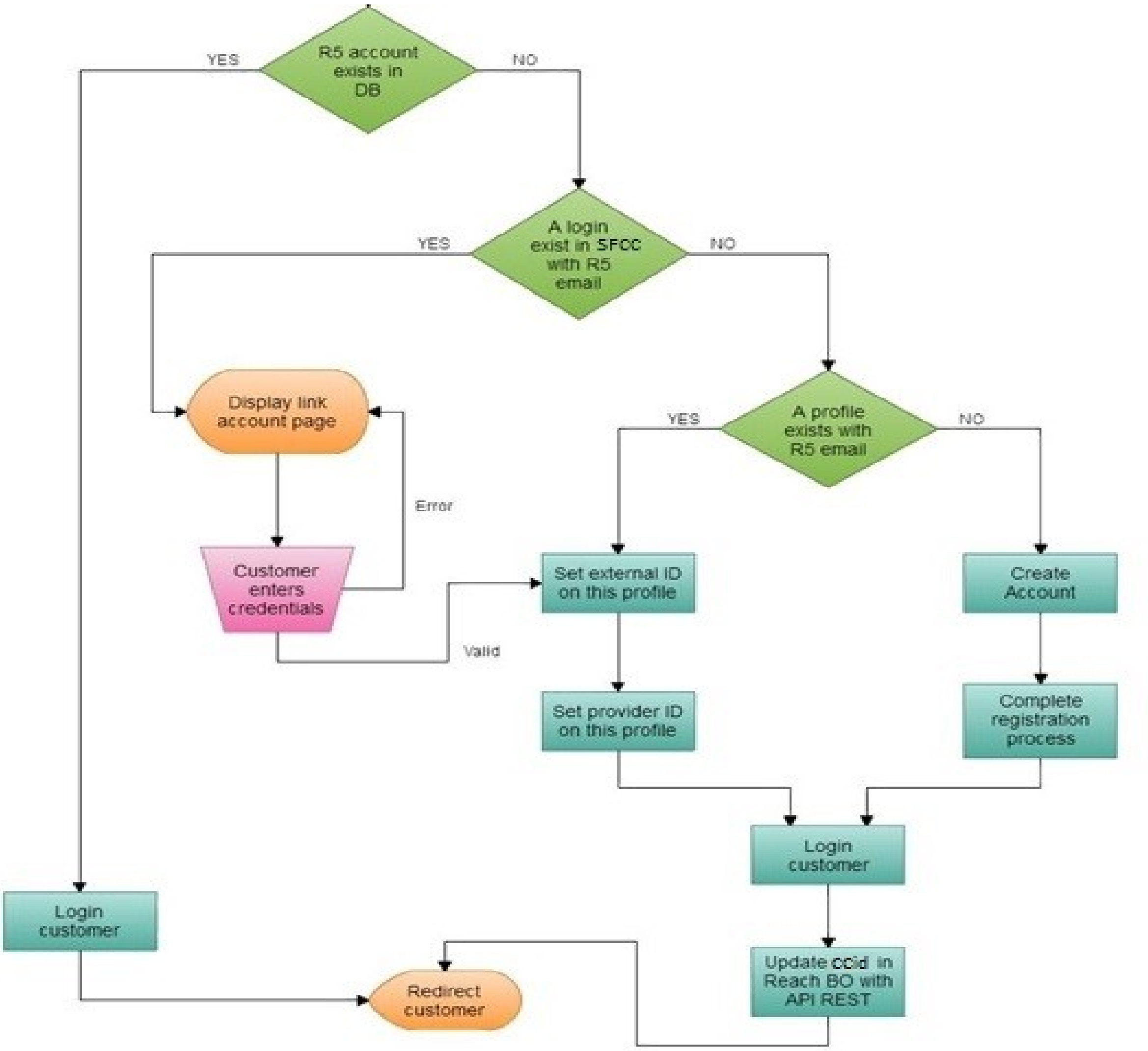
In the SSO scenario and Social Login scenario the button for Social Login are present in the following pages:

- Login/Registration Page
- Checkout Page

The SSO signup widget create a Profile in ReachFive server.
The SSO login widget search for a Profile present on ReachFive server.
The Social Login widget perform an oauth authentication with the social network account and pass the profile information to ReachFive server.

The cartridge flow process manages the link of ReachFive profile information with a customer in SFCC.
The business logic is described in the following diagram:

R5 = ReachFive

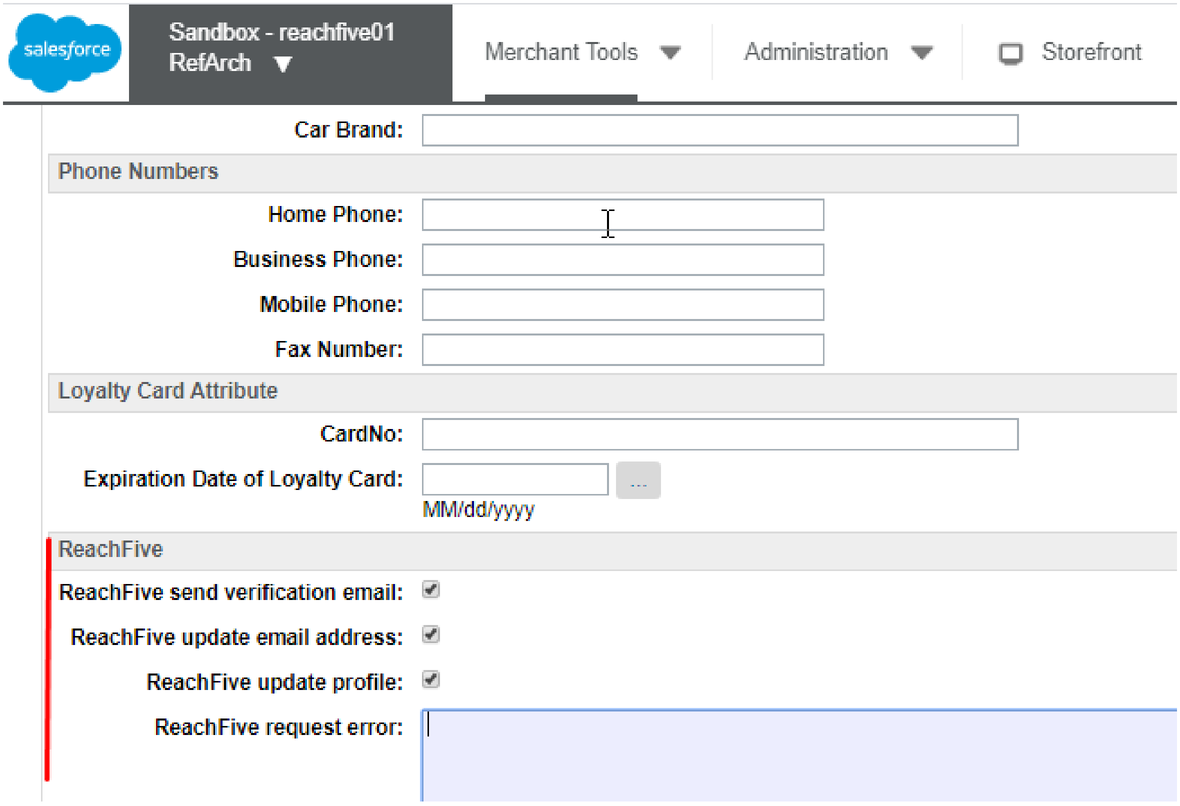

R5 account exists in DB
YES
NO
A login exist in SFCC with R5 email
YES
NO
A profile exists with R5 email
YES
NO
Display link account page
Error
Customer enters credentials
Valid
Set external ID on this profile
Set provider ID on this profile
Create Account
Complete registration process
Login customer
Update ccid in Reach BO with API REST
Login customer
Redirect customer

Details about ReachFive UI and Core SDK:
https://www.npmjs.com/package/@reachfive/identity-ui
https://developer.reachfive.com/sdk-ui/index.html

https://www.npmjs.com/package/@reachfive/identity-core
https://developer.reachfive.com/sdk-core/index.html

ReachFive Profiles Synchronization

‘ReachFive-Synchronization’ job was created. The job will take all customers that have one of the Profile attributes (reachfiveSendVerificationEmail, reachfiveUpdateEmailAddress, reachfiveUpdateProfile) set to true. Then for each of those customers it will do the appropiate ReachFive calls and set the flags to false. If any of the calls fail the error will be logged in the error logs and the ‘reachfiveError’ attribute will be populated only with the last errors.



Car Brand:

Phone Numbers

Home Phone:

Business Phone:

Mobile Phone:

Fax Number:

Loyalty Card Attribute

CardNo:

Expiration Date of Loyalty Card: MM/dd/yyyy

ReachFive

ReachFive send verification email: ☑

ReachFive update email address: ☑

ReachFive update profile: ☑

ReachFive request error:

