

SSO Integration Using SavvyMoney REST API

Version	Revised On	Changes
Version 1.0	Aug 10, 2018	
Version 1.4	Aug 13, 2019	Updated SSO user attribute information
Version 1.5	Nov 12, 2019	Added API Server Connection section
Version 1.6	Jun 19, 2020	Updated endpoints with static domain
Version 1.7	Jul 24, 2020	Updated Security section with TLS cipher information
Version 1.8	Oct 12, 2020	Updated with additional static IP address for production after infrastructure change
Version 1.9	Jan 20, 2021	Updated with information about Attribute Encryption
Version 2.0	Jul 14, 2022	Updated Supplemental Attribute examples
Version 2.1	Aug 8, 2022	Add SSO application endpoints

Introduction

This document provides technical specifications of Single Sign On (SSO) integration using SavvyMoney's REST API. This solution provides our Partners' end users, access to SavvyMoney's products and website without creating separate login credentials. Integration with SavvyMoney requires using SavvyMoney's APIs created specifically for establishing SSO.

SavvyMoney APIs use the JSON Web Tokens (JWTs) technology for Single Sign On (SSO) authentication and authorization. This document gives an overview of the SSO authorization scenarios that SavvyMoney supports.

Rules for Single Sign On

1. SavvyMoney's SSO will be a stand-alone application.
 - a. Session management will remain independent between SavvyMoney and the partner. The Partner's online banking session may not be kept active while the end user is engaged with SavvyMoney's website.
 - b. When a member is transferred from the Partner's online banking session to SavvyMoney website, SavvyMoney will create a new session, which will remain active until the end user is logged out.
 - c. Once the identity details passed by the partner are validated by SavvyMoney, the member will be shown the appropriate portion of the website.
 - d. There will be no reverse session exchange from SavvyMoney back to the Partner. A member who has been timed out of the SavvyMoney website will have to log into the online banking platform again to access SavvyMoney.
2. SavvyMoney will provide the Partner with a Partner ID, which will be used every time the Partner transmits a new session to SavvyMoney.
3. Security
4.
 - a. Confidentiality - data can be viewed only by the intended recipients. This will be accomplished by using HTTP over SSL.
 - b. Data integrity - data cannot be altered without detection. This is accomplished by issuing JSON Web Tokens encrypted by SavvyMoney.
 - c. Data origin authentication - data recipient will authenticate the claimed originator. This is accomplished by specifying limited "Audience Domains" associated with each API user.
 - d. Trust - SavvyMoney will provide partner with a set of user credentials so that both parties have a high degree of assurance that security requirements (encryption, data integrity, authentication) are being met.

Rest API Server Connection:

- SavvyMoney supports only TLS 1.2 SSL. We do not support the following weak ciphers on both our Beta and Production environments:
 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
 - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)
 - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)
 -
- Clients will need to whitelist SavvyMoney domains/static IPs for Beta (Test) and Production environments respectively to access SavvyMoney servers from the client servers.
 - PRODUCTION : creditscore.savvymoney.com
 - IP Address: 3.227.227.11
 - IP Address: 3.222.59.58
 - TEST/BETA : creditscoretest.savvymoney.com
 - IP Address: 18.210.174.44
 - IP Address: 75.101.165.109
- SavvyMoney does not require server whitelisting as it is open to the public.

Integration Steps

To begin, the partner must obtain user credentials from SavvyMoney. Partner's application requests an access token from the SavvyMoney SSO server, extracts a token from the response, and sends the token to the SavvyMoney API.

All applications follow a basic pattern when accessing SavvyMoney API. At a high level, here are the steps:

1. Obtain API user credentials from SavvyMoney

SavvyMoney provides SSO API user credentials such as an Authentication ID (Auth ID) and Authentication Key (Auth Key) that are known only to SavvyMoney and partner's application. The settings associated with the API user should include:

- Auth ID : client identifier
- Auth Key: authentication key in JWT format
- Audience Domains: SavvyMoney domains or client Credit Score sub-domains hosted by SavvyMoney
- Partner ID List: Partner IDs that the API user are authorized for SSO integration
- AES/CBC Encryption Key: encryption key for AES/CBC encryption of member attributes

2. Obtain an access token from the SavvyMoney SSO Server

Before the partner's application can access member's credit data, it must obtain an **access token** that grants access to SavvyMoney API. A single access token can grant varying degrees of access to multiple APIs. However, before getting the access token authentication is required.

