## Contents

1.1 SOLUTION SUMMARY ........................................................................................................... 3
1.2 PREREQUISITES ................................................................................................................. 3
1.3 HTML URL FORMAT .......................................................................................................... 3
1.4 HTML POST FORMAT ....................................................................................................... 4
1.5 FLOW DIAGRAM .............................................................................................................. 5
1.6 EXAMPLE HTML URL FOR TWO STEP SMS REALTIME ................................................. 6
1.7 EXAMPLE HTML POST FOR TWO STEP SMS REALTIME AUTH .................................... 7
1.8 EXAMPLE POST FOR PRE-LOADED SMS IN ONE STEP AUTH ..................................... 8
1.9 EXAMPLE HTML POST FOR PUSH WITH OFF-LINE FAILOVER AUTH ....................... 9
1.1 Solution Summary

The following document provides a guide to authenticating users for 2FA through SecurEnvoy’s SecurAccess MFA solution using HTML POST.

1.2 Prerequisites

The following conditions are required to successfully authenticate users through the Authentication API:

- A SecurAccess MFA server installed, configured and working on a system with:
  - Windows Server 2012 R2 or higher.
  - An LDAP or Lightweight Directory Service database of users or alternative user database (SQL etc) if SecurAccess is only to provide the second stage (2FA) of the authentication process.

Note: Please see SecurEnvoy’s SecurAccess version 9.3 deployment guide on how to setup MFA server solution (On the www.securenvoy.com website)

1.3 HTML URL Format

Note: Both GET (URL format) and POST html requests are supported. Note that POST is considered better security as URL data can be cached in the browser.

http(s)://your_securenvoy_server_ip/secserver?FLAG=DESKTOP&VERSION=2.0&STATUS=AUTH&USERID=(my_userid)&PASSCODE=(6 digit passcode to check)&SESSIONKEY=(SESSIONKEY value if known)&CUSTOMMESSAGE=(optional pushsms message)
1.4 HTML Post Format

POST to http(s)://your_secureenvoy_server_ip/seceserver/securectrl.exe

Headers
Content-Type: text/html; charset=UTF8

Data

FLAG: DESKTOP
VERSION:2.0
STATUS:AUTH
USERID:(Userid of user authenticating including domain example fred@mydomain.com)
PASSCODE:(6-digit passcode to check)
SESSIONKEY:(return this from previous SESSIONKEY value if known)
CUSTOMMESSAGE:(optional push message URL Encoded with UTF8)

Return

VERSION:9.1.501 (the server sides version for information only)
RETURN:OK or ERR and an error message
AUTH:OK, DENIED or CHALLENGE

Additional Return If AUTH: CHALLENGE

SESSIONKEY:(This key MUST be return in the next connection)
REALTIMECHALLENGE:(Optional, if return this text should be displayed to the user)
1.5 Flow Diagram

- Send Data to Server
- Challenge
- Return
  - Ok
  - Auth
    - Deny
      - Access Denied
    - Ok
      - Access Accepted
- Exit and Display Error Message
### 1.6 Example HTML URL for Two Step SMS Realtime

**Step 1:** Client sends the following URL

https://your_secureenvoy_server/secserver?FLAG=DESKTOP&VERSION=2.0&STATUS=AUTH&USERID=fred@mydomain.com&PASSCODE=

**Step 2:** Server returns

<table>
<thead>
<tr>
<th>VERSION</th>
<th>9.1.501</th>
</tr>
</thead>
<tbody>
<tr>
<td>RETURN</td>
<td>OK</td>
</tr>
<tr>
<td>AUTH</td>
<td>CHALLENGE</td>
</tr>
<tr>
<td>SESSIONKEY</td>
<td>SE4E3A0A6202452F87F5757AD407003AA4D5295BB2</td>
</tr>
<tr>
<td>REALTIMECHALLENGE</td>
<td>Enter Your 6 Digit Passcode</td>
</tr>
<tr>
<td>GETPASSCODE</td>
<td>True</td>
</tr>
</tbody>
</table>

**Step 3:** As CHALLENGE was returned, client sends the following

https://your_secureenvoy_server/secserver?FLAG=DESKTOP&VERSION=2.0&STATUS=AUTH&USERID=fred@mydomain.com&PASSCODE=234123&SESSIONKEY=SE4E3A0A6202452F87F5757AD407003AA4D5295BB2

