Authentication API Guide

Introduction

SecureAuth's Authentication API embeds the SecureAuth IdP functionality into a custom application, enabling flexible workflow configurations and user interfaces. Using a RESTful API encrypted over SSL, SecureAuth IdP can validate user IDs, passwords, PINs, soft tokens, Push-to-Accept responses, and knowledge-based answers; can generate One-time Passwords (OTPs) delivered via phone call, SMS message, email message, help desk, or Push / Push-to-Accept Notification; can analyze a user's access attempt through SecureAuth's Device / Browser Fingerprinting, Adaptive Authentication, and Behavioral Biometric profile; and can evaluate IP address risk through threat intelligence data.

Each SecureAuth IdP realm can host its own uniquely configured Authentication API, enabling various workflows and registration methods.

By simply integrating an application with SecureAuth's Authentication API, enabling Multi-Factor Authentication mechanisms, and configuring Adaptive Authentication, customers can securely direct users through unique logins and interfaces without leaving the application.

NOTE: This Authentication API Guide is specifically for SecureAuth IdP 9.0.x

Information about using Identity Management API tools can be found in the Identity Management API Guide

If using SecureAuth IdP v9.1, see Authentication API Guide and Profile Validation API Guide for information on how to configure SecureAuth Authentication API to validate end-user information and to generate OTPs for end-user authentication

See Authentication API: Send Ad hoc OTP without Existing User Profile for specific configuration steps when using ad hoc OTP delivery to users who are not registered in the directory

Prerequisites

1. Have access to the application code
2. Have an on-premises directory with which SecureAuth IdP can integrate
3. Create a New Realm or access an existing realm in which the Authentication API will be enabled

The API can be included in any realm with any Post Authentication event as long as the appropriate directory is integrated, the Registration Methods are enabled for Multi-Factor Authentication use, Adaptive Authentication settings are in place, and device fingerprinting configurations are completed (if using all features)

4. Configure the Data tab in the SecureAuth IdP Web Admin

A directory integration is required for SecureAuth IdP to pull user profile information during the login process

The Behavioral Biometrics feature only supports LDAP directory integrations, while other Authentication API features support most directory type integrations

Ensure that the Registration Methods Profile Properties (e.g. Phone 1, Email 1, etc.) are accurately mapped to directory attributes to enable Multi-Factor Authentication workflows
NOTE: Only API section steps are required; all other Web Admin steps are optional and should be performed based on the features to be implemented.

**API**

**API Key**

1. Check Enable API for this realm in the API Key section

2. Click Generate Credentials to create a new Application ID and Application Key

   The Application ID and Application Key are unique per realm

   In appearance the API key looks like it is comprised of 64 random characters, but it is actually is comprised of 32 two-character base-16 hexadecimal values

   This is important to note when using the API key to produce the HMAC hash

3. Click Select & Copy to copy the contents from the fields

   These values will be required in the HTTP Header configuration steps below
API Permissions

4. Check **Enable Authentication API** in the **API Permissions** section

Click **Save** once the configurations have been completed and before leaving the **API** page to avoid losing changes

Optional Configurations

To enable Multi-Factor Authentication...

Registration Methods / Multi-Factor Methods
### Registration Configuration

#### Phone Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone Field 1</td>
<td>Voice Only</td>
</tr>
<tr>
<td>Phone Field 2</td>
<td>Voice and SMS/Text</td>
</tr>
<tr>
<td>Phone Field 3</td>
<td>Disabled</td>
</tr>
<tr>
<td>Phone Field 4</td>
<td>Disabled</td>
</tr>
<tr>
<td>Phone/SMS Selected</td>
<td>Voice</td>
</tr>
<tr>
<td>Phone/SMS Visible</td>
<td>True</td>
</tr>
<tr>
<td>Default Phone Country Code</td>
<td></td>
</tr>
<tr>
<td>Phone Mask (RegEx)</td>
<td></td>
</tr>
</tbody>
</table>

#### Email Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Field 1</td>
<td>Enabled (HTML)</td>
</tr>
<tr>
<td>Email Field 2</td>
<td>Enabled (HTML)</td>
</tr>
<tr>
<td>Email Field 3</td>
<td>Disabled</td>
</tr>
<tr>
<td>Email Field 4</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

#### Knowledge Based Settings

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>KB Questions</td>
<td>Enabled</td>
</tr>
<tr>
<td>KB Format</td>
<td>Base 64</td>
</tr>
<tr>
<td>Number of Questions</td>
<td>2</td>
</tr>
<tr>
<td>KB Conversion</td>
<td>False</td>
</tr>
</tbody>
</table>
1. In the Registration Configuration section, enable at least one Multi-Factor Authentication mechanism to be utilized in the Authentication API workflow. Refer to Registration Methods Tab Configuration for more information.

If not using Multi-Factor Authentication in the workflow, then no configuration is required.

The Authentication API supports the following registration methods:

- Telephony OTP
- SMS OTP
- Email OTP
- Knowledge-based Questions and Answers
- Help Desk
- OATH Token
- Push Notification and Push-to-Accept
- Static PIN

Ensure the Registration Methods Profile Properties (e.g. Phone 1, Email 1, etc.) are mapped appropriately to directory attributes in the Data tab to enable Multi-Factor Authentication.

Click Save once the configurations have been completed and before leaving the Registration Methods / Multi-Factor Methods page to avoid losing changes.

To enable Adaptive Authentication...

Workflow
## Adaptive Authentication

### Sorting Order

Drag and drop to sort the adaptive authentication factors from first (top) to last (bottom). Only enabled factor can be moved.

<table>
<thead>
<tr>
<th>Order</th>
<th>Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IP/Country Restriction</td>
</tr>
<tr>
<td>2</td>
<td>IP Reputation/Threat Data</td>
</tr>
<tr>
<td>3</td>
<td>User/Group Restriction</td>
</tr>
<tr>
<td>4</td>
<td>Geo-Velocity Restriction</td>
</tr>
</tbody>
</table>

### Settings

**Enable IP/Country Restriction**

| Restriction Type |  
|------------------|---
| IP Restriction   |  

**IP List**

- **Allow**

**Failure Action**

- **Hard stop**

- **Require user to enter username before adaptive authentication occurs**
1. In the **Adaptive Authentication** section, configure the realm to enable / disable functions to be used by the application. Refer to **Adaptive Authentication Guide** for the full configuration steps.

Be sure to select the preferred **Authentication Mode** (in the **Workflow** section), as it dictates the **suggested actions** by the API.

Click **Save** once the configurations have been completed and before leaving the **Workflow** page to avoid losing changes.
2. In the **IP Configuration** section, set the **Public IP Address** to the appliance's public IP address or 127.0.0.1 as preferred.

This step is required if using **Geo-Velocity** analysis to avoid errors with the Adaptive Authentication API.

Click **Save** once the configurations have been completed and before leaving the **System Info** page to avoid losing changes.

To enable Phone Number Profiling...
Registration Configuration

Phone Settings

Phone Number Blocking

- Cellular Telephones
- Landlines
- IP Phones
- Toll-free Numbers
- Premium Rate Numbers
- Pagers
- Unknown

Block phone numbers from the following sources:

Block phone numbers that have recently changed carriers:

- Enable
- Allow users to approve or delete a phone number that has recently changed carriers

Store carrier information in:

Aux ID 2

Block or allow phone numbers by carrier or country:

- Enable block/allow list

Define list of blocked/allowed numbers and carriers
1. In the **Phone Number Blocking** frame in the **Registration Configuration** section, enable at least one option

- Block phone numbers from the following [selected] sources
- Block phone numbers that have recently ported carriers
- Block or allow phone numbers by carrier or country

Refer to **Phone Number Profiling Service Configuration Guide** for complete configuration steps

See **/numberprofile Endpoints** for API configuration information

Click **Save** once the configurations have been completed and before leaving the **Multi-Factor Methods** page to avoid losing changes

To enable Multi-Factor Throttling...

**Multi-Factor Methods**
**Registration Configuration**

**Phone Settings**
- Synchronise VIP field: [ ]

**Multi-Factor Settings**
- Inline Initialization:
  - [ ] Missing Phone
  - [ ] Missing Email
  - [ ] Missing KB Answers
  - [ ] Missing PIN
- Auto-Submit When One Avail: [ ] Disabled
- OTP Length: 6

**Multi-Factor Throttling**
- [ ] Enable multi-factor throttling
- Only allow [ ] failed attempts in [ ] Minutes for each user
- [ ] Block use of multi-factor until time limit has expired
- [ ] Lock user account after exceeding attempts
- Store attempt count in [ ] Aux ID 1
Multi-Factor Throttling requires SecureAuth IdP version 9.0.2 or greater

1. In the Multi-Factor Settings section, check Enable multi-factor throttling

2. Configure the settings to customize the number of allowed failed attempts and the length of the rolling time window

3. Configure the action to take upon exceeding the allowed failed attempts

4. Select a profile property to store the count of failed attempts

Refer to Multi-Factor Throttling Configuration Guide for the full configuration steps

Click Save once the configurations have been completed and before leaving the Multi-Factor Methods page to avoid losing changes

To enable Device / Browser Fingerprinting (DFP)...
<table>
<thead>
<tr>
<th>Property</th>
<th>Source</th>
<th>Field</th>
<th>Data Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Groups</td>
<td>Default Provider</td>
<td>memberOf</td>
<td></td>
</tr>
<tr>
<td>First Name</td>
<td>Default Provider</td>
<td>givenName</td>
<td></td>
</tr>
<tr>
<td>Last Name</td>
<td>Default Provider</td>
<td>sn</td>
<td></td>
</tr>
<tr>
<td>Phone 1</td>
<td>Default Provider</td>
<td>telephoneNumber</td>
<td></td>
</tr>
<tr>
<td>Phone 2</td>
<td>Default Provider</td>
<td>mobile</td>
<td></td>
</tr>
<tr>
<td>Phone 3</td>
<td>Default Provider</td>
<td>homePhone</td>
<td></td>
</tr>
<tr>
<td>Phone 4</td>
<td>Default Provider</td>
<td>pager</td>
<td></td>
</tr>
<tr>
<td>Fingerprints</td>
<td>Default Provider</td>
<td>audio</td>
<td>Plain Binary</td>
</tr>
<tr>
<td>Push Notification</td>
<td>Default Provider</td>
<td>jpegPhoto</td>
<td>Plain Binary</td>
</tr>
<tr>
<td>Tokens</td>
<td></td>
<td>postalAddress</td>
<td></td>
</tr>
<tr>
<td>OATH Tokens</td>
<td>Default Provider</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Histories</td>
<td>Default Provider</td>
<td>photo</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[Add Property]
1. In the **Membership Connection Settings** section, map a directory field to the **Fingerprints** property.