Client application needs to send an **authentication** request with provided API user credentials and member attributes to SavvyMoney SSO server. This request should be made from client application server and not from the user's web browser. If the request is valid, SavvyMoney SSO server sends the partner application a short-lived authorization code (in JWT format) that the application can use to obtain an access token. If the request is invalid, the server returns an error. Optionally for enhanced security, the partner's application can obtain a browser "Fingerprint" from SavvyMoney SSO Server that can be used to restrict access to the REST API from the same user browser. This request should be made from the web browser.

Finally, to obtain an access token, the client application needs to send a **sign-on** request with the provided authorization code and optional fingerprint from the Internet Browser.

3. Send access token to SavvyMoney API

After an application obtains an access token, it sends the token to a SavvyMoney API in an HTTP authorization header.

Note - Access tokens are restricted to access the set of partners from the set of audience domains described in the SSO client credentials.

4. Prolong the access token, if necessary

Access tokens have limited lifetimes. If partner's application needs access to a SavvyMoney API beyond the lifetime of an access token, a prolong request to SavvyMoney SSO server should be made.

5. Log off access token

Make a logoff request to SavvyMoney SSO server in order to log off the access token immediately. Otherwise, the access token will automatically expire in 10 minutes.

SSO User Attributes

Partner application can exchange the following SSO user attributes in the SSO authentication API:

Name (Case Sensitive)	Description	Format	Required	Encryption	Sample value
partnerId	Unique identifier of the partner assigned by SavvyMoney.	Alphanumeric	Yes	False	201
partnerMemberId	Unique immutable member identifier of the SSO user in the partner's system. This is case sensitive. Note: Cannot be the SSN of the user	Numeric or alphanumeric	Yes	True*/ False	123456789 or ABC123
firstName	SSO user's First name	Alphanumeric	No	True*/ False	John
lastName	SSO user's Last name	Alphanumeric	No	True*/ False	Malkovich
email	SSO User's Contact Email address used to send score updates and monitoring notifications	Valid email address	No	True*/ False	john.malkovich@partner.me
address1	SSO user's main address line 1	Alphanumeric	No	True*/ False	323 North Lake Ave.
address2	SSO user's main address line 2	Alphanumeric	No	True*/ False	Apt. 1030
city	SSO user's city of residence	Alphanumeric	No	True*/ False	Florenceville
state	SSO user's State of residence. US State	Format - 2 letter abbreviation	No	True*/ False	CA or TX
zip	SSO user's Zip code US Zip code	Format - XXXXX Only 5 digits	No	True*/ False	94588
dob	SSO user's date of birth	Date format - MMDDYYYY (Numeric, no dashes or slashes)	No	True*/ False	04181950
ssn	SSO user's Social Security Number Format - 9 digits - no dashes	Format - XXXXXXXXX (Numeric, no dashes)	No	True*/ False	999999990
supplemental1	Used to pass additional information associated with the user. Examples - membernumber for Loan applications, information about a segment of members, the organization a member belongs to. Note: Prior to using supplemental attributes the value and format should be discussed with SavvyMoney.	Format: "name:value"	No	True*/ False	"MemberIdentifier":"ABC123-6789"
supplemental2	Supplemental attribute #2	Format: "name:value"	No	True*/ False	Organization:Costco
supplemental3	Supplemental attribute #3	Format: "name:value"	No	True*/ False	SEG:Retail

**True - If encryption is set to true, follow the steps in "Attribute Encryption Guide" to encrypt the attributes correctly.*

Integration Scenarios

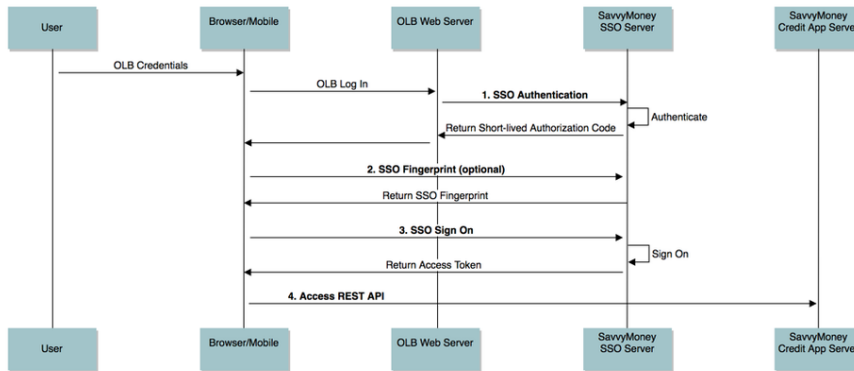
Note: The first SSO Authentication API call should be made from OLB web server. OLB may require to whitelist SavvyMoney SSO server IP addresses on their firewall.

