Multi-Factor Authentication API Guide

Updated December 2, 2019

Introduction

Use this guide to configure the SecureAuth Authentication API to access user information, including Multi-Factor Authentication mechanisms configured for that profile.

Prerequisites

1. Complete the steps in the Authentication API guide.

2. Configure the realm to enable Multi-Factor Authentication Methods.

Endpoint

The **/users/{username}/factors** endpoint uses the **GET** method to access the end-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

GET

HTTP Method	URI	Example
GET	`/api/v2/users/{username}/factors`	`https://secureauth.company.com/secureauth2/api/v2/users/jsmith/factors`

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.)

GET Endpoint Response Examples

Success


```
{
  "status": "found",
  "message": "",
  "user_id": "jsmith",
  "factors": [
    {
      "type": "phone",
      "id": "Phone1",
      "value": "123-456-7890",
      "capabilities": [
        "call"
      ]
    },
    {
      "type": "phone",
      "id": "Phone2",
      "value": "987-654-3210",
      "capabilities": [
        "sms",
        "call"
      ]
    },
    {
      "type": "email",
      "id": "Email1",
      "value": "jsmith@company.com"
    },
    {
      "type": "kbq",
      "id": "KBQ1",
      "value": "What city were you born in?"
    },
    {
      "type": "kbq",
      "id": "KBQ2",
      "value": "What was your favorite childhood game?"
    },
    {
      "type": "kbq",
      "id": "KBQ3",
      "value": "What was your dream job as a child?"
    },
    {
      "type": "kbq",
      "id": "KBQ4",
      "value": "Who is your personal hero?"
    },
    {
      "type": "kbq",
      "id": "KBQ5",
      "value": "What is the last name of your favorite
school teacher?"
    },
    {
```


Fail / Error


```
{
  "status": "not_found",
  "message": "User Id was not found"
}
HTTP Status 404
```

```
{
  "status": "invalid_group",
  "message": "User Id is not associated with a
valid group."
}
HTTP Status 200
```

```
{
  "status": "disabled",
  "message": "Account is disabled."
}
HTTP Status 200
```

```
{
  "status": "lock_out",
  "message": "Account is locked out."
}
HTTP Status 200
```

```
{
  "status": "password_expired",
  "message": "Password is expired."
}
HTTP Status 200
```


See **Server Error** information below

If a server error is encountered, then the follow response is returned:


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


Related documentation

Symbol-to-Accept API endpoints

Biometric API endpoints

API configuration guide

Authentication API configuration