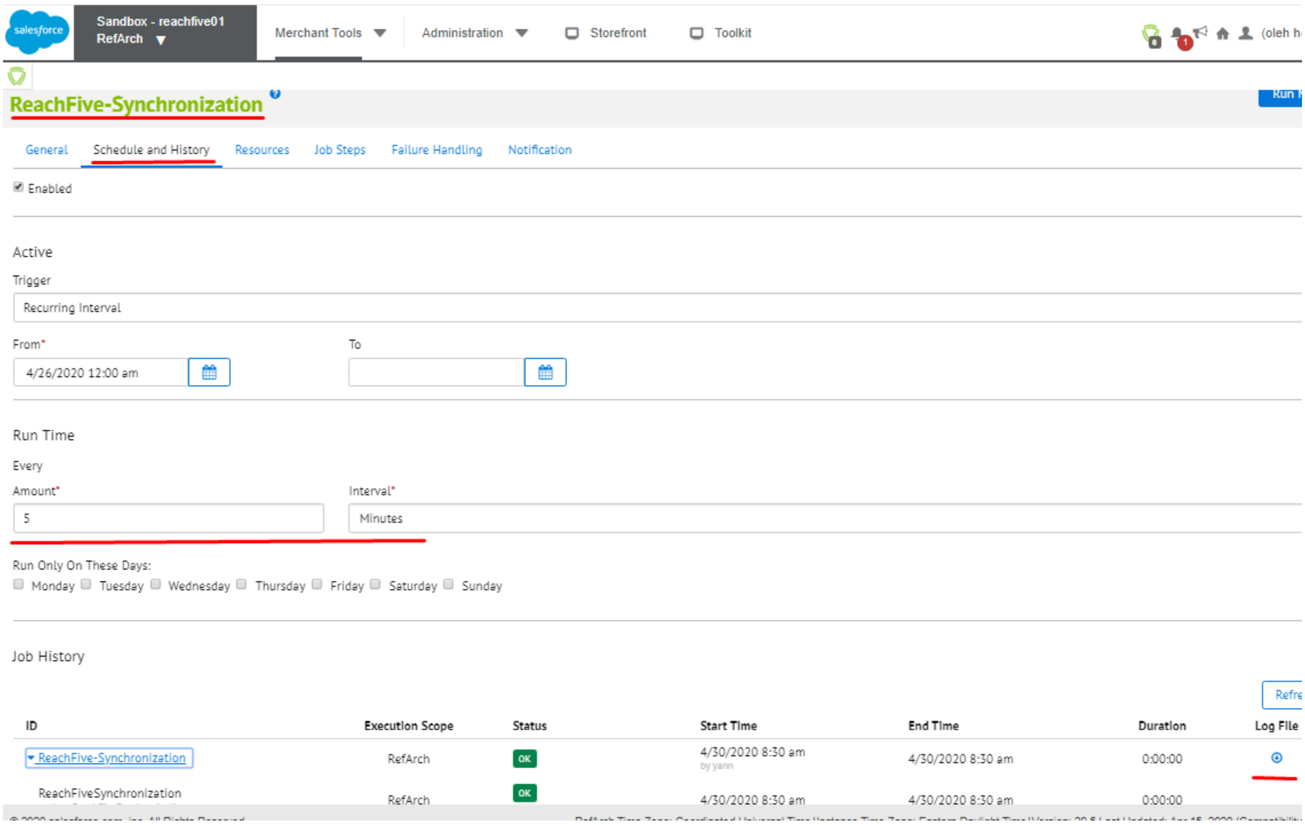
When synching the profile the job uses the “reach5ProfileFieldsJSON” Site preference in ‘ReachFive’ group to determine which fields need to be synched and mapping between SFCC and ReachFive profile fields.

The job uses such services:

- reachfive.rest.auth – to get management access token which is used in other reachFive API calls
- reachfive.updateprofile.put – to update email and profile fields
- reachfive.verifyemail.post – to send the verification email for updated email address

This job is scheduled to run every 5 minutes by default.

All issues and exceptions which occur during job running are added to job log.



ReachFive-Synchronization

General | Schedule and History | Resources | Job Steps | Failure Handling | Notification

☑ Enabled

Active

Trigger: Recurring Interval

From*: 4/26/2020 12:00 am

To:

Run Time

Every

Amount*: 5

Interval*: Minutes

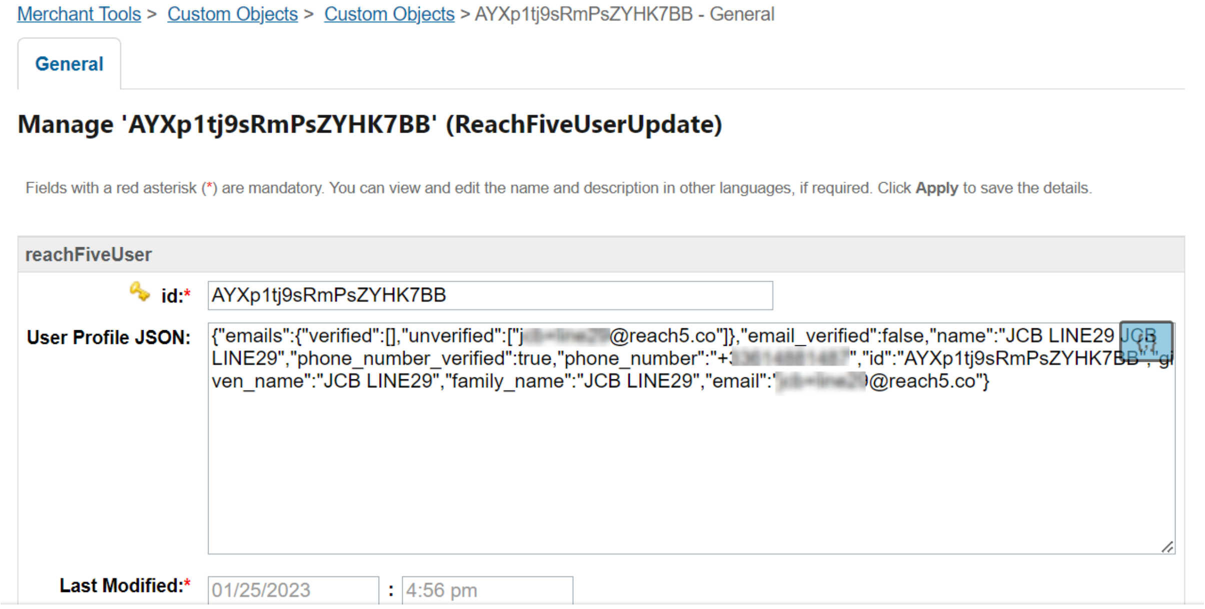
Run Only On These Days:
□ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday

Job History

ID	Execution Scope	Status	Start Time	End Time	Duration	Log File
▾ ReachFive-Synchronization	RefArch	OK	4/30/2020 8:30 am by yann	4/30/2020 8:30 am	0:00:00	⊕
ReachFiveSynchronization	RefArch	OK	4/30/2020 8:30 am	4/30/2020 8:30 am	0:00:00	

Webhook.
An additional purpose of the "ReachFive-Synchronization" job is the processing of custom objects created on the basis of the work of the reverse mechanism of synchronization of "ReachFive-Salesforce" profiles to the consequences of a Webhook:

1. The ReachFive user profile is changed externally.
2. ReachFive Post-Event Webhooks are called by Salesfroce with profile data.
3. Salesforce creates a custom "ReachFiveUserUpdate" object with the new user data.



Merchant Tools > Custom Objects > Custom Objects > AYXp1tj9sRmPsZYHK7BB - General

Manage 'AYXp1tj9sRmPsZYHK7BB' (ReachFiveUserUpdate)

Fields with a red asterisk (*) are mandatory. You can view and edit the name and description in other languages, if required. Click **Apply** to save the details.

reachFiveUser

id:* AYXp1tj9sRmPsZYHK7BB

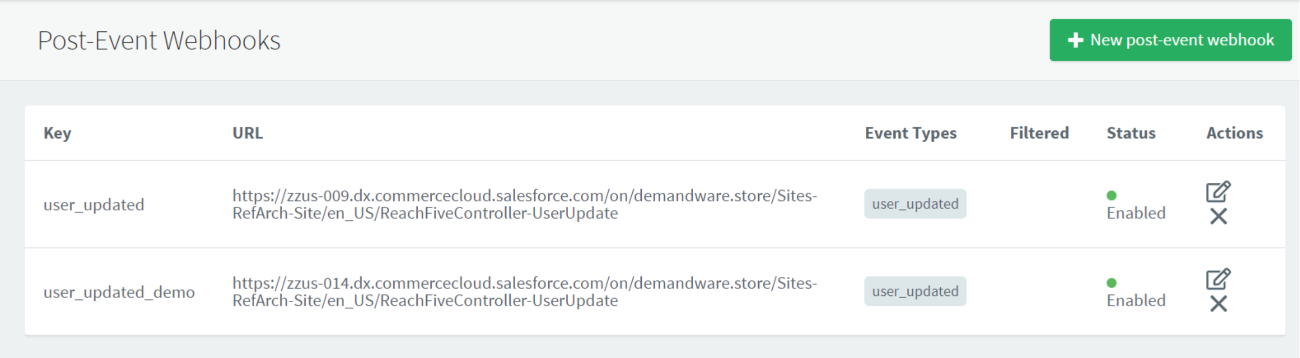
User Profile JSON: {"emails":{"verified":[],"unverified":["j[redacted]@reach5.co"]},"email_verified":false,"name":"JCB LINE29 JCB LINE29","phone_number_verified":true,"phone_number":"+[redacted]","id":"AYXp1tj9sRmPsZYHK7BB","given_name":"JCB LINE29","family_name":"JCB LINE29","email":"[redacted]@reach5.co"}

Last Modified:* 01/25/2023 : 4:56 pm

4. The "ReachFive-Synchronization" job updates the user data using the "UserSynchronization" step.

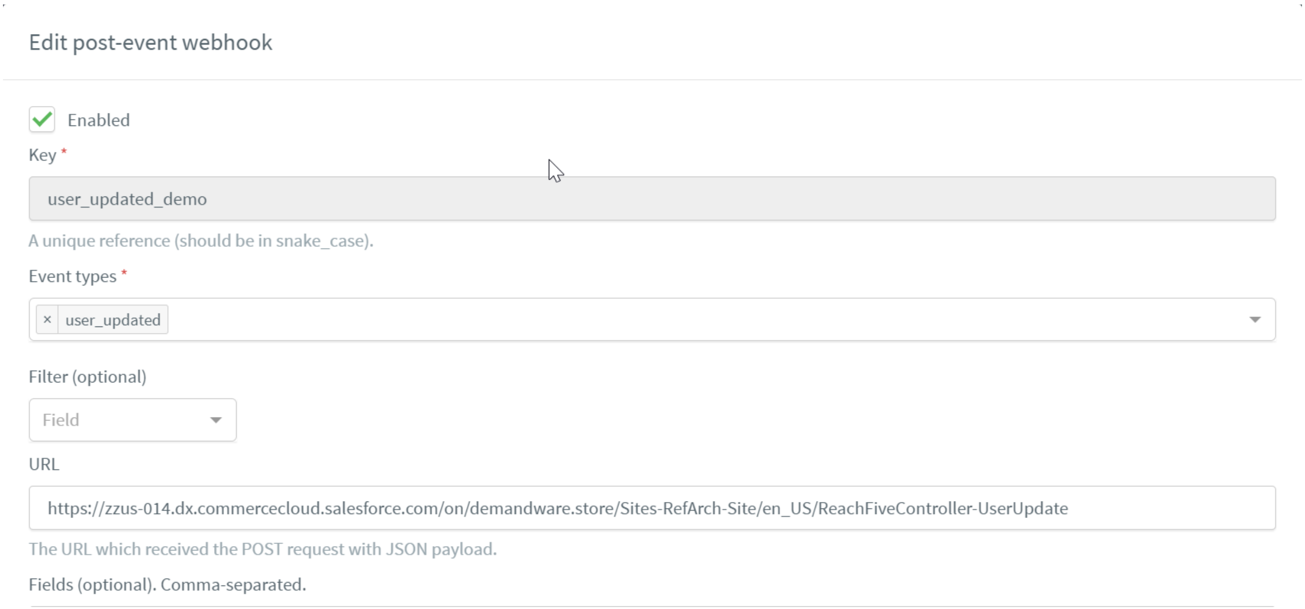
Webhook configuration.
Normally we use webhook post-event. The post-event webhook documentation can be found at this link: https://developer.reachfive.com/docs/webhooks.html#post-event-webhooks.