   In typical AD deployments the audio directory field is utilized.

2. Check **Writable**

The **Fingerprints** Property can be stored as **Plain Binary** or in **JSON** format, and has distinct requirements for the LDAP directory attribute mapped to the Property based on the **Data Format** selection.

For **Plain Binary**, these requirements must be met for the directory field that contains the fingerprint information:

- **Length**: 4096 minimum
- **Data Type**: Octet string (bytes)
- **Multi-valued**

For **JSON**, these requirements must be met for the directory field that contains the fingerprint information:

- **Length**: No limit / undefined
- **Data Type**: DirectoryString
- **Multi-valued**
3. Configure the Device / Browser Fingerprinting settings to enable the use of /dfp endpoints

Refer to **Device / Browser Fingerprinting - Heuristic-based Authentication** for the full configuration steps
Click **Save** once the configurations have been completed and before leaving the **Data** page to avoid losing changes

To enable Behavioral Biometrics...
1. In the Profile Fields section, map the Behavior Biometrics Property to a directory field, e.g. comment

2. Check Writable
Click Save once the configurations have been completed and before leaving the Data page to avoid losing changes.

HTTP Header

To authenticate against the API, an HTTP basic authorization header and Content-Type header are required.

1. Add a Content-Type header with a value of application/json.
2. Create an Authorization Header for all requests by following the steps below.

Authorization Header

For GET endpoint:

1. Build a string based on the request:
   - METHOD (GET)
   - DATE/TIME
   - APPLICATION ID (from SecureAuth IdP Web Admin)
   - PATH (API endpoint, e.g. /secureauth2/api/v1/users/<userID>/factors)

2. Create an HMAC SHA256 hash of step 1 using the Application Key (from SecureAuth IdP Web Admin).
   - This step is executed by calling the HMAC and producing the hash value.
3. Encode the HMAC SHA256 hash from step 2 in Base64.
4. Concatenate the "Application ID", ":", and the "Base64 encoded HMAC SHA256 hash" from step 3.
   - ApplicationID:Base64EncodedHMACSHA256Hash
5. Encode the value from step 4 in Base64.
6. Concatenate "Basic " and the "Value of Step 5".
   - Basic Step5Value
GET Request Example

Step 1
GET
Wed, 08 Apr 2015 21:37:33 GMT
1b700d2e7b7b4abfa1950c865e23e81a
/secureauth2/api/v1/users/jsmith/factors

End Result: "GET
Wed, 08 Apr 2015 21:37:33 GMT
1b700d2e7b7b4abfa1950c865e23e81a
/secureauth2/api/v1/users/jsmith/factors"

Step 2
Non-printable bytes are produced in this step

Step 3
F5yqdLDJddUY01rpB1OJBh/YCUIMVCsWejuhiCrqMmw=

Step 4
1b700d2e7b7b4abfa1950c865e23e81a:F5yqdLDJddUY01rpB1OJBh/YCUIMVCsWejuhiCrqMmw=

Step 5
MWI3MDBkMmUtN2I3Yi00YjUxLWExOTUtMGM4Nzg4vFlsTmNvNjRqQkRENVJkRHFiZ0h0d0Uw
YwEQ4d1d4bTgvWVx9

Step 6
Basic
MWI3MDBkMmUtN2I3Yi00YjUxLWExOTUtMGM4Nzg4vFlsTmNvNjRqQkRENVJkRHFiZ0h0d0Uw
YwEQ4d1d4bTgvWVx9

End Result:
Method: GET,
Version: 1.1,
Headers: {
  Connection: Keep-Alive
  Date: Wed, 08 Apr 2015 21:37:33 GMT
  Authorization: Basic
  MWI3MDBkMmUtN2I3Yi00YjUxLWExOTUtMGM4Nzg4vFlsTmNvNjRqQkRENVJkRHFiZ0h0d0Uw
  YwEQ4d1d4bTgvWVx9
  Host: secureauth.company.com
  Content-Length: 0
}

For POST endpoint:

1. Build a string based on the request

   METHOD (POST)
   DATE/TIME
   APPLICATION ID (from SecureAuth IdP Web Admin)
   PATH (API endpoint, e.g. /secureauth2/api/v1/auth)
   CONTENT (JSON Parameters)

2. Create an HMAC SHA256 hash of step 1 using the Application Key (from SecureAuth IdP Web Admin)
   This step is executed by calling the HMAC and producing the hash value

3. Encode the HMAC SHA256 hash from step 2 in Base64

4. Concatenate the "Application ID", "-", and the "Base64 encoded HMAC SHA256 hash" from step 3
   ApplicationId:Base64EncodedHMAC256Hash
5. Encode the value from step 4 in Base64
6. Concatenate "Basic" and the "Value of Step 5"

Basic Step5Value

POST Request Example

Step 1
POST
Wed, 08 Apr 2015 21:27:30 GMT
1b700d2e7b7b4abfa1950c865e23e81a
/secureauth2/api/v1/auth
("user_id":"jsmith","type":"user_id")

End Result: "POST
Wed, 08 Apr 2015 21:27:30 GMT
1b700d2e7b7b4abfa1950c865e23e81a
/secureauth2/api/v1/auth
("user_id":"jsmith","type":"user_id")"

Step 2
Non-printable bytes are produced in this step

Step 3
D6nkepAEtk/M+cpkyWQ/h2MXZxP32L++522a6+pB8U=

Step 4
1b700d2e7b7b4abfa1950c865e23e81a:D6nkepAEtk/M+cpkyWQ/h2MXZxP32L++522a6+pB8U=

Step 5
MWI3MDBkMmUtN2I3Yi00YWJmLWEwOTUtMG44NjVlMjN1ODFhOkQ2bmtlcEFp
wrKzVaWmE2K3BCOFU9

Step 6
Basic
MWI3MDBkMmUtN2I3Yi00YWJmLWEwOTUtMG44NjVlMjN1ODFhOkQ2bmtlcEFp
wrKzVaWmE2K3BCOFU9

End Result:
Method: POST
RequestUri: 'https://secureauth.company.com/secureauth2/api/v1/auth'
Version: 1.1
Headers: {
    Connection: Keep-Alive
    Date: Wed, 08 Apr 2015 21:27:30 GMT
    Authorization: Basic
    Expect: 100-continue
    Host: secureauth.company.com
    Content-Length: 36
    Content-Type: application/json; charset=utf-8
}
When an Authorization Header cannot be validated, one of the following responses will be returned:

<table>
<thead>
<tr>
<th>Status</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>invalid</td>
<td>Missing authentication header.</td>
</tr>
<tr>
<td>invalid</td>
<td>Unknown authentication scheme.</td>
</tr>
<tr>
<td>invalid</td>
<td>Clock skew of message is outside threshold.</td>
</tr>
<tr>
<td>invalid</td>
<td>AppId is unknown.</td>
</tr>
<tr>
<td>invalid</td>
<td>Authentication header value is empty.</td>
</tr>
<tr>
<td>invalid</td>
<td>Authentication header has been seen before.</td>
</tr>
<tr>
<td>invalid</td>
<td>Authentication header value's format should be 'appId:hash'.</td>
</tr>
<tr>
<td>invalid</td>
<td>Invalid credentials.</td>
</tr>
</tbody>
</table>

3. (OPTIONAL) If utilizing the Email 2-Factor Authentication method and a different language than US English, create an Accept-Language header to generate the Email OTP messages in the preferred language.

If no Accept-Language header is present, the Email OTP messages default to US English.

### Endpoints

- /users Endpoints
- /numberprofile Endpoints
- /adaptauth POST Endpoint
- /auth POST Endpoints
- /accesshistory POST Endpoint
- /ipeval POST Endpoint
- /dfp Endpoints
- /behavebio Endpoints
The `/factors` endpoint returns a list of enabled Multi-Factor Authentication methods.

By utilizing the username in the endpoint URL, SecureAuth IdP can access the user's profile and respond with the list of available Multi-Factor Authentication mechanisms.

As a GET endpoint, there is no body, so no JSON parameters are required.

**Definitions**

- **status**: The status of user ID provided (found, not_found, invalid, etc.); will always be in response
- **message**: Additional information regarding the status; will always be in response
- **user_id**: The user ID provided; will always be in response, whether successful or not
- **factors**: The list of available multi-factor authentication methods available to the user

  - **type**: The type of method (phone, kbq, push, etc.)
  - **id**: The SecureAuth IdP Profile Property that is mapped to the directory field containing the information required to conduct the authentication (Phone1, Email2, etc.)

    - The indexed knowledge-based questions within the Knowledge-based Questions SecureAuth IdP Property (KBQ1, KBQ2, etc.)
    - A unique identifier provided to SecureAuth IdP by the mobile device during the provisioning process (for OATH and Push)

  - **value**: The information contained in the SecureAuth IdP Property / directory field (phone number, email address, device name, etc.)
  - **capabilities**: The variations available for the factor that require user selection (phone call, text message, etc.)

