API Workflow: Customer Password Reset

Table of Contents

Summary

SessionM supports a client reaching out to a customer with a password reset email and then resetting, or changing, their password. This workflow documents the steps that enable this process.

Use Cases

The need to reset a password can derive from a variety of different contexts. For example, you may need to migrate your customer's password from an external system to your own; or, your customer may simply have forgotten their password. These use case steps are typical for clients resetting their customers' passwords:

- Search for customer.
- Use internal ID of found customer to send them a password reset email.
- Customer uses email to access password reset site and reset password.
- Customer ignores email, fails in login attempt and then accesses password reset site from a "Forgot Password" link.

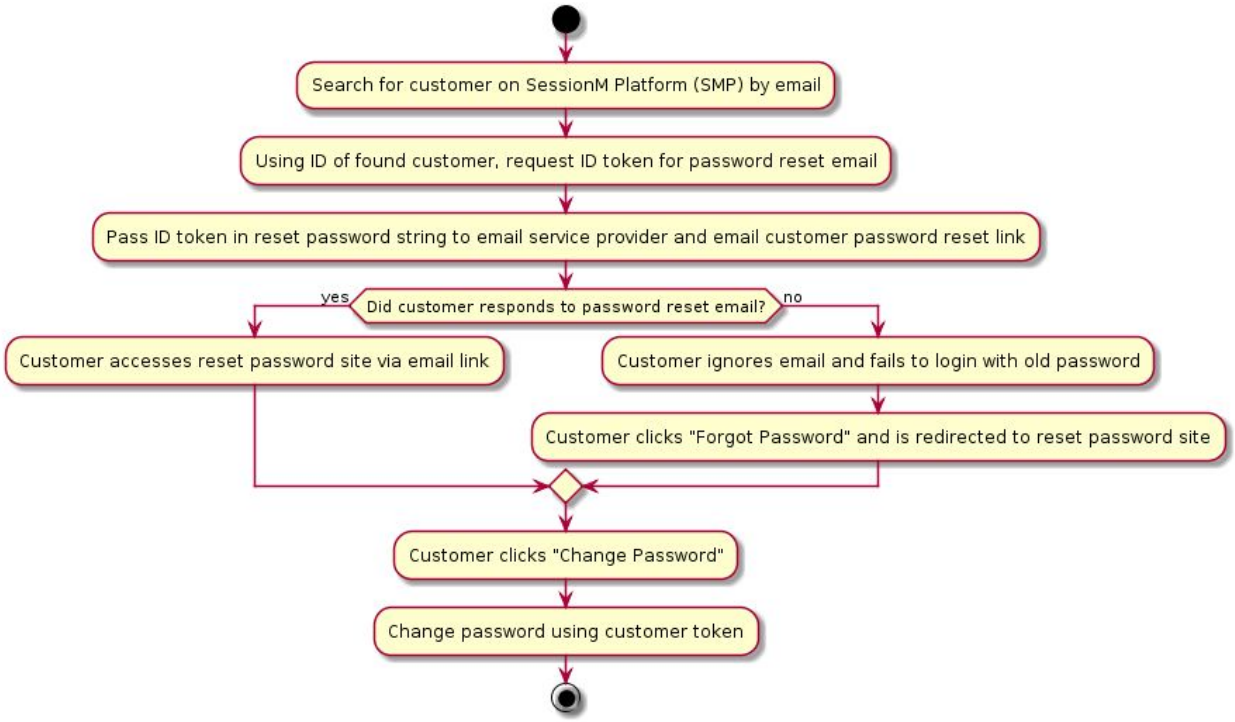
Data Configuration Prerequisites

This workflow presumes the client has performed the following tasks before it can be implemented for password resets:

- Creates and hosts a password reset site that customers can access.
- Sets up server to implement the SessionM S2S APIs.
- Customer's email is known.

Step by Step

The workflow describes sending a password reset email and then resetting, or changing, the password. It follows the step-by-step decision tree diagrammed below:



The workflow for sending a customer a password reset email and then actually resetting the password follows the step-by-step decision tree diagrammed below:

When issuing curl commands for platform transactions, adhere to the following syntax:

- Begin each curl command with either `POST` or `GET`.
- Specify: `-H 'Content-Type: application/json' -H 'authorization: Basic AUTH_ID'`
- Begin URL with same endpoint + API key: `https://[ENDPOINT]/priv/v1/apps/API_KEY`

Step 1: Lookup the Customer by Email

The first step in this workflow is to lookup, or search for, the customer based on their email address. Using the Standard Profile API, specify this endpoint to search for the customer:

```
GET /priv/v1/apps/:api_key/users/search?email=test@example.com
```

After the endpoint makes the request for the query, the platform returns a response object, which is shown below:

Response


```
{
      "status": "ok",
      "user": {
            "id": "e76fc440-d7f0-11e8-91e4-469b02598280",
            "external_id": "88888888",
            "opted_in": true,
            "activated": false,
            "proxy_ids": [],
            "email": "zzz@example.com",
            "gender": "m",
            "dob": "1980-01-01",
            "created_at": "2018-10-25 00:57:11",
            "updated_at": "2018-10-25 00:57:11",
            "address": "7 Tremont Street",
            "city": "Boston",
            "zip": "02021",
            "dma": "506",
            "state": "MA",
            "country": "USA",
            "suspended": false,
            "last_name": "Smith",
            "first_name": "ZZ",
            "registered_at": "2018-10-25 00:57:10",
            "profile_photo_url": "/images/account-neutral.png",
            "test_account": false,
            "account_status": "good",
            "tier_levels": [],
            "referrer_code": "ZZS-B27C94",
            "phone_numbers": [{
                  "phone_number": "1234123123",
                  "phone_type": "home",
                  "preference_flags": ["primary"],
                  "verified_ownership": false
            }]
      }
}
```

This response contains an ID for the customer returned by the query, *e76fc440-d7f0-11e8-91e4-469b02598280*. You can include this value as a parameter for the endpoint that sends the password reset email and resets, or changes, the password.