Here is an example how webhook configuration can looks like:



Post-Event Webhooks

Key	URL	Event Types	Filtered	Status	Actions
user_updated	https://zzus-009.dx.commercecloud.salesforce.com/on/demandware.store/Sites-RefArch-Site/en_US/ReachFiveController-UserUpdate	user_updated		● Enabled	✎ ✕
user_updated_demo	https://zzus-014.dx.commercecloud.salesforce.com/on/demandware.store/Sites-RefArch-Site/en_US/ReachFiveController-UserUpdate	user_updated		● Enabled	✎ ✕



Edit post-event webhook

☑ Enabled

Key *

user_updated_demo

A unique reference (should be in snake_case).

Event types *

× user_updated

Filter (optional)

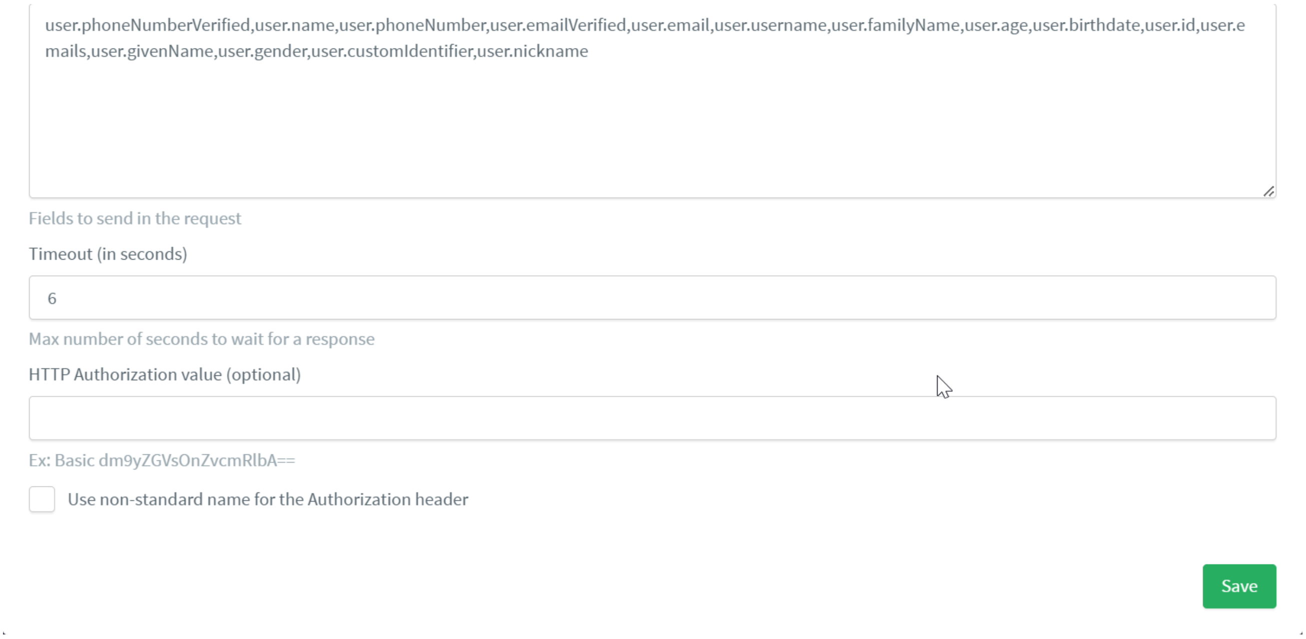
Field

URL

https://zzus-014.dx.commercecloud.salesforce.com/on/demandware.store/Sites-RefArch-Site/en_US/ReachFiveController-UserUpdate

The URL which received the POST request with JSON payload.

Fields (optional). Comma-separated.



user.phoneNumberVerified,user.name,user.phoneNumber,user.emailVerified,user.email,user.username,user.familyName,user.age,user.birthdate,user.id,user.emails,user.givenName,user.gender,user.customIdentifier,user.nickname

Fields to send in the request

Timeout (in seconds)

6

Max number of seconds to wait for a response

HTTP Authorization value (optional)

Ex: Basic dm9yZGVsOnZvcmRlbA==

□ Use non-standard name for the Authorization header

These two approaches will allow you to keep user profiles up to date and in sync.

2.2 Use Cases

The following use cases are managed by the **int_reachfive** and **int_reachfive_sfra** cartridges :

SSO:

1. Registration of a new customer through a ReachFive Signup widget
2. Synchronization the newsletter consent when reachFive account is created on SFCC
3. Login of an existing SFCC Customer through ReachFive. The SFCC Customer account has been created through the native SFRA account creation form.
4. Login of an existing ReachFive customer. The SFCC customer is created and linked to the ReachFive Profile
5. Social Account Activation/Deactivation, in My Account the customer using a widget can connect more than one social account to his profile.

Social Login

1. Registration of a new customer through a ReachFive supported social connect provider
2. Login of a customer who has previously created his SFCC Customer account through a ReachFive supported social connect provider
3. Login of an existing SFCC Customer through ReachFive. The SFCC Customer account has been created through the native SFRA account creation form.
4. Login of an existing SFCC Customer through ReachFive. The SFCC Customer account has been created through a non ReachFive social connect provider (i.e through the social connect provider natively proposed by SFRA)
5. Social Account Activation/Deactivation, in My Account the customer using a widget can connect more than one social account to his profile.

Transition Mode:

1. Registration of a new customer through a SFCC Signup form.
2. First time device login determined by cookies.
3. First time Login with SFCC login form. The SFCC Customer account will be created on Reachfive with the same login and password. Customer relogin with Reachfive account.
4. Second time Login on the same device - Reachfive Login form display.
5. All other features of the previously described modes of operation are retained and used.

ReachFive Profiles Synchronization:

1. Update the email address
2. Send verification email for new email address
3. Update customer profile and addresses

ReachFive Profiles Synchronization with Webhook:

1. Automatically updates the Salesforce profile
2. Creates a custom object to ensure updates

The Customer Registration and login through ReachFive works whether the Customer logs in / registers while in the checkout process or in the standard account registration / login page.

2.3 Limitations, Constraints

There is currently no limitations nor constraints identified with this component at this time.

2.4 Compatibility

The latest release is compatible with SFRA 6.3.0.

2.5 Privacy

The int_reachfive_sfra cartridge accesses the SFCC Customer.ID and the SFCC Site.ID properties' values and stores this information within the ReachFive platform. Moreover, during the social connect process, ReachFive stores the social data (coming from the social provider), that the Customer has willingly accepted to share, and makes this data available to the merchant.

During the registration / login process:

If the data is available through the social provider and if there is no previous value stored within SFCC for these properties, the following properties are set on the Customer profile on the SFCC side:

- Profile.lastName
- Profile.firstName
- Profile.email

The following Credentials properties will be set during the registration / login process through ReachFive :

- Credentials.authenticationProviderID
  - The value set is a custom value chosen by the merchant and manageable in the ReachFive Custom Site Preferences of SFCC Business Manager.
- Credentials.externalID
  - This property stores the ReachFive user ID.

2.6 Security

The social login process has to happen on SFCC's side, which implies a risk that a malicious attacker will attempt to tamper with the data sent from the client to the server.
In the next paragraph we explain the authentication process and how it prevents security issues

Step 1: User authentication process

The user authenticates via email/password or social login. This process must be at least partially implemented using the suitable ReachFive's SDK depending on the client platform (Web, mobile…).

ReachFive's Identity SDKs allow different authentication flows. For server-side authentication, you must use a code response type, and set your login callback URL in the redirectUri attribute
(The URI must be whitelisted in the "Allowed Callback URLs" field of your ReachFive's account settings).

For security reasons, you have to list all callback URLs in the Allowed Callback URLs field of your ReachFive console.
You can find below an example using the Identity SDK for Web.

```
sdkUiClient.showAuth({
  container: 'auth-container',
  auth: {
    responseType: 'code', // This is the default value when "redirectUri" attribute is set.
    redirectUri: 'https://www.example.com/login/callback'
  }
});
```

Step 2: Handle the Authorization Response

After the authentication process, ReachFive responds to your application by redirecting the user to the previously-specified callback URL (redirectUri attribute).

If the authentication succeeds, then the response contains an authorization code. If not (e.g. when the user does not approve access to his social data), the response contains an error message. The authorization code or error message that is returned to your web server appears in the query string, as shown below.

An authorization code response:

https://www.example.com/login/callback?code=A8sLD49d-lPcKyUwBaSm4oThfjp4

An error response:

https://www.example.com/login/callback?error=access_denied

Step 3: Exchange authorization code for ID token

After the web server receives the authorization code, it can exchange it for an ID token using an HTTP request to the ReachFive's token endpoint.

The string YOUR_REACHFIVE_DOMAIN should be replaced with the domain of your ReachFive account and the string YOUR_REACHFIVE_CLIENT_ID should be replaced with the client ID of your ReachFive account.

```
POST /oauth/token HTTP/1.1
Host: https://YOUR_REACHFIVE_DOMAIN
Content-Type: application/x-www-form-urlencoded

code=A8sLD49d-lPcKyUwBaSm4oThfjp4
&client_id=YOUR_REACHFIVE_CLIENT_ID
&redirect_uri=https://www.example.com/login/callback
&grant_type=authorization_code
```

Success response example:

```
{
  "id_token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1N...",
  "access_token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIU...",
  "token_type": "Bearer",
  "expires_in": 3600
}
```

Step 4: Retrieve user’s profile data from ID Token

After your application obtains an ID token, you can use the token to retrieve the user’s profile data by parsing it. An id_token is a JWT (JSON Web Token), that is, a cryptographically signed Base64-encoded JSON object. As you are communicating directly with ReachFive over HTTPS channel, it is normally not critical that you validate your id_token before parsing it. However most API libraries combine the validation with the work of decoding the base64 and parsing the JSON.

Example:

```
var decodedToken = jwt.verify(idToken, clientSecret);
```

Success example:

```
{
  "sub": "AVPw-jHcQG5c_BvJk9e_",
  "given_name": "John",
  "family_name": "Doe",
  "email": "john.doe@example.com"
}
```

3. Implementation Guide

3.1 Setup

3.1.1 Import Cartridge

Import the ***int_reachfive*** and ***int_reachfive_sfra*** cartridges in you project.