**Response:**
<table>
<thead>
<tr>
<th>Success</th>
<th>Fail / Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>{</td>
<td>{</td>
</tr>
<tr>
<td>&quot;status&quot;: &quot;found&quot;,</td>
<td>&quot;status&quot;: &quot;not_found&quot;,</td>
</tr>
<tr>
<td>&quot;message&quot;: &quot;&quot;,</td>
<td>&quot;message&quot;: &quot;User Id was not found&quot;</td>
</tr>
<tr>
<td>&quot;user_id&quot;: &quot;jsmith&quot;,</td>
<td>}</td>
</tr>
<tr>
<td>&quot;factors&quot;: [</td>
<td>HTTP Status 404</td>
</tr>
<tr>
<td>{</td>
<td></td>
</tr>
<tr>
<td>&quot;type&quot;: &quot;phone&quot;,</td>
<td>{</td>
</tr>
<tr>
<td>&quot;id&quot;: &quot;Phone1&quot;,</td>
<td>&quot;status&quot;: &quot;invalid_group&quot;,</td>
</tr>
<tr>
<td>&quot;value&quot;: &quot;123-456-7890&quot;,</td>
<td>&quot;message&quot;: &quot;User Id is not associated with a valid group.&quot;</td>
</tr>
<tr>
<td>&quot;capabilities&quot;: [</td>
<td>}</td>
</tr>
<tr>
<td>&quot;call&quot;</td>
<td>HTTP Status 200</td>
</tr>
<tr>
<td>],</td>
<td></td>
</tr>
<tr>
<td>{</td>
<td></td>
</tr>
<tr>
<td>&quot;type&quot;: &quot;phone&quot;,</td>
<td>{</td>
</tr>
<tr>
<td>&quot;id&quot;: &quot;Phone2&quot;,</td>
<td>&quot;status&quot;: &quot;disabled&quot;,</td>
</tr>
<tr>
<td>&quot;value&quot;: &quot;987-654-3210&quot;,</td>
<td>&quot;message&quot;: &quot;Account is disabled.&quot;</td>
</tr>
<tr>
<td>&quot;capabilities&quot;: [</td>
<td>}</td>
</tr>
<tr>
<td>&quot;sms&quot;,</td>
<td>HTTP Status 200</td>
</tr>
<tr>
<td>&quot;call&quot;</td>
<td></td>
</tr>
<tr>
<td>],</td>
<td></td>
</tr>
<tr>
<td>{</td>
<td></td>
</tr>
<tr>
<td>&quot;type&quot;: &quot;email&quot;,</td>
<td>{</td>
</tr>
<tr>
<td>&quot;id&quot;: &quot;Email1&quot;,</td>
<td>&quot;status&quot;: &quot;lock_out&quot;,</td>
</tr>
<tr>
<td>&quot;value&quot;: &quot;<a href="mailto:jsmith@company.com">jsmith@company.com</a>&quot;</td>
<td>&quot;message&quot;: &quot;Account is locked out.&quot;</td>
</tr>
<tr>
<td>},</td>
<td>}</td>
</tr>
<tr>
<td>{</td>
<td>HTTP Status 200</td>
</tr>
<tr>
<td>&quot;type&quot;: &quot;kbq&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;id&quot;: &quot;KBQ1&quot;,</td>
<td>{</td>
</tr>
<tr>
<td>&quot;value&quot;: &quot;What city were you born in?&quot;</td>
<td>&quot;status&quot;: &quot;password_expired&quot;,</td>
</tr>
<tr>
<td>},</td>
<td>&quot;message&quot;: &quot;Password is expired.&quot;</td>
</tr>
<tr>
<td>{</td>
<td>}</td>
</tr>
<tr>
<td>&quot;type&quot;: &quot;kbq&quot;,</td>
<td>HTTP Status 200</td>
</tr>
<tr>
<td>&quot;id&quot;: &quot;KBQ2&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;value&quot;: &quot;What was your favorite childhood game?&quot;</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
</tbody>
</table>

See Server Error information below
### /users/{username}/throttle

<table>
<thead>
<tr>
<th>HTTP Method</th>
<th>URI</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET</td>
<td>/api/v1/users/{username} /throttle</td>
<td><a href="https://secureauth.company.com/secureauth2/api/v1/users/jsmith">https://secureauth.company.com/secureauth2/api/v1/users/jsmith</a> /throttle</td>
</tr>
<tr>
<td>PUT</td>
<td>/api/v1/users/{username} /throttle</td>
<td><a href="https://secureauth.company.com/secureauth2/api/v1/users/jsmith">https://secureauth.company.com/secureauth2/api/v1/users/jsmith</a> /throttle</td>
</tr>
</tbody>
</table>

The Multi-Factor Throttling API provides protection against an attacker attempting to 1) brute force an account via trial-and-error using large numbers of OTPs and 2) disrupt service via a denial-of-service attack where an attacker attempts to overwhelm the system by generating a large number of OTPs.

The **GET** method retrieves the current count of Multi-Factor attempts for the given username.

The **PUT** method resets the count of Multi-Factor attempts to 0 (suggested after a successful authentication); the attempt count is stored in a directory attribute configured in the Web Admin (refer to Multi-Factor Throttling Configuration Guide for more information).

The thresholds for this API are configured within the Multi-Factor Methods tab of the Web Admin; any authentication attempts exceeding these thresholds are disregarded and an error message is displayed to the end-user.

#### GET Responses:

<table>
<thead>
<tr>
<th>Success</th>
<th>Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>{</td>
<td></td>
</tr>
<tr>
<td>&quot;status&quot;: &quot;found&quot;,</td>
<td>&quot;status&quot;: &quot;not_found&quot;,</td>
</tr>
<tr>
<td>&quot;message&quot;: &quot;&quot;,</td>
<td>&quot;message&quot;: &quot;User Id was not found&quot;,</td>
</tr>
<tr>
<td>&quot;count&quot;: &quot;&quot;,</td>
<td>&quot;count&quot;: &quot;0&quot;,</td>
</tr>
<tr>
<td>}</td>
<td>}</td>
</tr>
<tr>
<td>HTTP Status 200</td>
<td>HTTP Status 404</td>
</tr>
</tbody>
</table>

#### PUT Responses:

<table>
<thead>
<tr>
<th>Success</th>
<th>Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>{</td>
<td></td>
</tr>
<tr>
<td>&quot;status&quot;: &quot;found&quot;,</td>
<td>&quot;status&quot;: &quot;not_found&quot;,</td>
</tr>
<tr>
<td>&quot;message&quot;: &quot;&quot;,</td>
<td>&quot;message&quot;: &quot;User Id was not found&quot;,</td>
</tr>
<tr>
<td>&quot;count&quot;: &quot;&quot;,</td>
<td>&quot;count&quot;: &quot;&quot;</td>
</tr>
<tr>
<td>}</td>
<td>}</td>
</tr>
<tr>
<td>HTTP Status 200</td>
<td>HTTP Status 404</td>
</tr>
</tbody>
</table>

### /numberprofile Endpoints

**NOTE:** The SecureAuth IdP Detect license is required to use this feature / endpoint.

<table>
<thead>
<tr>
<th>HTTP Method</th>
<th>URI</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>POST / PUT</td>
<td>/api/v1/numberprofile</td>
<td><a href="https://secureauth.company.com/secureauth2/api/v1/numberprofile">https://secureauth.company.com/secureauth2/api/v1/numberprofile</a></td>
</tr>
</tbody>
</table>

Endpoints for /numberprofile are used on demand to view an end-user’s phone number profile and update the record if information such as carrier, network, and / or country has changed.

**NOTE:** For phone numbers that are *roaming*, SecureAuth IdP still retrieves the carrier information, upholding the carrier blocking configurations set in the Web Admin.

The **POST** method retrieves the phone profile record from the data provider which includes the original carrier information.

If a change needs to be made to the end-user carrier information, the **PUT** method is used to update the directory to reflect the change – e.g. recently-ported phone number status change and / or carrier change.

After the change is made, a subsequent **POST** call retrieves the original carrier information from the directory and the current carrier information from the data provider.

If a discrepancy exists between the original carrier information and current carrier information, a **PUT** call is made to update the phone profile record.
Definitions

**user_id**: user ID provided

**phone_number**: user phone number provided

**status**: state of the user ID or phone number provided (not_found, invalid, valid, etc.)

**message**: additional information regarding the status of the user ID or phone number; will always be in response

**providerRequestId**: unique reference identification number for the request, generated by the data provider

**portedStatus**: user phone status for the option to block phone numbers that recently changed carriers (not_ported, ported)

**originalCarrier**: the first time a POST call is made, user phone profile information from the data provider information appears here – on subsequent POST calls, user phone profile information stored in the directory appears here

**currentCarrier**: following a PUT call and a subsequent POST call, user phone profile information from the data provider appears here

**carrierCode**: 6-digit number or a concatenation of the country code and phone type

**carrier**: name of the carrier or a concatenation of the country code and phone type

**countryCode**: 2-character country code

**networkType**: phone connection source (landline, tollfree, mobile, virtual, unknown, landline_tollfree)

**carrierStatus**: state of the carrier (blocked, allowed) based on the configuration defined in the Web Admin

**reason**: explanation for the state of the carrier (network_type, ported, country, carrier) based on the configuration defined in the Web Admin

See **Phone Number Profiling Service** for configuration settings
### POST Endpoint