1. REST API in Web application

SavvyMoney can be integrated in a partner's application through the use of REST APIs provided. This approach is common in mobile integration but can also be used in a desktop application.

SavvyMoney SSO server endpoint supports web applications that use common languages and frameworks such as PHP, Java, Python, Ruby, and ASP.NET.

The authorization sequence is described in this diagram:

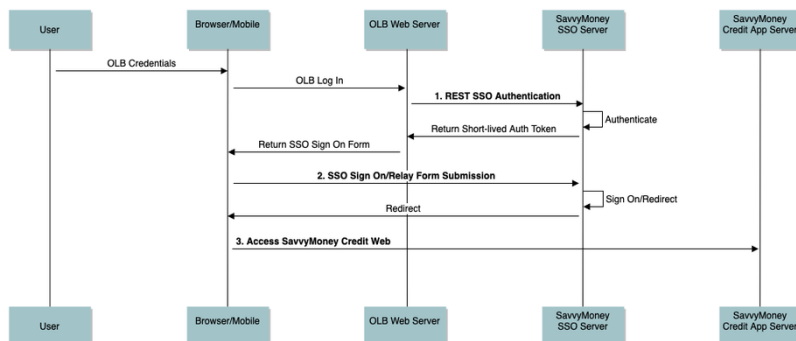


1. SSO Authentication API
2. SSO Fingerprint API (optional)
3. SSO Sign On API
4. Credit REST API

2. iFrame in Web Application

SavvyMoney UI (widget) can be embedded in a partner's application using an iFrame. This approach is common in desktop integration.

The authorization sequence is described in this diagram:

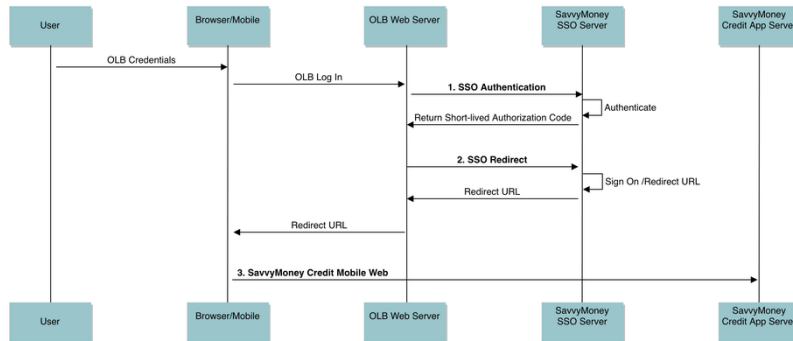


1. SSO Authentication API
2. SSO Sign On/Relay Form POST
3. Redirect to Credit Web

3. Mobile Web Application

SavvyMoney mobile UI can be launched with a redirect URL.

The authorization sequence is described in this diagram:



1. SSO Authentication API
2. SSO Redirect API
3. Redirect to Credit Mobile web

SavvyMoney Integration Application Endpoints

The value of “**appUrl**” in Redirect API, and “**AuthAppUrl**” in Relay Form Submission(RelayPost) is used to set SavvyMoney application to be launched after SSO integration. Here are some examples in SavvyMoney beta/test environment:

- Regular widget: <https://creditscoretest.savvymoney.com/ui/widget-ss0>
- Desktop dashboard: <https://creditscoretest.savvymoney.com/ui/sso>
- Mobile dashboard: <https://creditscoretest.savvymoney.com/ui/mobile-ss0>
- Mobile widget: <https://creditscoretest.savvymoney.com/ui/mobile-widget-ss0>
- Score widget: <https://creditscoretest.savvymoney.com/ui/score-widget-ss0>
- Offer widget: <https://creditscoretest.savvymoney.com/ui/offer-widget-ss0>

Sample REST API Code

Server Side - SSO APIs:

1. SSO Authentication API

Request JSON Model

```
1 {
2   "authId" : "<Auth User ID>",
3   "authKey" : "<Auth Key>",
4   "domain" : "<SavvyMoney Application Domain>",
5   "attributes" : [ {
6     "key" : "partnerId",
7     "value" : "992",
8     "encrypted" : false
9   }, {
```

```
10     "key" : "partnerMemberId",
11     "value" : "ac1oJqHnAk3HxbVwMwtYw==",
12     "encrypted" : true
13 }, {
14     "key" : "firstName",
15     "value" : "QtSIJrPy1KwPVU3jBWPgjQ==",
16     "encrypted" : true
17 }, {
18     "key" : "lastName",
19     "value" : "UD9phxcc0QIPUcoxBXqShw==",
20     "encrypted" : true
21 }, {
22     "key" : "email",
23     "value" : "3SGotQAMWVvH6nH6+a7Fj00LqCrbJXHHouqmQAJv7/EfmkKYzdEB2h80IJqEMeu1",
24     "encrypted" : true
25 }, {
26     "key" : "address1",
27     "value" : "+1D2STL4x2RtdtMsmPKr+g==",
28     "encrypted" : true
29 }, {
30     "key" : "city",
31     "value" : "tJiIMLV4bTUpYs+ACnYeXQ==",
32     "encrypted" : true
33 }, {
34     "key" : "state",
35     "value" : "j8KNBKeEGUK9CDRX3ngkww==",
36     "encrypted" : true
37 }, {
38     "key" : "zip",
39     "value" : "KLfWVdL1HbELogYfAyBt+g==",
40     "encrypted" : true
41 }, {
42     "key" : "dob",
43     "value" : "LFbUeBj0bjx+MHbAhrGIHA==",
44     "encrypted" : true
45 }, {
46     "key" : "ssn",
47     "value" : "09g15YgZne2MNhI/p7vj3A==",
48     "encrypted" : true
49 }, {
50     "key" : "supplemental1",
51     "value" : "Gaejq5h693u6jU14fzXNYw==",
52     "encrypted" : true
53 }, {
54     "key" : "supplemental2",
55     "value" : "41zA1TbElwj2g/dGZ0dtoQ==",
56     "encrypted" : true
57 }, {
58     "key" : "supplemental3",
59     "value" : "uzujGFB0XhF+m/9A0zMgpg==",
60     "encrypted" : true
61 } ]
62 }
63
64
```

Response body

```
1 {  "hasErrors": false,  "authCode": "<Authorization Code>",  "notBeforeTime": "2018-05-14T14:34:51.047-04:00",
```

2. SSO Redirect API Without Browser Fingerprint

Request JSON Model

```
1 {
2   "authCode": "<Authorization Code>",
3   "appUrl": "<SavvyMoney Credit App URL>"
4 }
5
```

Response body

```
1 {
2   "hasErrors": false,
3   "accessToken": "<Access Token>",
4   "expirationTime": "2018-12-03T18:50:51.101Z",
5   "redirectUrl": "<SavvyMoney Credit App URL with smtoken>"
6 }
```

JavaScript inside Browser:

1. SSO Fingerprint API

Response body

```
1 {  "hasErrors": false,  "fingerprint": "<Fingerprint>" }
```

2. SSO Sign On API With Browser Fingerprint

Request JSON Model

```
1 { "authCode": "<Authorization Code>", "fingerprint": "<Fingerprint>" }
```

CURL Command:

```
1 curl -X POST "https://creditscoretest.savvymoney.com/sso/api/rest/signon" -H "accept: */*" -H "Content-Type: appl
```

Response body

```
1 {  "hasErrors": false,  "accessToken": "<Access Token>",  "expirationTime": "2018-05-14T12:29:04.015-07:00" }
```

3. SSO Prolong API

CURL Command:

```
1 curl -X POST " https://creditscoretest.savvymoney.com/sso/api/rest/prolong" -H "accept: */*" -H "Authorization: <
```

Response body

```
1 {  "hasErrors": false,  "expirationTime": "2018-05-14T12:59:24.082-07:00" }
```

4. SSO Log Off API

CURL Command:

```
1 curl -X POST " https://creditscoretest.savvymoney.com/sso/api/rest/logoff" -H "accept: */*" -H "Authorization: <
```

Response body

```
1 {   "hasErrors": false,   "loggedOff": true }
```

iFrame Widget HTML Code

```
1 <form id="ssoForm" name="ssoForm" method="POST" action="https://creditscoretest.savvymoney.com/sso/api/RelayPost
2 <input id="AuthCode" name="AuthCode" type="hidden" value="<Authorization Code>">
3 <input id="AuthAppUrl" name="AuthAppUrl" type="hidden" value="https://creditscoretest.savvymoney.com/ui/widget-s
4 </form>
5 <iframe name="savvy_iframe" id="savvy_iframe" width="400px" height="500px"></iframe>
6 <script>
7     $(document).ready(function() {
8         $('#ssoForm').submit();
9     });
10 });
11 </script>
```

This document describes SavvyMoney's REST API solution, and should not be reproduced, copied, transformed or adopted in any form or means without the prior permission of SavvyMoney, Inc.