Step 2: Request an ID Token to be Used in the Reset Password Email

The next step in the workflow is sending a request to the SessionM server to generate the ID token you need to compose a reset password email. Using the Identity Services API, specify the following endpoint:

```
POST
/priv/v1/apps/:api_key/users/e76fc440-d7f0-11e8-91e4-469b02598280/perform
```

This endpoint specifies the user ID that was acquired from the customer search in the previous step and the endpoint passes in this request object:

Request

```
{
    "sendPasswordResetEmail":{
        "email":"test@example.com",
        "send_email":false
    }
}
```

The request contains the email address for the customer as well as whether or not you or SessionM is actually sending the email. This workflow supports having you, the client, send the email. As such, the *send_email* attribute is set to “false”, thereby allowing you - in conjunction with your email service provider - to send the email out manually.

After the endpoint makes the request for sending a password reset email, the platform returns a response object, which is shown below:

Response

```
{
      "status": "ok",
      "user": {
            "send_email": false,
```

```
            "verification_string":
"RmdTUWhUU0dSMkJVQTRqUGF1MG9tSS8zY0pya2thNE9kS0hvbTM4OFl2cz0tLXRzYUhoZHE4TFIxc
jhEMlNKbjlhRjd1b0diOWswbXZFTmY0bER2cnFseW9PcW1lZFJlM2Y1MWdlWHRsV0x1YWRSaXN5V3V
GanhVQjVXQmVQN0dxSk8wcWY2YXhZQ1pJbzVSOFJ4Z2hFa0xtUzFCWE9sNWl4NW5XL1RiVWp4NzF3Z
HUwdE5BPT0=",
            "reset_link":
"https://login-economy.stg-sessionm.com/c6b7e6f1ea04f6ad3e57cb84059865dfb0555b
33/accounts/reset_password?token=RmdTUWhUU0dSMkJVQTRqUGF1MG9tSS8zY0pya2thNE9kS
0hvbTM4OFl2cz0tLXRzYUhoZHE4TFIxcjhEMlNKbjlhRjd1b0diOWswbXZFTmY0bER2cnFseW9PcW1
lZFJlM2Y1MWdlWHRsV0x1YWRSaXN5V3VGanhVQjVXQmVQN0dxSk8wcWY2YXhZQ1pJbzVSOFJ4Z2hFa
0xtUzFCWE9sNWl4NW5XL1RiVWp4NzF3ZHUwdE5BPT0="
      }
}
```

This response contains the *reset_link*, which contains the *verification_string* in the link, or URL, to the password reset site.

Step 3: Send Reset Password Email to the Customer

Now you can send the customer a reset password email message that contains a reset link returned in the previous step. Using that link, the customer can reset their password. However, this is not always the case: the customer doesn't always respond to the email. For more information on how the workflow accounts for this possibility, proceed to the next step.

Step 4: Determine if the Customer has Responded to the Email

This workflow begins with determining whether your customer has responded to the email sent to them or has ignored it.

If they have responded to it, they can access the reset password site via the link sent to them in the email.

If they have ignored it, they are likely to attempt a login with the old password and fail. At that point, the customer can click "Forgot Password" and be redirected to the reset password site.

Once they have access the site, the process for actually resetting the password can begin, as shown in the next step.

Step 5: Change the Customer Password

The next step in the workflow is changing the password on the reset password site. Using the Identity Services API, specify the following endpoint:

```
POST
/priv/v1/apps/:api_key/users/e76fc440-d7f0-11e8-91e4-469b02598280/perform
```

This endpoint specifies the user ID acquired from the search query that located the customer, and it passes in this request object to do the actual password change:

Request


```
{
    "updatePassword":{
"token":"RmdTUWhUU0dSMkJVQTRqUGF1MG9tSS8zY0pya2thNE9kS0hvbTM4OFl2cz0tLXRzYUhoZHE4TFIxcjhEMlNKbjlhRjd1b0diOWswbXZFTmY0bER2cnFseW9PcW1lZFJlM2Y1MWdlWHRsV0x1YWRSaXN5V3VGanhVQjVXQmVQN0dxSk8wcWY2YXhZQ1pJbzVSOFJ4Z2hFa0xtUzFCWE9sNWl4NW5XL1RiVWp4NzF3ZHUwdE5BPT0=",
        "password":"Password1"
    }
}
```


Like the *verification_string* and the *reset_link*, this request includes the ID token; it also includes the password necessary to execute the password reset.

After the endpoint makes the request for the password change, the platform returns a response object, which is shown below:

Response


```
{
      "status": "ok",
      "user": {}
}
```