<table>
<thead>
<tr>
<th>JSON Parameters</th>
<th>Success Response (Phone profile is returned with this response)</th>
<th>Fail / Error Response (Phone profile is not returned with this response)</th>
</tr>
</thead>
<tbody>
<tr>
<td>{ &quot;user_id&quot;: &quot;&lt;USERNAME&gt;&quot;,  &quot;phone_number&quot;: &quot;&lt;PHONE NO.&gt;&quot; }</td>
<td>{  &quot;numberProfileResult&quot;: {  &quot;providerRequestId&quot;: &quot;01eda1b2-d47c-4290-b1ca-6de8b2573836&quot;,  &quot;internationalFormat&quot;: &quot;19491234567&quot;,  &quot;nationalFormat&quot;: &quot;(949) 123-4567&quot;,  &quot;countryPrefix&quot;: &quot;1&quot;,  &quot;countryCode&quot;: &quot;US&quot;,  &quot;countryCodeISO3&quot;: &quot;USA&quot;,  &quot;country&quot;: &quot;United States of America&quot;,  &quot;portedStatus&quot;: &quot;not_ported&quot;,  &quot;validNumber&quot;: null,  &quot;reachable&quot;: null,  &quot;roamingInfo&quot;: null,  &quot;currentCarrier&quot;: {  &quot;carrierCode&quot;: &quot;US-FIXED&quot;,  &quot;carrier&quot;: &quot;United States of America Landline&quot;,  &quot;countryCode&quot;: &quot;US&quot;,  &quot;networkType&quot;: &quot;landline&quot;,  &quot;carrierStatus&quot;: {  &quot;status&quot;: &quot;blocked&quot;,  &quot;reason&quot;: [  &quot;networkType&quot; ]  }  },  &quot;originalCarrier&quot;: {  &quot;carrierCode&quot;: &quot;US-FIXED&quot;,  &quot;carrier&quot;: &quot;T-mobile USA, Inc.&quot;,  &quot;countryCode&quot;: &quot;US&quot;,  &quot;networkType&quot;: &quot;mobile&quot;,  &quot;carrierStatus&quot;: {  &quot;status&quot;: &quot;allowed&quot;,  &quot;reason&quot;: null  }  },  &quot;ipInfo&quot;: null,  &quot;ipWarning&quot;: null  },  &quot;status&quot;: &quot;valid&quot;,  &quot;message&quot;: &quot;&quot;  }</td>
<td>{  &quot;status&quot;: &quot;not_found&quot;,  &quot;message&quot;: &quot;User Id was not found.&quot;  }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HTTP Status 200 (OK - Non-existing user)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{  &quot;status&quot;: &quot;not_found&quot;,  &quot;message&quot;: &quot;The requested resource cannot be found.&quot;  }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HTTP Status 404 (Not Found - Non-existing endpoint)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{  &quot;status&quot;: &quot;invalid&quot;,  &quot;message&quot;: &quot;Request validation failed with: PhoneNumber was not present.&quot;  }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HTTP Status 400 (Bad Request - Missing phone number)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{  &quot;status&quot;: &quot;valid&quot;,  &quot;message&quot;: &quot;&quot;  }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HTTP Status 200 (OK - Invalid phone number)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{  &quot;status&quot;: &quot;not_found&quot;,  &quot;message&quot;: &quot;The requested resource cannot be found.&quot;  }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HTTP Status 404 (Not Found - Non-existing endpoint)</td>
</tr>
</tbody>
</table>

Example:

```
{  "user_id": "jsmith",  "phone_number": "19491234567" }
```
## PUT Endpoint

### JSON Parameters

```
{
    "user_id": "<USERNAME>",
    "phone_number": "<PHONE NO.>",
    "portedStatus": "not_ported",
    "carrierInfo": {
        "carrierCode": "<6-DIGIT NO. OR COUNTRY CODE + PHONE TYPE>",
        "carrier": "<CARRIER NAME OR COUNTRY CODE + PHONE TYPE>",
        "countryCode": "<2-CHARACTER COUNTRY CODE>",
        "networkType": "<TYPE OF NETWORK CONNECTION>"
    }
}
```

### Success Response (Phone profile is returned with this response)

```
{
    "status": "valid",
    "message": ""
}
```

HTTP Status 200 (OK - Successful PUT)

### Fail / Error Response (Phone profile is not returned with this response)

```
{
    "status": "not_found",
    "message": "User Id was not found."
}
```

HTTP Status 200 (OK - Non-existing user)

```
{
    "status": "not_found",
    "message": "The requested resource cannot be found."
}
```

HTTP Status 404 (Not Found - Non-existing endpoint)

```
{
    "status": "invalid",
    "message": "Request validation failed with: PhoneNumber was not present."
}
```

HTTP Status 400 (Bad Request - Missing phone number)

```
{
    "status": "valid",
    "message": ""
}
```

HTTP Status 200 (OK - Invalid phone number)

```
{
    "status": "not_found",
    "message": "The requested resource cannot be found."
}
```

HTTP Status 404 (Not Found - Non-existing endpoint)

## /auth Endpoints

### /auth

**HTTP Method** | **URI** | **Example**
--- | --- | ---
POST | /api/v1/auth | https://secureauth.company.com/secureauth2/api/v1/auth

Validates auth information (e.g. username, password, etc.) and generates OTPs for authentication
Definitions

**evaluate_number**: (optional) evaluate recipient's phone number and return whether the number is valid to be used for the dispatch of an SMS or Voice OTP

Replace the `<CONTENT>` with the actual JSON Parameter values before sending the POST requests

- `<USERNAME>`: User ID, e.g. jsmith
- `<PASSWORD>`: User password, e.g. P@$SW0RD
- `<ANSWER>`: User answer to knowledge-based question
- `<KBQ PROPERTY>`: Indexed location of the specific KBQ being used for the authentication, e.g. KBQ2
- `<OTP>`: One-time password generated by the OATH token or on an ad hoc basis
- `<DEVICE IDENTIFIER>`: Unique identifier provided to SecureAuth IdP by the mobile device during the provisioning process (for OATH and Push)
- `<PIN NUMBER>`: User's static PIN number (e.g. 1234)
- `<PHONE PROPERTY>`: SecureAuth IdP Profile Property that is mapped to the directory field containing the required phone number, e.g. Phone1
- `<EMAIL PROPERTY>`: SecureAuth IdP Profile Property that is mapped to the directory field containing the required email address, e.g. Email1
- `<UNREGISTERED PHONE>`: Phone number that is not stored in the directory
- `<UNREGISTERED EMAIL>`: Email address that is not stored in the directory
- `<HELPDESK PROPERTY>`: Help desk option being used for this authentication, e.g. HelpDesk1

In the **Registration Methods / Multi-Factor Methods** tab in the SecureAuth IdP Web Admin, there are two Help Desk authentication options to enable (HelpDesk1 and HelpDesk2)

- `<IP ADDRESS>`: IP Address of the user's device
- `<COMPANY>`: Company name, configured in the **Registration Methods / Multi-Factor Methods** tab of the Web Admin for Push-to-Accept or can be overridden in code
- `<APP>`: Application / realm name, configured in the **Registration Methods / Multi-Factor Methods** tab of the Web Admin for Push-to-Accept or can be overridden in code

---

**New Functions Introduced in v9.0.2**

**Evaluate Phone Number for OTP**

Include the optional `evaluate_number` flag in any `/auth` request to evaluate a recipient's phone number for validity before delivering an OTP via SMS or Voice call. The criteria used to determine whether a phone number is valid or invalid for use is configured in the **Multi-Factor Methods** tab.

Refer to **Phone Number Profiling Service Configuration Guide** for more information
**NOTE:** For phone numbers that are *roaming*, SecureAuth IdP still retrieves the carrier information, upholding the carrier blocking configurations set in the Web Admin.

For OTP delivery, SecureAuth IdP delivers to the OTP to the carrier, and then the carrier forwards the message to the roaming partner’s network.

## Send Ad hoc OTP

The Send Ad hoc OTP API allows for an OTP to be dispatched on an ad hoc basis to a valid phone number or email address that is not currently stored in the directory (i.e. unregistered).

Use the **token** request parameter to define unregistered recipient phone numbers and email addresses.

Refer to **Authentication API: Send Ad hoc OTP without Existing User Profile** for specific configuration steps when using ad hoc OTP delivery to users that are not registered in the directory.

<table>
<thead>
<tr>
<th>Function</th>
<th>JSON Parameters</th>
<th>Success Response</th>
<th>Fail / Error Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>ad hoc call</td>
<td><code>{ &quot;user_id&quot;: &quot;&lt;USERNAME&gt;&quot;, &quot;type&quot;: &quot;call&quot;, &quot;token&quot;: &quot;&lt;UNREGISTERED PHONE&gt;&quot;, &quot;evaluate_number&quot;: &quot;true&quot; }</code></td>
<td><code>{ &quot;status&quot;: &quot;valid&quot;, &quot;message&quot;: &quot;&quot; }</code></td>
<td><code>{ &quot;status&quot;: &quot;invalid&quot;, &quot;message&quot;: &quot;Request validation failed with: User Id was not present.&quot; }</code></td>
</tr>
</tbody>
</table>

**Example:**

```
{
  "user_id": "jsmith",
  "type": "call",
  "token": "44396551234",
  "evaluate_number": "true"
}
```

Note that for ad hoc OTP delivery the only supported "type" values are: sms, call, and email.