3.1.2 Import Site Preferences and Custom Objects

Import the system object customizations into the SFCC Business Manager.

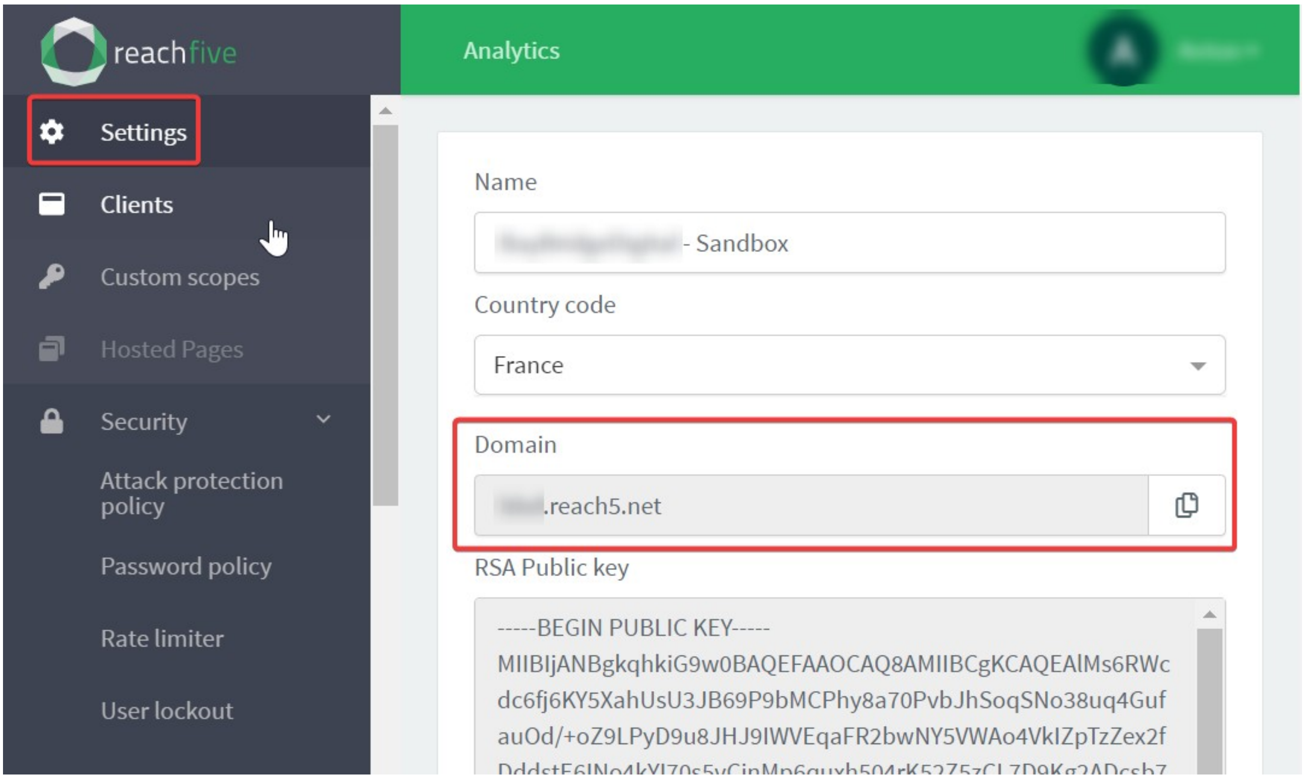
- Log into the SFCC Business Manager.
- Click Administration -> Sites Development -> Site Import & Export
- Click the upload link or button in the “Import” section.
- Use the upload control to browse for the *site_template.zip* file
- Note: if you are configuring the RefArch site, you can import the site_template.zip like this, otherwise you should follow these steps:
    - Cd in the Metadata downloaded from bitbucket/github
    - Cd /site_template/sites
    - Rename the folder Refarch with the Id of your site
    - zip -r site_template.zip site_template
- Click Upload
- Select the *site_template.zip* file that was just uploaded
- Click Import

3.2 ReachFive Configuration

In order to perform the following operations, you need access to the developer's console (https://console-staging.reach5.co/bbd/admin/settings) or someone's help from Reachfive

3.2.1 Domain

For the integration to work correctly, you must specify the domain value, which can be found: https://console-staging.reach5.co/<your-domain>/admin/settings