**Step 4:** Server returns:

<table>
<thead>
<tr>
<th>VERSION</th>
<th>9.1.501</th>
</tr>
</thead>
<tbody>
<tr>
<td>RETURN</td>
<td>OK</td>
</tr>
<tr>
<td>AUTH</td>
<td>OK</td>
</tr>
</tbody>
</table>
1.7 Example HTML POST for Two Step SMS Realtime Auth

Step 1: Client sends the following raw data

Content-Type: text/html; charset=UTF8 (2 carriage returns to end html headers)

FLAG:DESKTOP
VERSION:2.0
STATUS:AUTH
USERID:fred@mydomain.com (the userid of the user authenticating)
PASSCODE: leave this blank as it's not known at this stage)

Step 2: Server returns

VERSION:9.1.501
RETURN:OK
AUTH:CHALLENGE
SESSIONKEY:SE4E3A0A6202452F87F5757AD407003AA4D5295BB2
REALTIMECHALLENGE:Enter Your 6 Digit Passcode
GETPASSCODE:True

Step 3: Client sends the following

FLAG:DESKTOP
VERSION:2.0
STATUS:AUTH
USERID:fred@mydomain.com (the userid of the user authenticating)
PASSCODE:234123  (The 6 digit passcode entered by the user)
SESSIONKEY:SE4E3A0A6202452F87F5757AD407003AA4D5295BB2

Step 4: Server returns:

VERSION:9.1.501
RETURN:OK
AUTH:OK
### 1.8 Example POST for Pre-Loaded SMS In One Step Auth

**Step 1:** Client sends the following

Content-Type: text/html; charset=UTF8
FLAG:DESKTOP
VERSION:2.0
STATUS:AUTH
USERID:fred@mydomain.com (the userid of the user authenticating)
PASSCODE:234123 (The 6 digit passcode entered by the user)

**Step 2:** Server returns

VERSION:9.1.501
RETURN:OK
AUTH:OK
1.9 Example HTML POST for Push with off-line failover Auth

Step 1: Client sends the following raw data

Content-Type: text/html; charset=UTF8 (2 carriage returns to end html headers)

FLAG:DESKTOP
VERSION:2.0
STATUS:INIT (this will send the push request to the user)
CUSTOMMESSAGE:(optional, message to display in push notification, must be URL encoded with UTF8)
USERID:fred@mydomain.com (the userid of the user authenticating with PUSH)

Step 2: Server returns

VERSION:9.1.501
RETURN:OK
GETPASSCODE:False (Push returned OK and Authentication is OK)
    OR
GETPASSCODE:True (Push rejected or timed out, need to prompt for a passcode)

Step 3: Only required if GETPASSCODE: True returned

FLAG:DESKTOP
VERSION:2.0
STATUS:AUTH
USERID:fred@mydomain.com (the userid of the user authenticating)
PASSCODE:234123 (The 6 digit passcode entered by the user)

Step 4: Server returns:

VERSION:9.1.501
RETURN:OK
AUTH:OK
Please Reach Out to Your Local SecurEnvoy Team...

UK & IRELAND
The Square, Basing View
Basingstoke, Hampshire
RG21 4EB, UK
Sales
E sales@SecurEnvoy.com
T 44 (0) 845 2600011
Technical Support
E support@SecurEnvoy.com
T 44 (0) 845 2600012

EUROPE
Freibadstraße 30,
81543 München, Germany
General Information
E info@SecurEnvoy.com
T +49 89 70074522

ASIA-PAC
Level 40 100 Miller Street
North Sydney
NSW 2060
Sales
E info@SecurEnvoy.com
T +61 9911 7778

USA - West Coast
Mission Valley Business Center
8880 Rio San Diego Drive
8th Floor San Diego CA 92108
General Information
E info@SecurEnvoy.com
T (866) 777-6211

USA - Mid West
3333 Warrenville Rd
Suite #200
Lisle, IL 60532
General Information
E info@SecurEnvoy.com
T (866) 777-6211

USA - East Coast
373 Park Ave South
New York,
NY 10016
General Information
E info@SecurEnvoy.com
T (866) 777-6211

www.securenvoy.com