See **Server Error** information below.

```json
{
  "status": "server_error",
  "message": "Error parsing phone field."
}
```

```json
{
  "status": "server_error",
  "message": "The specified string is not in the form required for an e-mail address."
}
```
### ad hoc sms
Deliver OTP via text message to a phone number not stored in the directory

```json
{
  "user_id": "<USERNAME>",
  "type": "sms",
  "token": "<UNREGISTERED PHONE>",
  "evaluate_number": "true"
}
```

**Example:**
```json
{
  "user_id": "jsmith",
  "type": "sms",
  "token": "44396551234",
  "evaluate_number": "true"
}
```

### ad hoc email
Deliver OTP via email to an email address not stored in the directory

```json
{
  "user_id": "<USERNAME>",
  "type": "email",
  "token": "<UNREGISTERED EMAIL>",
}
```

**Example:**
```json
{
  "user_id": "jsmith",
  "type": "email",
  "token": "jsmith@company.com",
}
```

<table>
<thead>
<tr>
<th>Function</th>
<th>JSON Parameters</th>
<th>Success Response</th>
<th>Fail / Error Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>user_id</td>
<td>Validate user ID</td>
<td></td>
<td>See Fail / Error Responses in <code>users</code> endpoint table</td>
</tr>
</tbody>
</table>
|                 | {
|                 |   "user_id": "<USERNAME>",
|                 |   "type": "user_id"
|                 | }                                 | {
|                 |   "status": "found",
|                 |   "message": "User Id found"
|                 | }                                 | {
|                 |   "status": "invalid",
|                 |   "message": "User Id or password is invalid."
| password        | Validate user password           |                                 |                       |
|                 | {
|                 |   "user_id": "<USERNAME>",
|                 |   "type": "user_id"
|                 | }                                 | {
|                 |   "status": "valid",
|                 |   "message": ""
|                 | }                                 | {
|                 |   "status": "invalid",
|                 |   "message": "User Id or password is invalid."}
<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Example</th>
<th>Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;type&quot;: &quot;password&quot;</td>
<td>Validation of password</td>
<td>`{ &quot;user_id&quot;: &quot;jsmith&quot;, &quot;type&quot;: &quot;password&quot;, &quot;token&quot;: &quot;P@$$W0RD&quot; }</td>
<td>{ &quot;status&quot;: &quot;invalid&quot;, &quot;message&quot;: &quot;A &lt;X&gt; value is required for this type.&quot; }</td>
</tr>
<tr>
<td>kba</td>
<td>Validate knowledge-based answer</td>
<td>`{ &quot;user_id&quot;: &quot;&lt;USERNAME&gt;&quot;, &quot;type&quot;: &quot;kba&quot;, &quot;token&quot;: &quot;&lt;ANSWER&gt;&quot;, &quot;factor_id&quot;: &quot;&lt;KBQ PROPERTY&gt;&quot; }</td>
<td>{ &quot;status&quot;: &quot;invalid&quot;, &quot;message&quot;: &quot;Knowledge base answer is incorrect.&quot; }</td>
</tr>
<tr>
<td>oath</td>
<td>Validate OATH token</td>
<td>`{ &quot;user_id&quot;: &quot;&lt;USERNAME&gt;&quot;, &quot;type&quot;: &quot;oath&quot;, &quot;token&quot;: &quot;&lt;OTP&gt;&quot;, &quot;factor_id&quot;: &quot;&lt;DEVICE IDENTIFIER&gt;&quot; }</td>
<td>{ &quot;status&quot;: &quot;invalid&quot;, &quot;message&quot;: &quot;OTP is invalid.&quot; }</td>
</tr>
<tr>
<td>pin</td>
<td>Validate static PIN</td>
<td>`{ &quot;user_id&quot;: &quot;&lt;USERNAME&gt;&quot;, &quot;type&quot;: &quot;pin&quot;, &quot;token&quot;: &quot;&lt;PIN NUMBER&gt;&quot; }</td>
<td>{ &quot;status&quot;: &quot;invalid&quot;, &quot;message&quot;: &quot;PIN is invalid.&quot; }</td>
</tr>
</tbody>
</table>

Example:

- Password:
  ```json
  { "user_id": "jsmith", "type": "password", "token": "P@$$W0RD" }
  ```
- KBA:
  ```json
  { "user_id": "<USERNAME>", "type": "kba", "token": "<ANSWER>", "factor_id": "<KBQ PROPERTY>" }
  ```
- OATH:
  ```json
  { "user_id": "<USERNAME>", "type": "oath", "token": "<OTP>", "factor_id": "<DEVICE IDENTIFIER>" }
  ```
- PIN:
  ```json
  { "user_id": "<USERNAME>", "type": "pin", "token": "<PIN NUMBER>" }
  ```
call
Deliver OTP via phone call

```
{  
"user_id": "<USERNAME>",  
"type": "call",  
"factor_id": "<PHONE PROPERTY>",  
"evaluate_number": "true" 
}
```

Example:

```
{  
"user_id": "jsmith",  
"type": "call",  
"factor_id": "Phone1"  
"evaluate_number": "true" 
}
```

sms
Deliver OTP via text message

```
{  
"user_id": "<USERNAME>",  
"type": "sms",  
"factor_id": "<PHONE PROPERTY>",  
"evaluate_number": "true" 
}
```

Example:

```
{  
"user_id": "jsmith",  
"type": "sms",  
"factor_id": "Phone1"  
"evaluate_number": "true" 
}
```

email
Deliver OTP via email

```
{  
"user_id": "<USERNAME>",  
"type": "email",  
"factor_id": "<EMAIL PROPERTY>",  
"evaluate_number": true" 
}
```

Example:

```
{  
"user_id": "jsmith",  
"type": "email",  
"factor_id": "Email1" 
}```

```
{  
"status": "valid",  
"message": "",  
"user_id": "jsmith",  
"otp": 8430 
}
```

See Server Error information below
push
Deliver OTP via Push Notification

```
{  
  "user_id": "<USERNAME>",
  "type": "push",
  "factor_id": "<DEVICE IDENTIFIER>"
}
```

Example:

```
{
  "user_id": "j smith",
  "type": "push",
  "factor_id": "z0y9x87wv6u5t43srq2plon"
}
```

push_accept
Deliver Push-to-Accept notification

```
{  
  "user_id": "<USERNAME>",
  "factor_id": "<DEVICE IDENTIFIER>",
  "type": "push_accept",
  "push_accept_details": {  
    "company_name": "<COMPANY>",
    "application_description": "<APP>",
    "enduser_ip": "<IP ADDRESS>"
  }
}
```

Example:

```
{
  "user_id": "j smith",
  "factor_id": "8117b289773e7b4xxxxx",
  "type": "push_accept",
  "push_accept_details": {  
    "company_name": "ACME Corp",
    "application_description": "Salesforce",
    "enduser_ip": "111.222.33.44"
  }
}
```

help_desk
Deliver OTP via help desk

```
{  
  "user_id": "<USERNAME>",
  "type": "help_desk",
  "factor_id": "<HELPDESK PROPERTY>"
}
```

Example:

```
{
  "user_id": "j smith",
  "type": "help_desk",
  "factor_id": "HelpDesk1"
}
```

```
{  
  "status": "valid",
  "message": "",
  "user_id": "j smith",
  "otp": "8430"
}
```
### /auth/REF_ID

<table>
<thead>
<tr>
<th>HTTP Method</th>
<th>URI</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET</td>
<td>/api/v1/auth/</td>
<td><a href="https://secureauth.company.com/secureauth2/api/v1/auth/f50ab2d7-178f-4421-b3ae-9f5634fa54ef">https://secureauth.company.com/secureauth2/api/v1/auth/f50ab2d7-178f-4421-b3ae-9f5634fa54ef</a></td>
</tr>
</tbody>
</table>

Checks the status of Push-to-Accept responses

When a Push-to-Accept request is made, the corresponding response contains a Reference ID, which is then appended to the /auth endpoint to continuously check whether the login request is accepted, denied, pending, or other.

### Definitions

**status:** The status of Push-to-Accept response (found, not_found, or invalid); will always be in response

**message:** Additional information regarding the status; will always be in response

<table>
<thead>
<tr>
<th>Success Response</th>
<th>Fail / Error Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>`{</td>
<td>`{</td>
</tr>
</tbody>
</table>
|   "status": "found",
|   "status": "not_found",
|   "message": "ACCEPTED"
|   "message": "NOTFOUND"
|   "message": "DENIED"
|   "message": "DENIED"
|   "message": "FAILED"
|   "message": "Invalid reference ID."
|   "message": "EXPIRED"
|   "message": "PENDING"

### /adaptauth Endpoint

<table>
<thead>
<tr>
<th>HTTP Method</th>
<th>URI</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>POST</td>
<td>/api/v1/adaptauth</td>
<td><a href="https://secureauth.company.com/secureauth2/api/v1/adaptauth">https://secureauth.company.com/secureauth2/api/v1/adaptauth</a></td>
</tr>
</tbody>
</table>

Enables SecureAuth IdP Adaptive Authentication, which analyzes an end-user’s profile, group, IP address, country, geo-velocity, and any risks detected by threat intelligence data

The API utilizes the information configured in the Adaptive Authentication section of the SecureAuth IdP Web Admin. Refer to Adaptive Authentication Guide for more information

SecureAuth IdP returns a response that contains the **Status**, **Realm Workflow**, and **Suggested Action**

The **Status** is the configured Failure Action; the **Realm Workflow** is the workflow configured in the Web Admin; and the **Suggested Action** is the suggested next step to take based on the configurations
<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continue</td>
<td>End-user continues onto the configured workflow <em>(Failure Action: Resume auth in Web Admin)</em></td>
</tr>
<tr>
<td>SkipTwoFactor</td>
<td>End-user bypasses 2-Factor Authentication and moves forward to next workflow step, e.g. password <em>(Failure Action: Step down auth in Web Admin)</em></td>
</tr>
<tr>
<td>TwoFactor</td>
<td>End-user undergoes additional 2-Factor Authentication <em>(Failure Action: Step up auth in Web Admin)</em></td>
</tr>
<tr>
<td>Authenticated</td>
<td>End-user is taken directly to post-authentication target, bypassing additional analysis or 2-Factor Authentication <em>(Failure Action: Post auth in Web Admin)</em></td>
</tr>
<tr>
<td>HardStop</td>
<td>End-user is stopped immediately in the workflow and cannot continue <em>(Failure Action: Hard Stop in Web Admin)</em></td>
</tr>
<tr>
<td>Redirect</td>
<td>End-user is redirected to URL provided, e.g. another SecureAuth IdP realm <em>(Failure Action: Redirect in Web Admin)</em></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Suggested Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2ndfactor_password</td>
<td>End-user must undergo 2-Factor Authentication and then provide password</td>
</tr>
<tr>
<td>password</td>
<td>End-user must provide password</td>
</tr>
<tr>
<td>2ndfactor</td>
<td>End-user must undergo 2-Factor Authentication</td>
</tr>
<tr>
<td>none</td>
<td>End-user is not required to perform authentication or password validation</td>
</tr>
<tr>
<td>stop</td>
<td>End-user is stopped immediately in workflow and cannot continue</td>
</tr>
<tr>
<td>redirect</td>
<td>End-user is redirected to the provided URL</td>
</tr>
</tbody>
</table>

### JSON Parameters