Name: [redacted] - Sandbox

Country code: France

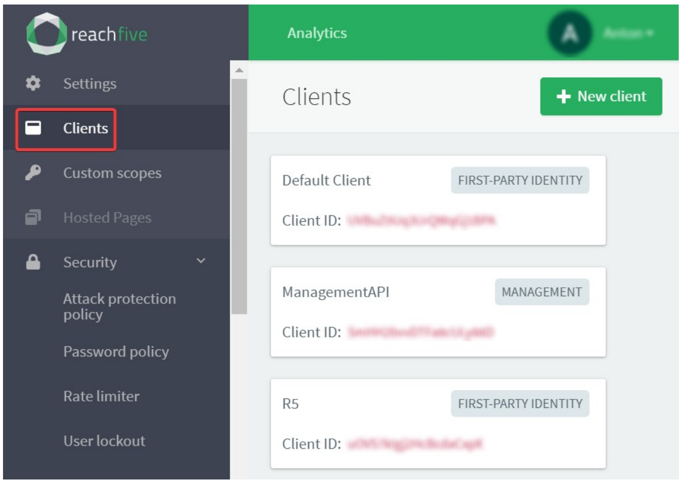
Domain: [redacted].reach5.net

RSA Public key

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlMs6RWc
dc6fj6KY5XahUsU3JB69P9bMCPhy8a70PvbJhSoqSNo38uq4Guf
auOd/+oZ9LPyD9u8JHJ9IWVEqaFR2bwNY5VWAo4VkIZpTzZex2f
DddstF6INo4kYI70s5vCinMp6quxh504rK52Z5zCL7D9Kg2ADcsh7
```

3.2.2 First-party Identity client

The list of keys can be found in the "Clients" tab. It contains both clients First-party Identity clients and Management clients list.



Default Client FIRST-PARTY IDENTITY
Client ID: [redacted]

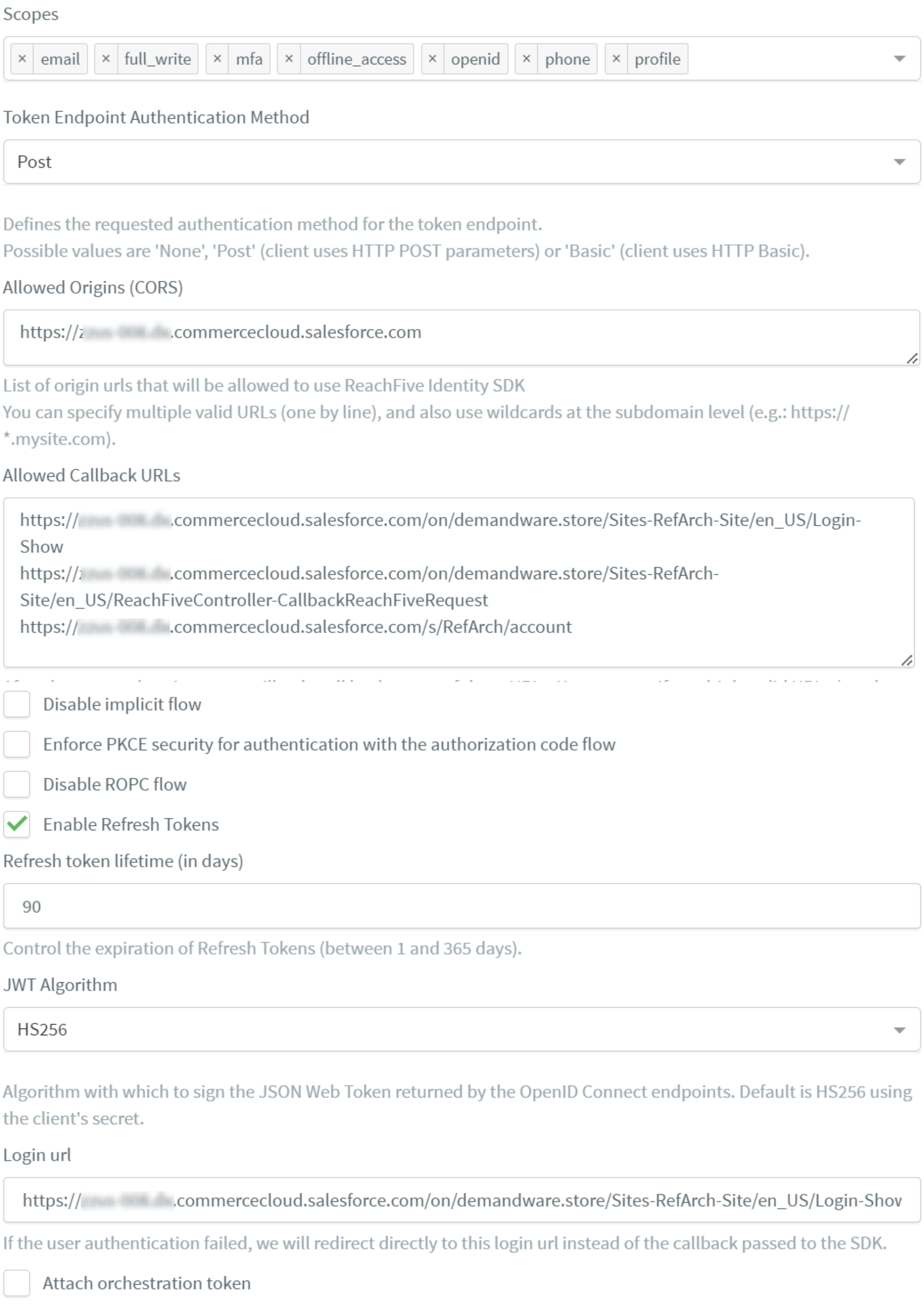
ManagementAPI MANAGEMENT
Client ID: [redacted]

R5 FIRST-PARTY IDENTITY
Client ID: [redacted]

Select your First-party Identity client and update clent preference with your site values (https://developer.reachfive.com/docs/clients.html#first-party-identity-clients).
Here is an example how it could be configured for some “Refarch” site:

Scopes	**full_write, openid, profile**
Token Endpoint Authentication Method	**POST**
Allowed Origins (CORS)	**https://<your-sandbox>.dx.commercecloud.salesforce.com**
Allowed Callback URLs	**https://<your-sandbox>.dx.commercecloud.salesforce.com/on/demandware.store/Sites-RefArch-Site/en_US/Login-Show** **https://<your-sandbox>.commercecloud.salesforce.com/on/demandware.store/**

	Sites-RefArch-Site/en_US/ReachFiveController-CallbackReachFiveRequest
	(false) **Disable implicit flow** (false) **Enforce PKCE security for authentication with the authorization code flow** (false) **Disable ROPC flow** (true) **Enable Refresh Tokens**
JWT Algorithm	**HS256**
Login url	**https://<your-sandbox>.dx.commercecloud.salesforce.com/on/demandware.store/Sites-RefArch-Site/en_US/Login-Show**



Scopes

× email × full_write × mfa × offline_access × openid × phone × profile

Token Endpoint Authentication Method

Post

Defines the requested authentication method for the token endpoint.
Possible values are 'None', 'Post' (client uses HTTP POST parameters) or 'Basic' (client uses HTTP Basic).

Allowed Origins (CORS)

https://[redacted].commercecloud.salesforce.com

List of origin urls that will be allowed to use ReachFive Identity SDK
You can specify multiple valid URLs (one by line), and also use wildcards at the subdomain level (e.g.: https://*.mysite.com).

Allowed Callback URLs

https://[redacted].commercecloud.salesforce.com/on/demandware.store/Sites-RefArch-Site/en_US/Login-Show
https://[redacted].commercecloud.salesforce.com/on/demandware.store/Sites-RefArch-Site/en_US/ReachFiveController-CallbackReachFiveRequest
https://[redacted].commercecloud.salesforce.com/s/RefArch/account

☐ Disable implicit flow

☐ Enforce PKCE security for authentication with the authorization code flow

☐ Disable ROPC flow

☑ Enable Refresh Tokens

Refresh token lifetime (in days)

90

Control the expiration of Refresh Tokens (between 1 and 365 days).

JWT Algorithm

HS256

Algorithm with which to sign the JSON Web Token returned by the OpenID Connect endpoints. Default is HS256 using the client's secret.

Login url

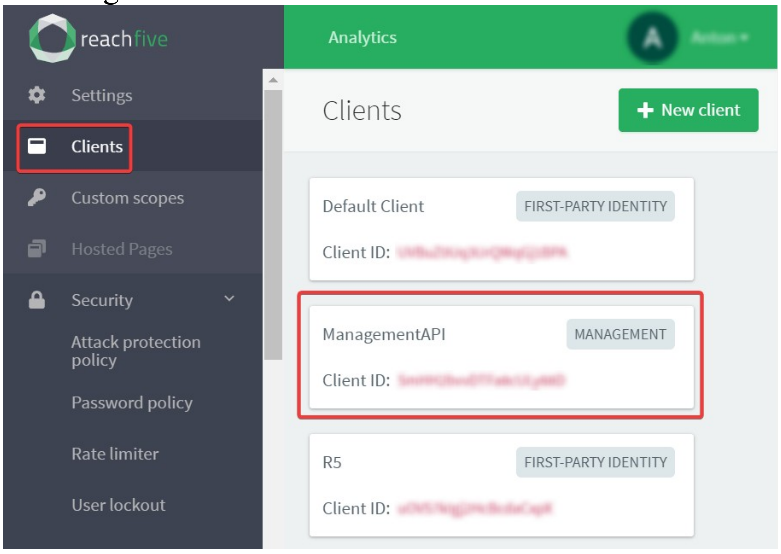
https://[redacted].commercecloud.salesforce.com/on/demandware.store/Sites-RefArch-Site/en_US/Login-Shov

If the user authentication failed, we will redirect directly to this login url instead of the callback passed to the SDK.

☐ Attach orchestration token

3.2.3 Management client

Some operations are more sensitive to security and require a separate access level. This is provided with an additional access key ("management" client) which allows from the back-end side communicate with the management API.



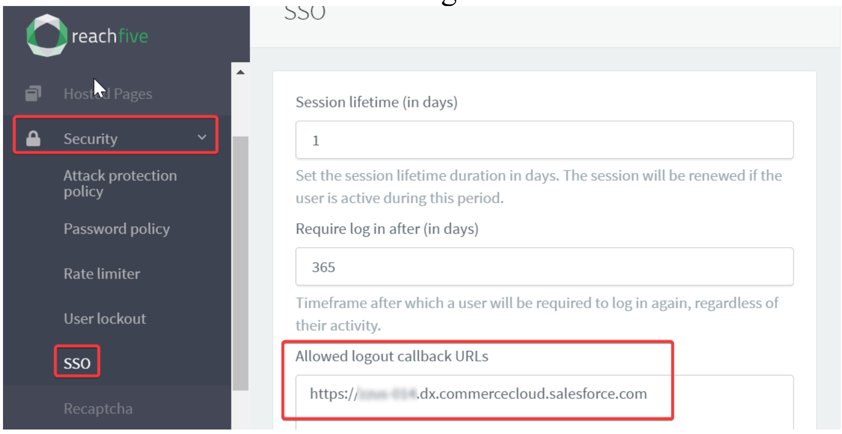
Clients

Default Client	FIRST-PARTY IDENTITY
Client ID: [redacted]	
ManagementAPI	MANAGEMENT
Client ID: [redacted]	
R5	FIRST-PARTY IDENTITY
Client ID: [redacted]	

Use the documentation (https://developer.reachfive.com/docs/clients.html#management-clients) to set up the client's management API or contact Reachfive for support.

3.2.4 SSO

When the SSO feature is activated on your account, ReachFive manages the end user cookie session. Here is an example how SSO session could be configured:



SSO

Session lifetime (in days)

1

Set the session lifetime duration in days. The session will be renewed if the user is active during this period.

Require log in after (in days)

365

Timeframe after which a user will be required to log in again, regardless of their activity.

Allowed logout callback URLs

https://[redacted].dx.commercecloud.salesforce.com

In order to obtain additional details please check documentation: https://developer.reachfive.com/docs/sso.html

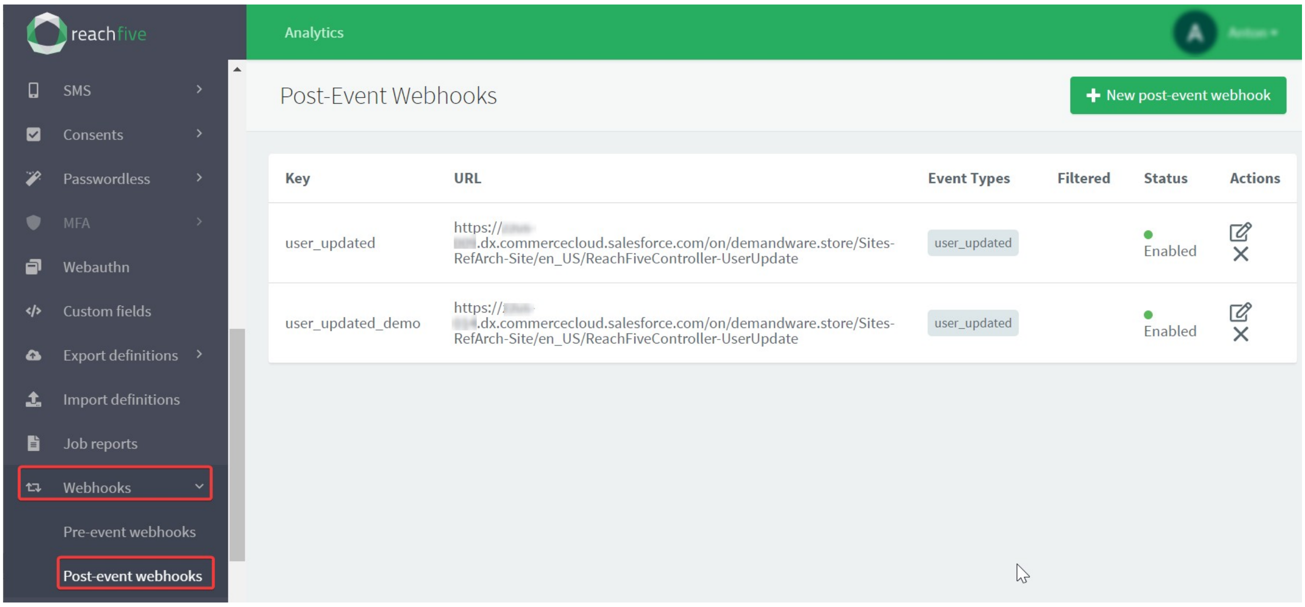
3.2.5 Webhooks

Documentation about webhook could be founded here: https://developer.reachfive.com/docs/webhooks.html

Normally we are using post-event webhook in order recive all changes for profile before call update. Here is an example, how webhook configuration could look like:

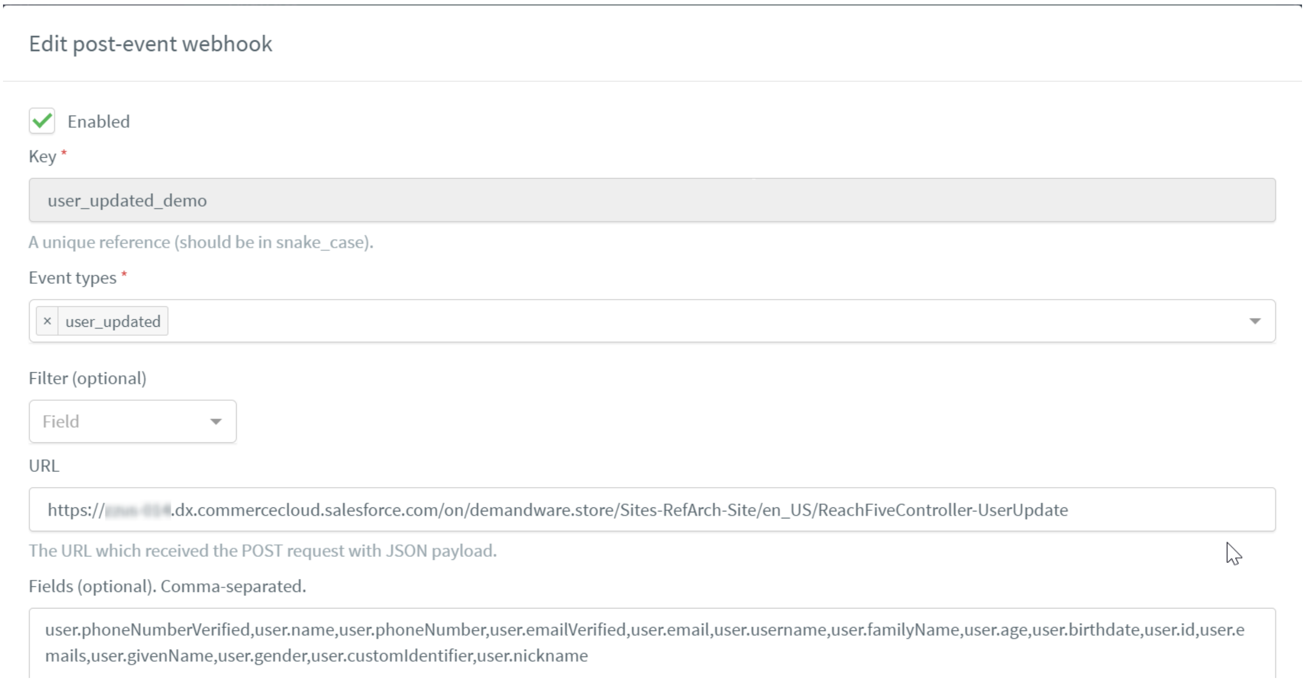
Preference	Value
Key	user_updated_demo

Event types	user_update
URL	https://<your-sandboxId>.dx.commercecloud.salesforce.com/on/demandware.store/Sites-RefArch-Site/en_US/ReachFiveController-UserUpdate
Fields	user.phoneNumberVerified,user.name,user.phoneNumber,user.emailVerified,user.email,user.username,user.familyName,user.age,user.birthdate,user.id,user.emails,user.givenName,user.gender,user.customIdentifier,user.nickname



Post-Event Webhooks

Key	URL	Event Types	Filtered	Status	Actions
user_updated	https://[redacted].dx.commercecloud.salesforce.com/on/demandware.store/Sites-RefArch-Site/en_US/ReachFiveController-UserUpdate	user_updated		● Enabled	✎ ✕
user_updated_demo	https://[redacted].dx.commercecloud.salesforce.com/on/demandware.store/Sites-RefArch-Site/en_US/ReachFiveController-UserUpdate	user_updated		● Enabled	✎ ✕



Edit post-event webhook

☑ Enabled

Key *

user_updated_demo

A unique reference (should be in snake_case).

Event types *

× user_updated

Filter (optional)

Field

URL

https://[redacted].dx.commercecloud.salesforce.com/on/demandware.store/Sites-RefArch-Site/en_US/ReachFiveController-UserUpdate

The URL which received the POST request with JSON payload.

Fields (optional). Comma-separated.

user.phoneNumberVerified,user.name,user.phoneNumber,user.emailVerified,user.email,user.username,user.familyName,user.age,user.birthdate,user.id,user.emails,user.givenName,user.gender,user.customIdentifier,user.nickname

3.3 Salesfroce Configuration

3.3.1 Add the Reach Five Cartridge to your Storefront Cartridge Path

Append int_reachfive_sfra at the beginning of the effective cartridge path

- Log into SFCC's Business Manager.
- Click Administration -> Sites -> Manage Sites
- Select the desired site
- Click on the Settings tab.
- Append "**int_reachfive_sfra**:app_storefront_base:**int_reachfive**" to the cartridges path.
- Click Apply

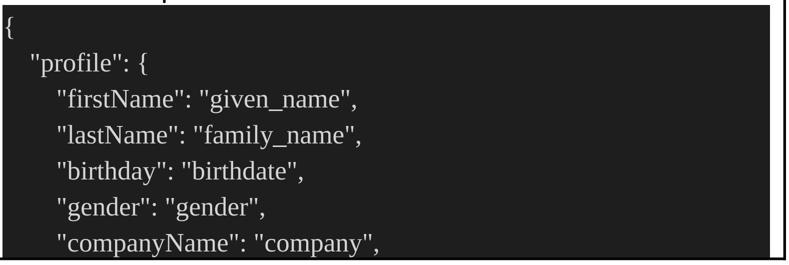
3.3.2 Configure Reach Five Site Preferences

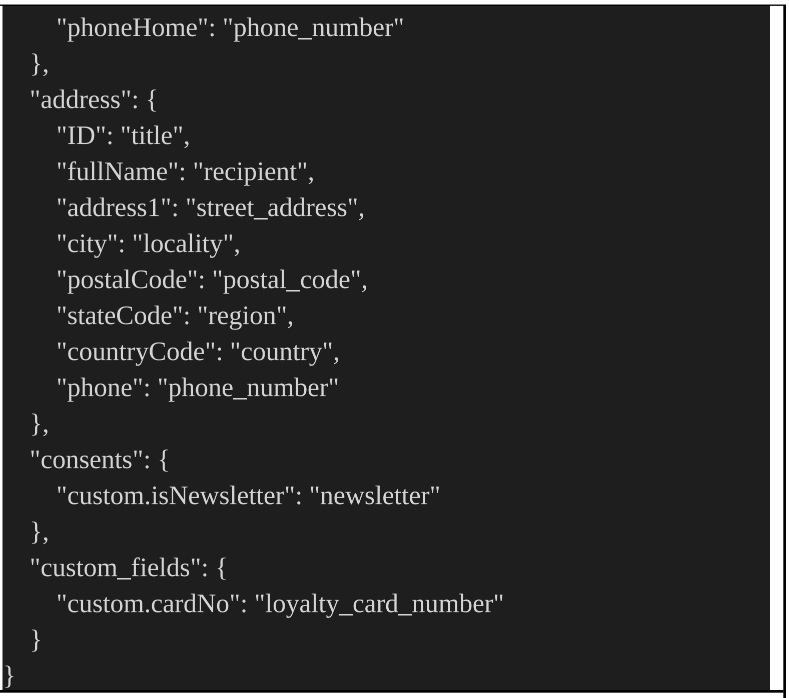
Configure Reach Five Custom Preferences using the SFCC Business Manager

- Log into the SFCC Business Manager
- Select the desired site from the tabs across the top of the page.
- Click Site Preferences -> Custom Preferences
- Fill in the Site Preferences

Entity	Description
cartridgeControllersName	**NOT USED FOR SFRA.** Name of the base controllers cartridge (i.e. app_storefront_base)
isReachFiveEnabled	If set to true, ReachFive is activated
isReachFiveTransitionActive	Activate "transition" mode. This mode suppose soft/shadow transfer Salesfroce accounts on Reachfive during customer authentification.
reachFiveTransitionCookieDuration	**NOT USED FOR SFRA.**
isReachFiveSessionForcedAuth	Enable SSO forced active session authentification from any page of the site. Generally it give you ability maintain customer authentificated even after Salesforce session is finished: https://developer.reachfive.com/docs/sso.html
isReach5ThemeActive	If set to true, default theme is activated (not currently used)
reach5Domain	The domain name of the ReachFive environment
reach5ApiKey	The API key required to access the ReachFive Environment
reach5ClientSecret	The client secret key required to access the ReachFive environment
reachFiveProviderId	The name of the provider that will be used to populate the Credentials.authenticationProviderID properties value for the Customers who will register or log in on the SFCC storefront through ReachFive
isReachFastRegister	If "No", pending the Social Login or SSO, if the user profile does not exist in SFCC database, the user is redirected to a registration page, with pre-filled but editable fields. If "Yes", pending the Social Login or SSO, if the user profile does not exist in SFCC Database, it is created using

	the information from the Social Login or SSO.
isReachFiveLoginAllowed	If “No” the Social Login scenario is enabled: the social buttons are added to login page, registration page, checkout page, personal data page. If “Yes” the Single Sign On scenario is enable: the reach five login / signup widget will be present in login page, registration page, checkout page. In Personal Data page, there will be the social account widget that permits to the customer to enable or disable social account related to his profile.
reach5ManagementApiKey	The API key required to access the ReachFive Managment API: https://developer.reachfive.com/docs/clients.html#management-clients
reach5ManagementClientSecret	The client secret key required to access the ReachFive Managment API: https://developer.reachfive.com/docs/clients.html#management-clients
reach5ManagementScope	Space-delimited list of Management permissions. The default value is “manage:users read:users”

reach5ProfileFieldsJSON	ReachFive JSON allows the flexible configuration for updating profiles fields without code changing.
