instalogin

INSTALOGIN IMPLEMENTATION GUIDE

VERSION 1.3.1

INSTALOGIN IMPLEMENTATION GUIDE

VERSION 1.3.1

INTRODUCTION

Below is a quick guide how to integrate Instalogin in your project to test it easily. We are preparing a comprehensive documentation covering all possible use cases and parameters.

PREREQUISITES

To use the Instalogin API you'll be provided a Key and a Secret, which will be used to authenticate at our API.

```
KEY=0O0Nc2E0mCo5CE3FRi0ArTi3b7I3RYzU
SECRET=89a203b3e6e56008e4bf3fb2305e973ed1f7c7d93e9b53d4015d227a47fbdbdb
```

Note: Example data

INSTALOGIN API

We use signed Json Web Tokens (JWT) for API authentication. To provide maximum security, we also use additional claims related to the request.

The following example request:

```
POST /v1/entity/provision HTTP/1.1
Content-Type: application/json; charset=utf-8
...
{"sendEmail":true,"identifier":"john.doe@example.com"}
```


Insta Holding AG
Grafenaustraße 15
6300 Zug
Switzerland

E-Mail hello@insta.ag
Web www.instalog.in

Migros Bank AG
BIC MIGRCHZZXXX
IBAN CHF CH75 0840 1000 0600 9085 5
IBAN EUR CH70 0840 1000 0601 0326 4

Umsatzsteuer ID: CHE-225.541.833

would require a JWT with a structure similar to this:

```
// Header:
{
  "typ": "JWT",
  "alg": "HS256"
}
// Claims
{
  "iss": "0O0Nc2E0mCo5CE3FRi0ArTi3b7I3RYzU", // API Key
  "aud": "api.instalog.in",                  // API Host
  "iat": 1577833201,                         // Unix Timestamp (seconds since Jan 01 1970)
  "method": "POST",                          // Request method, in upper letters
  "url": "/v1/entity/provision",             // API endpoint
  // The bodyHash below is a SHA256 hash of the request body in the example request
  "bodyHash": "61288241900d4ed0e545a4af4d0f3e433ae91840f0b5cbc9e73765a3ac4ea71e"
}
```

Note: These are the minimum claims required by the Instalogin API

This JWT needs to be signed with the API secret provided by Instalogin.

Please notice, you need to use the byte representation of the hex secret provided, to use it as a HMACSHA256 parameter. See the following .NET example:
How do you convert a byte array to a hexadecimal string, and vice versa?

Then simply add the signed JWT as an authorization header inside the request:

```
POST /v1/entity/provision HTTP/1.1
Content-Type: application/json; charset=utf-8
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOweqwe2241dgweiIw2324ew23qd ...
{"sendEmail":true,"identifier":"john.doe@example.com"}
```


Insta Holding AG
Grafenaustraße 15
6300 Zug
Switzerland

E-Mail hello@insta.ag
Web www.instalog.in

Migros Bank AG
BIC MIGRCHZZXXX
IBAN CHF CH75 0840 1000 0600 9085 5
IBAN EUR CH70 0840 1000 0601 0326 4

Umsatzsteuer ID: CHE-225.541.833

PROVISIONING

Before a user account can be used with the Instalogin app, it needs to be provisioned. The easiest way to provision an account with Instalogin is to send the user an email with a provisioning QR Code inside. A good starting point could be a "Provision with Instalogin" button somewhere in the protected frontend or administration backend, which triggers the following API call in the backend (simplified view):

```
POST /v1/entity/provision HTTP/1.1
{
  "sendEmail": true, // Let Instalogin send the Provisioning QR Code
  "identifier": "john.doe@example.com"
}
```

If for any reasons the account identifier is not an email address, where the QR Code can be send to, use the alternative way:

```
POST /v1/entity/provision HTTP/1.1
{
  "sendEmail": "john.doe@example.com", // Let Instalogin send the Provisioning QR Code
  "identifier": "john.doe" // Or any internal ID etc.
}
```

The response is a provisioning token with a response status of either 201 (Created) or 200 (Ok, in this case updated), and will look something like this:

```
{
  "id": "1d5e36b89c",
  "createdAt": "2020-02-25T08:26:50+00:00",
  "expiresAt": "2020-02-25T09:26:50+00:00",
  "identity": {
    "id": "0aa249e2-94ca-4bb2-89cf-bc3a329f4aac",
    "createdAt": "2020-02-21T10:16:11+00:00",
    "enabled": true,
    "identifier": "john.doe@example.com",
    "devices": []
  }
}
```


Insta Holding AG
Grafenaustraße 15
6300 Zug
Switzerland

E-Mail hello@insta.ag
Web www.instalog.in

Migros Bank AG
BIC MIGRCHZZXXX
IBAN CHF CH75 0840 1000 0600 9085 5
IBAN EUR CH70 0840 1000 0601 0326 4

Umsatzsteuer ID: CHE-225.541.833

This API call simply creates or uses an existing identity inside the Instalogin system, and sends out an email with a provisioning QR Code that needs to be scanned with the Instalogin app. Once done, the provisioning is completed, and the user is ready to authenticate using the Instalogin app.