```json
{}
```

### Success Response

<table>
<thead>
<tr>
<th>Status</th>
<th>Suggested Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continue</td>
<td>2ndfactor_password</td>
<td>End-user must undergo 2-Factor Authentication and then provide password</td>
</tr>
<tr>
<td>SkipTwoFactor</td>
<td>password</td>
<td>End-user must provide password</td>
</tr>
<tr>
<td>TwoFactor</td>
<td>2ndfactor</td>
<td>End-user must undergo 2-Factor Authentication</td>
</tr>
<tr>
<td>Authenticated</td>
<td>none</td>
<td>End-user is not required to perform authentication or password validation</td>
</tr>
<tr>
<td>HardStop</td>
<td>stop</td>
<td>End-user is stopped immediately in workflow and cannot continue</td>
</tr>
<tr>
<td>Redirect</td>
<td>redirect</td>
<td>End-user is redirected to the provided URL</td>
</tr>
</tbody>
</table>

### Failure / Error Response

```json
{}
```

The IP Address is not required if only performing user / group restriction; otherwise, it is required for all other functionality.
<table>
<thead>
<tr>
<th>realm_workflow</th>
<th>suggested_action</th>
<th>status</th>
<th>message</th>
</tr>
</thead>
<tbody>
<tr>
<td>2ndfactor</td>
<td>2ndfactor</td>
<td>Continue</td>
<td></td>
</tr>
<tr>
<td>2ndfactor</td>
<td>2ndfactor</td>
<td>SkipTwoFactor</td>
<td>None</td>
</tr>
<tr>
<td>2ndfactor</td>
<td>2ndfactor</td>
<td>TwoFactor</td>
<td>None</td>
</tr>
<tr>
<td>2ndfactor</td>
<td>2ndfactor</td>
<td>Authenticate</td>
<td>None</td>
</tr>
<tr>
<td>2ndfactor</td>
<td>2ndfactor</td>
<td>HardStop</td>
<td>None</td>
</tr>
<tr>
<td>2ndfactor</td>
<td>2ndfactor</td>
<td>IPRedirect</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>2ndfactor</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>SkipTwoFactor</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>TwoFactor</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>Authenticate</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>HardStop</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>IPRedirect</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>realm_workflow</th>
<th>suggested_action</th>
<th>status</th>
<th>message</th>
</tr>
</thead>
<tbody>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>2ndfactor</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>SkipTwoFactor</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>TwoFactor</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>Authenticate</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>HardStop</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>IPRedirect</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>realm_workflow</th>
<th>suggested_action</th>
<th>status</th>
<th>message</th>
</tr>
</thead>
<tbody>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>2ndfactor</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>SkipTwoFactor</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>TwoFactor</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>Authenticate</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>HardStop</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>IPRedirect</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>realm_workflow</th>
<th>suggested_action</th>
<th>status</th>
<th>message</th>
</tr>
</thead>
<tbody>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>2ndfactor</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>SkipTwoFactor</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>TwoFactor</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>Authenticate</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>HardStop</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>IPRedirect</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>realm_workflow</th>
<th>suggested_action</th>
<th>status</th>
<th>message</th>
</tr>
</thead>
<tbody>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>2ndfactor</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>SkipTwoFactor</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>TwoFactor</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>Authenticate</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>HardStop</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>IPRedirect</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>realm_workflow</th>
<th>suggested_action</th>
<th>status</th>
<th>message</th>
</tr>
</thead>
<tbody>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>2ndfactor</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>SkipTwoFactor</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>TwoFactor</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>Authenticate</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>HardStop</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>IPRedirect</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>realm_workflow</th>
<th>suggested_action</th>
<th>status</th>
<th>message</th>
</tr>
</thead>
<tbody>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>2ndfactor</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>SkipTwoFactor</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>TwoFactor</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>Authenticate</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>HardStop</td>
<td>None</td>
</tr>
<tr>
<td>usernamepassword</td>
<td>usernamepassword</td>
<td>IPRedirect</td>
<td>None</td>
</tr>
<tr>
<td>realm_workflow:</td>
<td>username:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>----------</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>suggested_action:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>status:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>message:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>realm_workflow:</th>
<th>username:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>suggested_action:</td>
</tr>
<tr>
<td></td>
<td>status:</td>
</tr>
<tr>
<td></td>
<td>message:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>realm_workflow:</th>
<th>username:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>suggested_action:</td>
</tr>
<tr>
<td></td>
<td>status:</td>
</tr>
<tr>
<td></td>
<td>message:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>realm_workflow:</th>
<th>username:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>suggested_action:</td>
</tr>
<tr>
<td></td>
<td>status:</td>
</tr>
<tr>
<td></td>
<td>message:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>realm_workflow:</th>
<th>username:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>suggested_action:</td>
</tr>
<tr>
<td></td>
<td>status:</td>
</tr>
<tr>
<td></td>
<td>message:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>realm_workflow:</th>
<th>persistent_token:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>suggested_action:</td>
</tr>
<tr>
<td></td>
<td>status:</td>
</tr>
<tr>
<td></td>
<td>message:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>realm_workflow:</th>
<th>persistent_token:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>suggested_action:</td>
</tr>
<tr>
<td></td>
<td>status:</td>
</tr>
<tr>
<td></td>
<td>message:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>realm_workflow:</th>
<th>persistent_token:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>suggested_action:</td>
</tr>
<tr>
<td></td>
<td>status:</td>
</tr>
<tr>
<td></td>
<td>message:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>realm_workflow:</th>
<th>persistent_token:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>suggested_action:</td>
</tr>
<tr>
<td></td>
<td>status:</td>
</tr>
<tr>
<td></td>
<td>message:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>realm_workflow:</th>
<th>persistent_token:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>suggested_action:</td>
</tr>
<tr>
<td></td>
<td>status:</td>
</tr>
<tr>
<td></td>
<td>message:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>realm_workflow:</th>
<th>persistent_token:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>suggested_action:</td>
</tr>
<tr>
<td></td>
<td>status:</td>
</tr>
<tr>
<td></td>
<td>message:</td>
</tr>
</tbody>
</table>
### /accesshistory Endpoint

<table>
<thead>
<tr>
<th>HTTP Method</th>
<th>URI</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>POST</td>
<td>/api/v1/accesshistory</td>
<td><a href="https://secureauth.company.com/secureauth2/api/v1/accesshistory">https://secureauth.company.com/secureauth2/api/v1/accesshistory</a></td>
</tr>
</tbody>
</table>

Creates a history of end-user's logins for use in geo-velocity (Adaptive Authentication)

Once an end-user is authenticated, the information is posted to the /accesshistory endpoint, and a new entry is created and stored in the user profile. For the next login attempt, SecureAuth IdP can use the stored information to validate whether the distance traveled from the previous login to the current attempt is feasible.

If geo-velocity is not enabled for Adaptive Authentication (in the SecureAuth IdP Web Admin), then this endpoint is not necessary.

<table>
<thead>
<tr>
<th>JSON Parameters</th>
<th>Success Response</th>
<th>Failure / Error Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>{</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;user_id&quot;:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;&lt;USERNAME&gt;&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;ip_address&quot;: &quot;&lt;IP ADDRESS&gt;&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>{</td>
<td></td>
</tr>
<tr>
<td>&quot;status&quot;: &quot;valid&quot;,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;message&quot;: &quot;Access History request has been processed.&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>{</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>{</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>{</td>
<td>&quot;status&quot;: &quot;invalid&quot;,</td>
</tr>
<tr>
<td>}</td>
<td>{</td>
<td>&quot;message&quot;: &quot;Access History was not saved.&quot;</td>
</tr>
<tr>
<td>}</td>
<td>{</td>
<td></td>
</tr>
</tbody>
</table>

### /ipeval Endpoint

<table>
<thead>
<tr>
<th>HTTP Method</th>
<th>URI</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>POST</td>
<td>/api/v1/ipeval</td>
<td><a href="https://secureauth.company.com/secureauth2/api/v1/ipeval">https://secureauth.company.com/secureauth2/api/v1/ipeval</a></td>
</tr>
</tbody>
</table>

Evaluates an IP address for risk factors based on threat intelligence data

This endpoint can be used as a standalone feature rather than alongside the other Adaptive Authentication features used in the /adaptauth endpoint.

If using the /ipeval endpoint and not the /adaptauth endpoint, then no configuration is required in the Adaptive Authentication section of the SecureAuth IdP Web Admin.
### Function JSON Parameters Success Response Failure / Error Response

<table>
<thead>
<tr>
<th>risk</th>
<th>IP Address Risk Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>risk</td>
<td>IP Address Risk Evaluation</td>
</tr>
</tbody>
</table>

**Example:**