	It determines which fields need to be synched and set mapping between SFCC and ReachFive profile fields. It consists of such Objects: profile, address, consents, custom_fields. Each Object matches to appropriate ReachFive Profile Object.
	Here are used key-value pairs to map SFCC and ReachFive fields. Key is SFCC profile attribute and value is ReachFive field. Also is possible to use custom Profile attribute in key. It should contain ‘custom.’ prefix.
	To send new attribute you need to add it to appropriate Object in such format:
	(custom.)SfccAttribute: reach_five_field
	
	For ‘address’ JSON Object are used SFCC CustomerAddress attributes for other Objects are used SFCC Profile attributes
	
	JSON Example:
	
	{
	  "profile": {
	    "firstName": "given_name",
	    "lastName": "family_name",
	    "birthday": "birthdate",
	    "gender": "gender",
	    "companyName": "company",

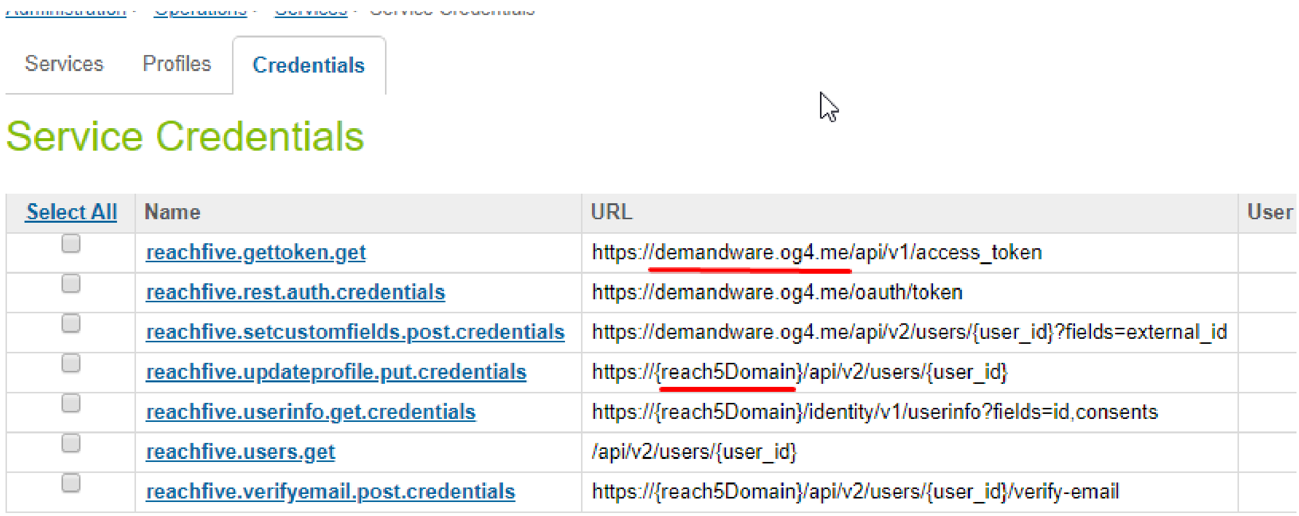
	
	"phoneHome": "phone_number"
	},
	"address": {
	"ID": "title",
	"fullName": "recipient",
	"address1": "street_address",
	"city": "locality",
	"postalCode": "postal_code",
	"stateCode": "region",
	"countryCode": "country",
	"phone": "phone_number"
	},
	"consents": {
	"custom.isNewsletter": "newsletter"
	},
	"custom_fields": {
	"custom.cardNo": "loyalty_card_number"
	}
	}

reach5UiSdkUrl	URL of the Reachfive UI SDK. We suggest use latest version of the script: https://cdn.jsdelivr.net/npm/@reachfive/identity-ui@latest/umd/identity-ui.min.js
reach5CoreSdkUrl	URL of the Reachfive Core SDK. We suggest use latest version of the script: https://cdn.jsdelivr.net/npm/@reachfive/identity-core@latest/umd/identity-core.min.js
reach5SupportedLanguageCodes	Supported ReachFive LanguageCodes. They set the language of ReachFive Form. The language lowercase ISO 639-1 codes. e.g: en, es, fr, it, nl ...
reach5DefaulLanguageCode	Defaul ReachFive LanguageCodes. It sets the language of ReachFive Form. The language lowercase ISO 639-1 code. e.g: en, es, fr, it, nl ... It is used when current site language is not supported.
reachFiveCheckCredentials	User Authentication Level Check Settings. Additional preset security level for customer data update.

3.3.3 Configure Reach Five Services

Services should be imported from site_template.zip with other metadata.

1. Log into the SFCC Business Manager.
2. Navigate to Administration -> Operations -> Services
3. Click on the Credentials tab.
4. If Credentials URL contains 'demandware.og4.me' domain then replace it to current reach5Domain.
   If URL contains '{reach5Domain}' domain then it will be replaced automatically with 'reach5Domain' Site Preference value.



Administration › Operations › Services › Service Credentials

Service Credentials

Select All	Name	URL	User
□	reachfive.gettoken.get	https://demandware.og4.me/api/v1/access_token	
□	reachfive.rest.auth.credentials	https://demandware.og4.me/oauth/token	
□	reachfive.setcustomfields.post.credentials	https://demandware.og4.me/api/v2/users/{user_id}?fields=external_id	
□	reachfive.updateprofile.put.credentials	https://{reach5Domain}/api/v2/users/{user_id}	
□	reachfive.userinfo.get.credentials	https://{reach5Domain}/identity/v1/userinfo?fields=id,consents	
□	reachfive.users.get	/api/v2/users/{user_id}	
□	reachfive.verifyemail.post.credentials	https://{reach5Domain}/api/v2/users/{user_id}/verify-email	

Configure services logging.

1. Log into the SFCC Business Manager.
2. Navigate to Administration -> Operations -> Services
3. Click on the Services tab and open needed service.
4. Set ‘Communication Log Enabled’ flag
5. Set ‘Log Name Prefix’ to ‘reachfive’
   The service responses and requests will be logged in the files with ‘service-reachfive-’ prefix.
   To see them navigate to Business Manager -> Administration -> Site Development -> Development Setup -> Security Log Files

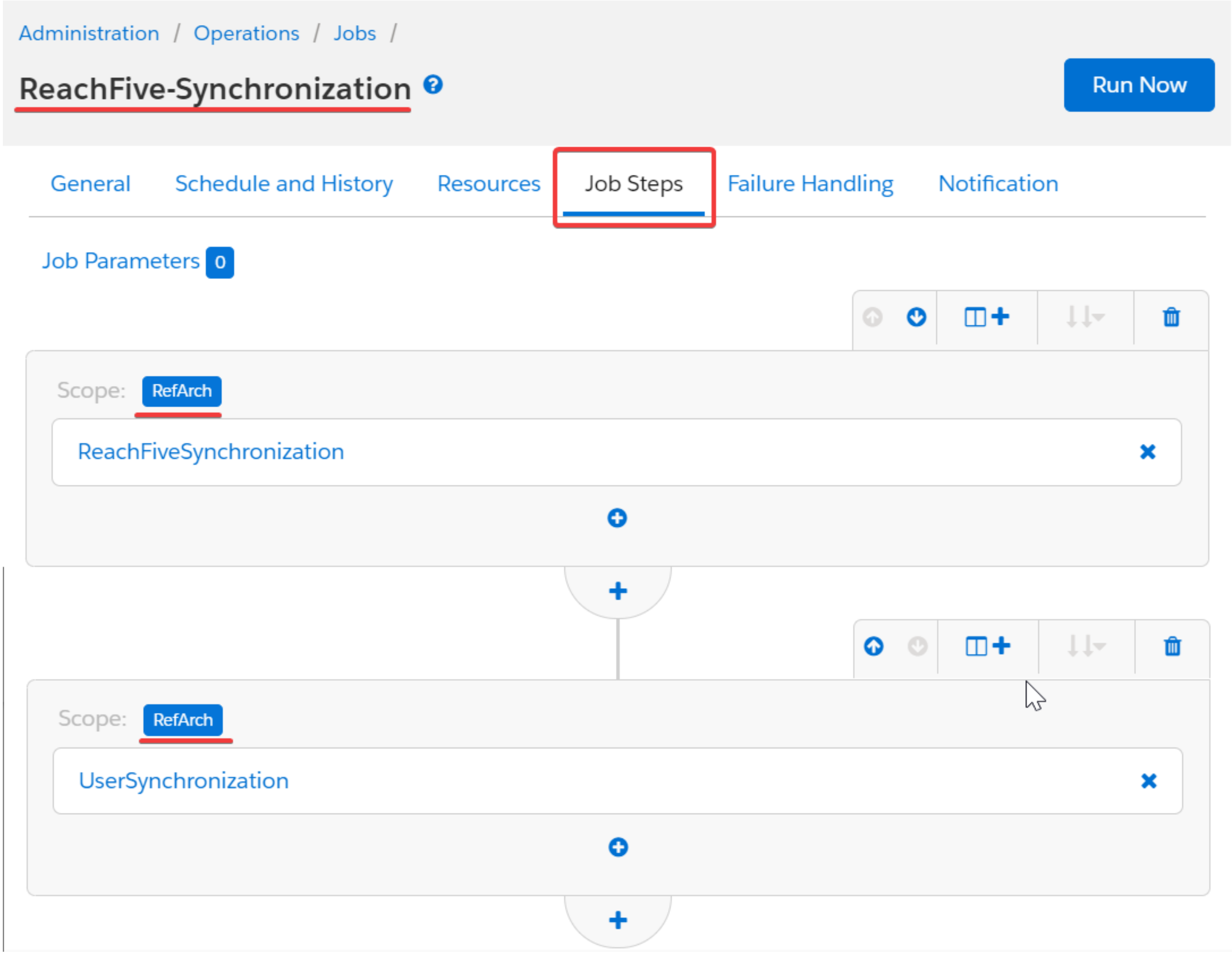
3.3.4 Configure Reach Five Jobs

Jobs should be imported from site_template.zip with other metadata.

Here is used ‘ReachFive-Synchronization’ job wich synchronizes prifile data from SFCC to ReachFive.

Set Scope:

1. Log into the SFCC Business Manager.
2. Navigate to Administration -> Operations -> Jobs
3. Click on the ‘Job Steps’ tab.
4. Set needed site in the Scope



Job Schedule:

(Job is scheduled to run every 5 minutes by default)

1. Log into the SFCC Business Manager.
2. Navigate to Administration -> Operations -> Jobs
3. Click on the ‘Schedule and History’ tab.
4. Set needed schedule or disable it

3.4 External Interfaces

A couple of services will be called during the social registration / login process. The first call generates a token which is required by the second call.

Authentication

In order to access to the API, you will need to provide an access token to authenticate with the API server. That token will be required for all API requests.
You can acquire that token with the API endpoint described in the following section.
Once you have acquired the API token, it may be provided preferably via an HTTP header.

Get an access token

Example Request