AUTHENTICATION

The authentication process involves two parts. The first part is about displaying the authentication image (QR Code / Smart Image) on the login page. The second part is about processing the authentication from Instalogin.

FRONTEND

Add the following few lines to your HTML frontend to show the Instalogin image used for authentication.

```
<!-- Place this HTML node wherever the Instalogin image should appear -->
<div id="instalogin"></div>

<!-- Load the JavaScript library asynchronously (non-blocking) and configure it -->
<script async id="instalogin-js" src="https://cdn.instalog.in/js/instalogin.js"></script>
<script>
    // Wait until the script has been loaded
    document.getElementById("instalogin-js").addEventListener("load", function() {
        new Instalogin.Auth({
            key: "0O0Nc2E0mCo5CE3FRi0ArTi3b7I3RYzU",       // The API key
            authenticationUrl: "/path/to/login-controller" // Your authentication controller
        }).start();
    });
</script>
```


Insta Holding AG
Grafenaustraße 15
6300 Zug
Switzerland

E-Mail hello@insta.ag
Web www.instalog.in

Migros Bank AG
BIC MIGRCHZZXXX
IBAN CHF CH75 0840 1000 0600 9085 5
IBAN EUR CH70 0840 1000 0601 0326 4

Umsatzsteuer ID: CHE-225.541.833

PROCESSING THE AUTHENTICATION

The authenticationUrl controller configured in the JavaScript snippet will receive a signed JWT inside the authorization header. A request to this controller will look something like:

```
GET /path/to/login-controller HTTP/1.1
Accept: application/json
X-Requested-With: XMLHttpRequest
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOweqwe2241dgweiIw2324ew23qd ...
```

The first thing that needs to be done inside the controller is to extract the JWT from the header and validate it with any JWT utility class using the API secret. Once done, you can retrieve three important claims from the token:

```
{
  "jti": "jLRyLyhK1tGf6S0TSuXcOEG3qvZ5CriX",  // Challenge Id
  "sub": "john.doe@example.com",              // Identifier
  "otp": "1c7eab97"                           // One Time Password
}
```

The next step is to use your own internal logic and check if the user with the identifier from the JWTs “sub” claim is actually in your database and enabled to login into your application.

Once the authentication attempt is verified, the final step is to check, if the passed one-time-password from the “otp” claim” was successfully signed on the Instalogin system by the identifier from the “sub” claim, and challenge from the “jti” claim:

```
POST /v1/entity/identities/john.doe@example.com/authenticate HTTP/1.1
{
  "challenge": "jLRyLyhK1tGf6S0TSuXcOEG3qvZ5CriX",
  "otp": "1c7eab97"
}
```


Insta Holding AG
Grafenaustraße 15
6300 Zug
Switzerland

E-Mail hello@insta.ag
Web www.instalog.in

Migros Bank AG
BIC MIGRCHZZXXX
IBAN CHF CH75 0840 1000 0600 9085 5
IBAN EUR CH70 0840 1000 0601 0326 4

Umsatzsteuer ID: CHE-225.541.833

Please notice, it is recommended to url-encode the “identifier” parameter when calling the authentication endpoint from the Instalogin API:

```
POST /v1/entity/identities/{identifier}/authenticate HTTP/1.1
{
  ...
}
```

The response is either a status code of 200 (Ok) or 401 (Unauthorized). At this point the user is successfully authenticated, the session can be set up and user redirected. The embedded Instalogin JavaScript handles any redirect response internally, you just have to return the appropriate redirect response (e.g., 301) with the final location from the controller.

Insta Holding AG
Grafenaustraße 15
6300 Zug
Switzerland

E-Mail hello@insta.ag
Web www.instalog.in

Migros Bank AG
BIC MIGRCHZZXXX
IBAN CHF CH75 0840 1000 0600 9085 5
IBAN EUR CH70 0840 1000 0601 0326 4

Umsatzsteuer ID: CHE-225.541.833