```
{  
  "user_id":  "<USERNAME>",  
  "type": "risk",  
  "ip_address": "<IP ADDRESS>"
}
```

**Risk Factor (threatType) Scores**

<table>
<thead>
<tr>
<th>Threat Type (AE. IP.threatType)</th>
<th>Score</th>
<th>SecureAuth IdP Risk Category</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous Proxy</td>
<td>100</td>
<td>Extreme</td>
<td>Authentication is coming from a server that is designed to hide or anonymize the actual source IP Address</td>
</tr>
<tr>
<td>Attacker</td>
<td>99</td>
<td>Extreme</td>
<td>Indicators confirmed to host malicious content, has functioned as a command-and-control (C2) server, and / or has otherwise acted as a source of malicious activity</td>
</tr>
<tr>
<td>Compromised</td>
<td>98</td>
<td>Extreme</td>
<td>Indicators confirmed to host malicious content due to compromise or abuse – the exact time and length of compromise is unknown unless disclosed within the report</td>
</tr>
<tr>
<td>Related</td>
<td>88</td>
<td>High</td>
<td>Indicators likely related to an attack, but potentially only partially confirmed – detailed by one or more methods, like passive DNS, geo-location, and connectivity detection</td>
</tr>
<tr>
<td>Victim</td>
<td>89</td>
<td>High</td>
<td>Indicators representing an entity that has been confirmed to have been victimized by malicious activity, where actors have attempted or succeeded compromise</td>
</tr>
<tr>
<td>Uncategorized</td>
<td>80</td>
<td>High</td>
<td>Uncategorized threat</td>
</tr>
</tbody>
</table>

See Server Error information below
<table>
<thead>
<tr>
<th>Threat Category (AE.IP. threatCategory)</th>
<th>Response Value</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous Proxy</td>
<td>0</td>
<td>Authentication is coming from a server that is designed to hide or anonymize the actual source IP Address</td>
</tr>
<tr>
<td>Cyber Espionage</td>
<td>1</td>
<td>Global issue with highly sophisticated nation-states and other actors targeting military, political, and commercial interests to gain decision advantage</td>
</tr>
<tr>
<td>Hacktivism</td>
<td>2</td>
<td>Activity ranges from nuisance level to sophisticated campaigns conducted by globally coordinated actors using increasingly sophisticated tools to negatively impact revenue or damage the brand</td>
</tr>
<tr>
<td>Enterprise</td>
<td>3</td>
<td>Threats specifically targeted at Enterprise</td>
</tr>
<tr>
<td>Critical Infrastructure</td>
<td>4</td>
<td>Threats specifically targeted at Critical Infrastructure</td>
</tr>
<tr>
<td>Cyber Crime</td>
<td>5</td>
<td>Threats typically orchestrated by criminal elements for financial benefit</td>
</tr>
<tr>
<td>Vulnerability and Exploitation</td>
<td>6</td>
<td>Threats targeting known software vulnerabilities</td>
</tr>
</tbody>
</table>

/dfp Endpoints

The /dfp endpoints enable the use of SecureAuth IdP’s device / browser fingerprinting, which collects unique information from an end-user’s device or browser, and stores it as a “fingerprint” in the user profile. This fingerprint is then used as a comparison for future login attempts; and if a match is made, then it is used as the second factor of authentication.

To utilize these endpoints, the SecureAuth IdP realm must be configured for Device / Browser Fingerprinting. Refer to Device / Browser Fingerprinting - Heuristic-based Authentication for more information.
<table>
<thead>
<tr>
<th>HTTP Method</th>
<th>URI</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET</td>
<td>/api/v1/dfp/js</td>
<td><a href="https://secureauth.company.com/secureauth2/api/v1/dfp/js">https://secureauth.company.com/secureauth2/api/v1/dfp/js</a></td>
</tr>
</tbody>
</table>

Enables the application to retrieve the javascript reference that is required to generate fingerprints

Using the reference, end-users' devices / browsers are analyzed and most of the required information is collected; but the remaining characteristics must be provided by the application.

Response to request:

```
{
  "src": "https://SecureAuthIdPFQDN/SecureAuthIdPRealm/assets/scripts/api/secureauth-api.js?ver=8.1.1.071"
}
```

**HTML Javascript Usage Example**

This is an example of how to use the javascript reference to capture a client-side digital fingerprint.

```html
<script>
$(function()
    // invoke getFingerprint() method to capture
    // client-side info and serialize to JSON string.
    var serializedData = JSON.stringify(secureAuth.api.getFingerprint());

    // assign JSON string to an input for posting
    // to web server.
    $('#results').val(serializedData);
});
</script>
```

**Fingerprint Components**

<table>
<thead>
<tr>
<th>Provided by Javascript Reference</th>
<th>Provided by Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>fonts</td>
<td>host_address (IP Address of end-user client)</td>
</tr>
<tr>
<td>plugins</td>
<td>user_id</td>
</tr>
<tr>
<td>timezone</td>
<td>accept</td>
</tr>
<tr>
<td>video</td>
<td>accept_charset</td>
</tr>
<tr>
<td>local_storage</td>
<td>accept_encoding</td>
</tr>
<tr>
<td>session_storage</td>
<td>accept_language</td>
</tr>
<tr>
<td>ie_user_data</td>
<td></td>
</tr>
<tr>
<td>cookie_enabled</td>
<td></td>
</tr>
<tr>
<td>user_agent</td>
<td></td>
</tr>
</tbody>
</table>
**/dfp/validate Endpoint**

<table>
<thead>
<tr>
<th>HTTP Method</th>
<th>URI</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>POST</td>
<td>/api/v1/dfp/validate</td>
<td><a href="https://secureauth.company.com/secureauth2/api/v1/dfp/validate">https://secureauth.company.com/secureauth2/api/v1/dfp/validate</a></td>
</tr>
</tbody>
</table>

Compares the presented fingerprint with those stored in the user profile. Based on the information provided from the directory, SecureAuth IdP returns a response stating whether the fingerprint is found or not found. If the fingerprint is found, then the end-user has completed 2-Factor Authentication, and no additional authentication steps are required for identity validation.

**Definitions**

- **fingerprint_id**: GUID of the fingerprint
- **fingerprint_name**: Descriptive name derived from the user_agent string
- **score**: Match score of the provided fingerprint (out of 100.00)
- **match_score**: Minimum score allowed to be accepted as second factor authentication (configured in realm)
- **update_score**: Minimum score allowed to be accepted to update existing fingerprint with new information (configured in realm, requires 2-Factor Authentication for update)
- **status**: Status of the matching outcomes:
  - **found**: Fingerprint found with acceptable match_score
  - **found_for_update**: Fingerprint found with unacceptable match_score, but acceptable update_score and can be updated by posting to `/dfp/confirm` endpoint
  - **found_with_id_mismatch**: Fingerprint found, but with different Fingerprint ID
  - **not_found**: Fingerprint not found and new one must be created by posting to `/dfp/confirm` endpoint

- **message**: Additional information regarding the status

<table>
<thead>
<tr>
<th>Function</th>
<th>JSON Parameters</th>
<th>Response</th>
</tr>
</thead>
</table>
Validate NEW Fingerprint

```json
{
  "user_id" : "<USERNAME>",
  "host_address" : "<IP ADDRESS>",
  "fingerprint" : {
    "fonts" : "<FONT LIST>",
    "plugins" : "<PLUGIN LIST>",
    "timezone" : "<TIMEZONE>",
    "video" : "<VIDEOS>",
    "local_storage" : "<T OR F>",
    "session_storage" : "<T OR F>",
    "ie_user_data" : "<T OR F>",
    "cookie_enabled" : "<T OR F>",
    "user_agent" : "<USER AGENT INFO>",
    "accept" : "<ACCEPT INFO>",
    "accept_charset" : "<CHARSET INFO>",
    "accept_encoding" : "<ENCODING INFO>",
    "accept_language" : "<LANG INFO>"
  }
}
```

Example:

```json
{
  "user_id" : "jsmith",
  "host_address" : "111.222.33.44",
  "fingerprint" : {
    "fonts" : "Agency FB,Aharoni,Algerian,Andalus,Angsana New,AngsanaUPC ...",
    "plugins" : "ActiveTouch General Plugin Container: ActiveTouch General Plugin Container Version 105 ...",
    "timezone" : "America/Los_Angeles",
    "video" : "1920x1080x24",
    "local_storage" : "false",
    "session_storage" : "false",
    "ie_user_data" : "false",
    "cookie_enabled" : "true",
    "user_agent" : "Mozilla/5.0 (Windows NT 6.1; WOW64; rv: 41.0) Gecko/20100101 Firefox/41.0",
    "accept" : "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8",
    "accept_charset" : "",
    "accept_encoding" : "gzip, deflate",
    "accept_language" : "en-US,en;q=0.5"
  }
}
```

Refer to the table in the /dfp/js endpoint section for more information on the required fingerprint components

Validate KNOWN Fingerprint

```json
{
  "user_id" : "<USERNAME>",
  "host_address" : "<IP ADDRESS>",
  "fingerprint_id" : "<FP ID>",
  "fingerprint" : {
    "fonts" : "<FONT LIST>",
    "plugins" : "<PLUGIN LIST>",
    "timezone" : "<TIMEZONE>",
    "video" : "<VIDEOS>",
    "local_storage" : "<T OR F>",
    "session_storage" : "<T OR F>",
    "ie_user_data" : "<T OR F>",
    "cookie_enabled" : "<T OR F>",
    "user_agent" : "<USER AGENT INFO>",
    "accept" : "<ACCEPT INFO>",
    "accept_charset" : "<CHARSET INFO>",
    "accept_encoding" : "<ENCODING INFO>",
  }
}
```