```
POST /oauth/token HTTP/1.1
Host: https://YOUR_DOMAIN
Content-Type: application/json

{
 "grant_type": "client_credentials",
 "client_id": "YOUR_CLIENT_ID",
 "client_secret": "YOUR_CLIENT_SECRET",
 "scope": "read:users manage:users"
}
```

Example Response

```
{
 "access_token": "kGu...uLs",
 "expires_in": 86400,
 "token_type": "Bearer"
}
```

Update User

Updates the specified user by setting the values of the object's properties passed. Any root properties (or custom fields) not provided will be left unchanged.

These are the user's attributes that can be updated at the root level:
external_id
email
email_verified
phone_number
custom_fields
given_name
middle_name
family_name
name
nickname
username
birthdate
gender
address
phone_number
picture
company
custom_fields

Example Request

```
PUT /api/v2/users/AVqvOB58Fg6nZfQ0ZqXt?fields=id,name,email,birthdate HTTP/1.1
Host: https://YOUR_DOMAIN
Authorization: Bearer YOUR_ACCESS_TOKEN

{
 "birthdate": "1981-10-13",
 "nickname": "Johnny"
}
```

Example Response

```
{
 "id": "AVqvOB58Fg6nZfQ0ZqXt",
 "name": "John Doe",
 "email": "johndoe@example.com",
 "birthdate": "1981-10-13"
}
```

3.5 Firewall Requirements

No firewall changes are required.

4. Data Storage

4.1 Availability

The ReachFive platform is designed to be up at any time.

4.2 Support

The following people should be contacted in case bug fixes or improvements are needed for this component:

Name	Role	Email
Guillaume Partenet	ReachFive Customer Success Manager	guillaume@reach5.co
Jose Diago	Salesforce Commerce Cloud Technical Architect	jdiago@salesforce.com
Aristide Okalla	Salesforce Commerce Cloud Technical Architect	aokalla@salesforce.com

5. User Guide

5.1 Roles, Responsibilities

The roles and responsibilities are shared among ReachFive and the merchant as described in the following table:

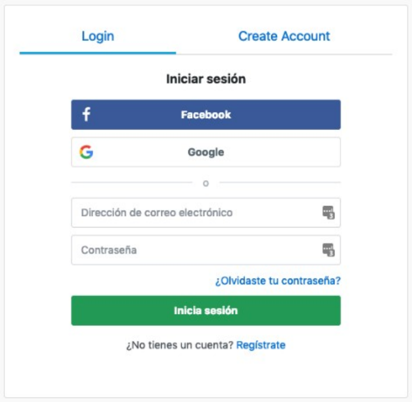
Who	Role & responsibilities
ReachFive	- Provide to the merchant the information required to connect to the ReachFive API : APISecret / APIKey - Provide and maintain the merchant's ReachFive platform.
Merchant	- Integrate the int_reachfive cartridge in the code version of its site following the documentation. - Subscribe to the ReachFive service.

5.2 Storefront Functionality

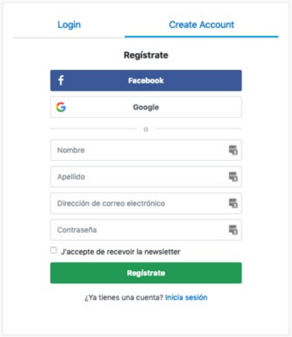
The int_reachfive_sfra cartridge generates social connect buttons on the login and registration page of SFRA. If Providers are configured in reachFive console then their social connect buttons will be added to the form. The following screenshots illustrates what it looks like with the default ReachFive template :

Case SSO Screen Shot

Login:

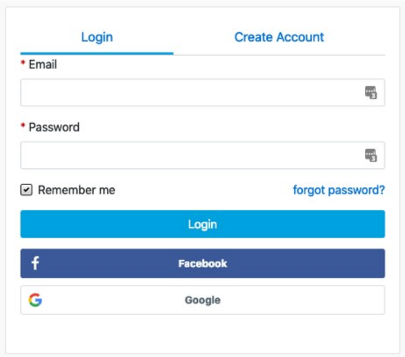

Login
Create Account
Iniciar sesión
Facebook
Google
o
Dirección de correo electrónico
Contraseña
¿Olvidaste tu contraseña?
Inicia sesión
¿No tienes un cuenta? Regístrate

Register:


Login
Create Account
Regístrate
Facebook
Google
o
Nombre
Apellido
Dirección de correo electrónico
Contraseña
□ J'accepte de recevoir la newsletter
Regístrate
¿Ya tienes una cuenta? Inicia sesión

Case Social Login

Login:



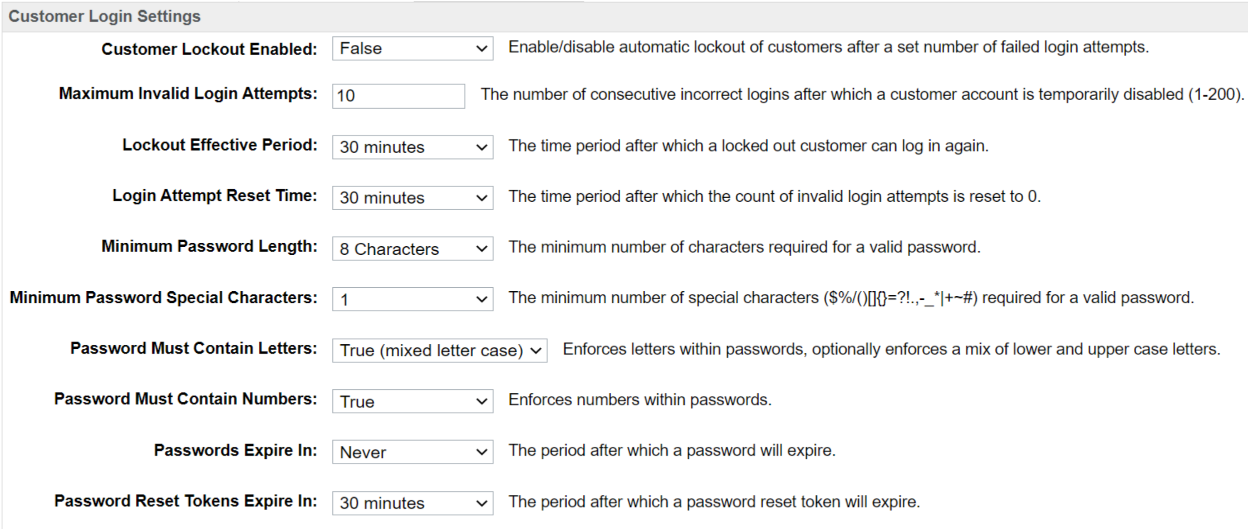
On the first register / login with a social connect provider, an OAuth provider page appears, asking for the user acceptance of data sharing.
On the acceptance of this terms, the user is logged in and then redirected to the My Account page or on the shipping address page, depending if the user was in the middle of the checkout process or not.

6. Known Issues

6.1 Password criteria sincronization

Since both systems have separately configurable password complexity policies, you need to make sure that they match. Otherwise, it may result in an error during user creation on the Reachfive side in transition mode.

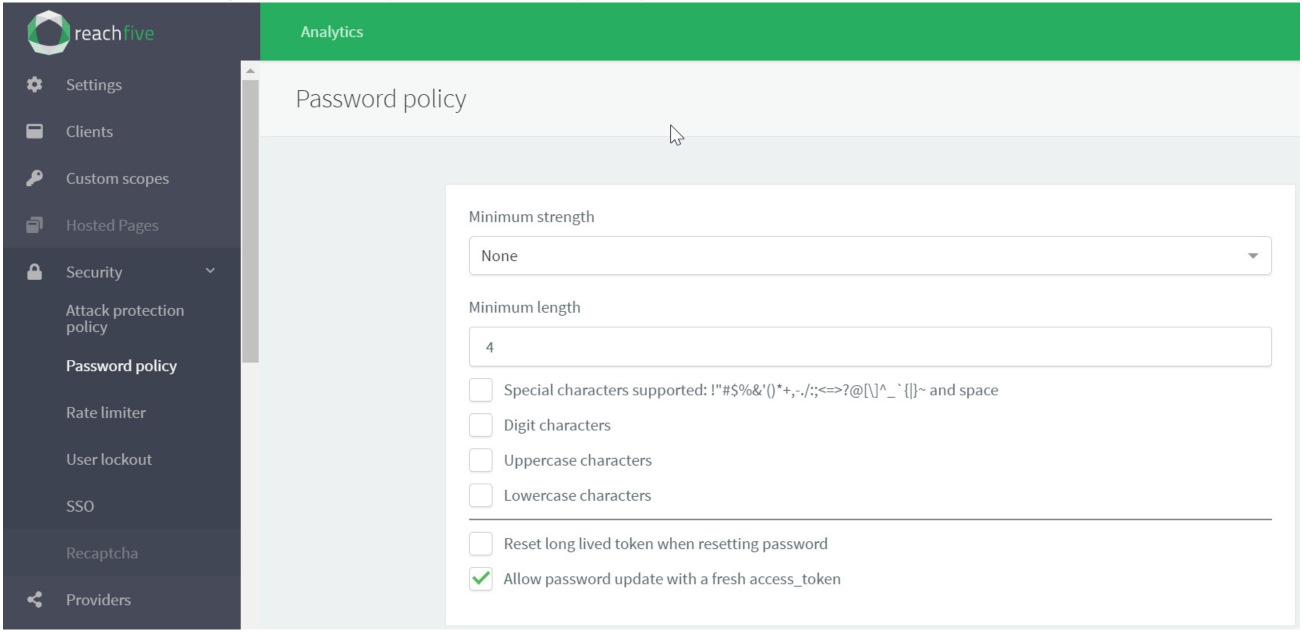
Salesforce: Administration → Sites → Customer Lists → RefArch



Customer Login Settings

Customer Lockout Enabled:	False	Enable/disable automatic lockout of customers after a set number of failed login attempts.
Maximum Invalid Login Attempts:	10	The number of consecutive incorrect logins after which a customer account is temporarily disabled (1-200).
Lockout Effective Period:	30 minutes	The time period after which a locked out customer can log in again.
Login Attempt Reset Time:	30 minutes	The time period after which the count of invalid login attempts is reset to 0.
Minimum Password Length:	8 Characters	The minimum number of characters required for a valid password.
Minimum Password Special Characters:	1	The minimum number of special characters ($%/()[]{}=?!.,-_*|+~#) required for a valid password.
Password Must Contain Letters:	True (mixed letter case)	Enforces letters within passwords, optionally enforces a mix of lower and upper case letters.
Password Must Contain Numbers:	True	Enforces numbers within passwords.
Passwords Expire In:	Never	The period after which a password will expire.
Password Reset Tokens Expire In:	30 minutes	The period after which a password reset token will expire.

Reachfive: Settings → Security → Password policy



Password policy

Minimum strength

None

Minimum length

4

□ Special characters supported: !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ and space

□ Digit characters

□ Uppercase characters

□ Lowercase characters

□ Reset long lived token when resetting password

☑ Allow password update with a fresh access_token

6.2 Phone validation

Reachfive performs phone validation based on Google's common Java, C++ and JavaScript library (https://developer.reachfive.com/docs/validating-phone-numbers.html), this can cause some difficulties in syncing phone numbers on the Salesforce side and Reachfive, which can be reflected in an error that occurs when you can't save a profile through a Salesforce form. Since, apart from this validation library, there is another intermediate step that verifies phone numbers, the error may not be representative enough and indicate an incorrect phone number format.
At the current level of development, the French phone number format is used.

7. Failover and recovery process

During emergencies like platform or service down situations, merchants disable the cartridge features from custom site preferences. This will enable the users to connect or register through native SFCC functionalities.

8. Release History

Version	Date	Changes
19.1.0	September 2019	Initial SFRA version
20.2.0	April 2020	Add ReachFive Profiles Synchronization Job Synchronization newsletter consent when reachFive account is created on SFCC
20.3.0	July 2020	Use synchronous web SDK: identity-ui@1.6.0, identity-core@1.15.0
20.4.0	Feb 2023	- Transition cartridge mode added - Reachfive SSO session maintain added - Reachfive webhook maintain added - no changes required for “app_storefront_base” cartridge - SFCC scripts initialization based on SFCC hook “app.template.afterFooter”
20.4.1	Apr 2023	- Email update added - Phone update added
20.4.2	May 2023	- JQuery dependencies removed from cartridge - Reworked approach to saving data to Salesforce session, added models for Reachfive responses. - Added the ability to change the password regardless of the current type of Reachfive authorization