```json
{
  "fingerprint_id" : "58e0f98642fe4354ba65a35a0d8b c6ff",
  "fingerprint_name" : "Windows 7 - Firefox 41.0",
  "score" : "100.00",
  "match_score" : "95.00",
  "update_score" : "80.00",
  "status" : "found",
  "message" : ""
}
```
Example:
{
  "user_id": "jsmith",
  "host_address": "111.222.33.44",
  "fingerprint_id": "58f0f98642fe4354ba65a35a0d8bc6ff",
  "fingerprint": {
    "fonts": "Agency FB, Aharoni, Algerian, Andalus, Angsana New, AngsanaUPC ...",
    "plugins": "ActiveTouch General Plugin Container: ActiveTouch General Plugin Container Version 105 ...",
    "timezone": "America/Los_Angeles",
    "video": "1920x1080x24",
    "local_storage": "false",
    "session_storage": "false",
    "ie_user_data": "false",
    "cookie_enabled": "true",
    "user_agent": "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:41.0) Gecko/20100101 Firefox/41.0",
    "accept": "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8",
    "accept_charset": "",
    "accept_encoding": "gzip, deflate",
    "accept_language": "en-US,en;q=0.5"
  }
}

### /dfp/confirm Endpoint

<table>
<thead>
<tr>
<th>HTTP Method</th>
<th>URI</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>POST</td>
<td>/api/v1/dfp/confirm</td>
<td><a href="https://secureauth.company.com/secureauth2/api/v1/dfp/confirm">https://secureauth.company.com/secureauth2/api/v1/dfp/confirm</a></td>
</tr>
</tbody>
</table>

Stores the new or updated fingerprints in the user profile in the directory.

If a fingerprint posted to the /dfp/validate endpoint returns a not_found or found_for_update status, then the information must be posted to the /dfp/confirm endpoint to create / update the fingerprint.

Once the fingerprint is validated, SecureAuth IdP returns a fingerprint_id, which is then posted to the confirm endpoint to create the entry.

<table>
<thead>
<tr>
<th>JSON Parameters</th>
<th>Success Response</th>
<th>Failure / Error Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>{</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
|   "user_id": "<USERNAME>",
   "fingerprint_id": "<FP ID>"
| }               |                     |                         |

Example:
{
  "user_id": "jsmith",
  "fingerprint_id": "58f0f98642fe4354ba65a35a0d8bc6ff"
}
If a server error is encountered, then the follow response is returned:

```json
{
    "status": "server_error",
    "message": "<Exception message describing the issue.>
}
```
HTTP Status 500

/behavbio Endpoints

Refer to Behavioral Biometrics Guide for more information on the feature

/behavbio/js Endpoint

<table>
<thead>
<tr>
<th>HTTP Method</th>
<th>URI</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET</td>
<td>/api/v1/behavbio/js</td>
<td><a href="https://secureauth.company.com/secureauth2/api/v1/behavbio/js">https://secureauth.company.com/secureauth2/api/v1/behavbio/js</a></td>
</tr>
</tbody>
</table>

Enables the application to retrieve the javascript reference that is required to gather and analyze a user's behavioral biometric profile.

Using the reference, most of the data required for the POST and PUT endpoints are provided; but the remaining information (user ID, host address, and user agent) must be provided by the application.

Response to request:

```json
{
    "src": "https://SecureAuthIdFQDN/SecureAuthIdPRealm/assets/scripts/api/behaveBio.obf.js?ver=9.0.0.22"
}
```
Sample Initialization Javascript

Code Example

```html
<form>
...
<input id="password" class="form-control" type="password" name="loginForm:Password" autocomplete="off" value="" placeholder="Password">
<input type="hidden" name="behavio_hidden" id="behavio_hidden">
<input id="textbox" class="form-control" type="text" name="loginForm:NotMonitored" autocomplete="off" value="" placeholder="Ignored">
...
</form>

<script>
$(document).ready(function() {
    secureAuth.api.behaveBio({
        anonymousByName: [],
        anonymousById: [],
        anonymousByType: ['password'],
        behavioHiddenId: ['behavio_hidden'],
        ignoreFields: ['loginForm:NotMonitored'],
        haveMouse: false
    });
});
</script>
```

Code Explanation

Form

- `<input type="hidden" name="behavio_hidden" id="behavio_hidden">` – Required anywhere in the `<form>` to create the behaviorProfile, with any preferred `name` and `id` values

- `<input id="password" class="form-control" type="password" name="loginForm:Password" autocomplete="off" value="" placeholder="Password">` – Example of input field with necessary components `id`, `type`, and `name` to identify anonymous fields

- `<input id="textbox" class="form-control" type="text" name="loginForm:NotMonitored" autocomplete="off" value="" placeholder="Not for Profile">` – Example of input field with necessary components `id`, `type`, and `name` to identify ignored fields

Script

Full script required in app code

- `anonymousByName` – Identifies anonymous fields by `name` (in `<input>`)
- `anonymousById` – Identifies anonymous fields by `id` (in `<input>`)
- `anonymousByType` – Identifies anonymous fields by `type` (in `<input>`, as shown in code example)
- `behavioHiddenId` – Calls to `<input type="hidden" ...>` line (required in `<form>`) with the same `id` value
- `ignoreFields` – Identifies fields to not include in the behaviorProfile by `name` (in `<input>`, as shown in code example)
- `haveMouse` – Monitors mouse movements as well as keystroke behavior (`true` or `false`)

/behavebio Endpoint

<table>
<thead>
<tr>
<th>HTTP Method</th>
<th>URI</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>POST</td>
<td>/api/v1/behavebio</td>
<td><a href="https://secureauth.company.com/secureauth2/api/v1/behavebio">https://secureauth.company.com/secureauth2/api/v1/behavebio</a></td>
</tr>
<tr>
<td>PUT</td>
<td>/api/v1/behavebio</td>
<td><a href="https://secureauth.company.com/secureauth2/api/v1/behavebio">https://secureauth.company.com/secureauth2/api/v1/behavebio</a></td>
</tr>
</tbody>
</table>

The **POST** method collects and creates the user's behavioral biometric profile
The **PUT** method resets the user's profile to enable retraining

**POST Endpoint**

At this endpoint, the user's behavioral biometric profile is created and then analyzed against subsequent profile information posted to the endpoint.

To utilize Behavioral Biometrics as a second factor, training must occur, which is simply the API gathering user keystroke, text input, and other factors while they fill out the application's provided fields (e.g. username, password, home address, phone number, etc.). Once a profile has been trained, the API can then return a score based on the comparison of the "normal" behavior and the current behavior. To **achieve a fully trained profile**, the fields must be filled out ten (10) times.

### Definitions

- **userID**: User's username
- **behaviorProfile**: User's behavioral biometric profile, generated by the javascript reference acquired in the `/behavebio/js` endpoint
- **hostAddress**: User's IP Address
- **userAgent**: User's user agent (computer / browser information)
- **TotalScore**: How similar the presented behavior is to the stored profile
- **TotalConfidence**: How confident the API is that the score is accurate
- **Device**: Type of device user employs
- **Results**: Breakdown of specific field scores
### JSON Parameters

```json
{
    "userId": "<USERNAME>",
    "behaviorProfile": '<BEHAVIORAL BIOMETRIC PROFILE>',
    "hostAddress": '<IP ADDRESS>',
    "userAgent": '<USER AGENT>'
}
```

### Success Response

- **Untrained Profile:**
  ```json
  {
    "BehaviorBioResults": {
      "TotalScore": 0.5,
      "TotalConfidence": 0,
      "Device": "DESKTOP",
      "Results": []
    },
    "status": "valid",
    "message": ""
  }
  ```

- **Trained Profile:**
  ```json
  {
    "BehaviorBioResults": {
      "TotalScore": 0.999999780,
      "TotalConfidence": 0.999780,
      "Device": "DESKTOP",
      "Results": [
        {
          "ControlID": "text#UserID",
          "Score": 0.99997949,
          "Confidence": 0.9997949,
          "Count": 10
        },
        {
          "ControlID": "password#Password",
          "Score": 0.99997807,
          "Confidence": 0.9997807,
          "Count": 10
        }
      ]
    },
    "status": "valid",
    "message": ""
  }
  ```

### Failure / Error Response

- **Request validation failed with: userId was not present.**
  ```json
  {
    "status": "invalid",
    "message": "Request validation failed with: userId was not present."
  }
  ```

- **Request validation failed with: behaviorProfile was not present.**
  ```json
  {
    "status": "invalid",
    "message": "Request validation failed with: behaviorProfile was not present."
  }
  ```

- **Request validation failed with: hostAddress was not present.**
  ```json
  {
    "status": "invalid",
    "message": "Request validation failed with: hostAddress was not present."
  }
  ```

- **Request validation failed with: userAgent was not present.**
  ```json
  {
    "status": "invalid",
    "message": "Request validation failed with: userAgent was not present."
  }
  ```
PUT Endpoint

At this endpoint, the user's trained profile information can be reset; this is especially useful after a user changes a password.

A profile can be completely reset, or specific fields from which behavior profile information is collected can be reset individually.

**Definitions**

**fieldName**: Name of field to reset (unique to application); or set to ALL for global reset.

**fieldType**: Type of field, either regulartext (actual values stored in profile) or anonymoustext (no actual values stored in profile, e.g. password entries); or set to ALL for global reset.

**deviceType**: Type of device used by user (Desktop or Mobile); or set to ALL for global reset.

**JSON Parameters**

<table>
<thead>
<tr>
<th>Success Response</th>
<th>Failure / Error Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>{</td>
<td>{</td>
</tr>
<tr>
<td>&quot;userId&quot;: &quot;&lt;USERNAME&gt;&quot;,</td>
<td>&quot;status&quot;: &quot;invalid&quot;,</td>
</tr>
<tr>
<td>&quot;fieldName&quot;: &quot;&lt;FIELD TO RESET&gt;&quot;,</td>
<td>&quot;message&quot;: &quot;Request validation failed with:</td>
</tr>
</tbody>
</table>
|   "fieldType": "<TYPE OF FIELD>", |   "userId was not present."
|   "deviceType": "<TYPE OF DEVICE>" |
| }                | }                        |

**Specific Field Reset Example:**

```json
{
   "userId": "jsmith",
   "fieldName": "UserID",
   "fieldType": "regulartext",
   "deviceType": "DESKTOP"
}
```

**Global Reset Example:**

```json
{
   "userId": "jsmith",
   "fieldName": "ALL",
   "fieldType": "ALL",
   "deviceType": "ALL"
}
```