Self-Service Verification Value-Added Module (VAM) Deployment Guide
Copyright Information

©2018. SecureAuth® is a registered trademark of SecureAuth Corporation. SecureAuth’s IdP software, appliances, and other products and solutions are copyrighted products of SecureAuth Corporation.

Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>2017-03-28</td>
<td>Initial draft</td>
</tr>
<tr>
<td>1.0</td>
<td>2017-09-27</td>
<td>First version</td>
</tr>
<tr>
<td>2.0</td>
<td>2018-07-23</td>
<td>Second version</td>
</tr>
<tr>
<td>2.01</td>
<td>2018-09-4</td>
<td>Known limitation noted</td>
</tr>
</tbody>
</table>

For information on support for this module, contact your SecureAuth support or sales representative:

Email: support@secureauth.com  
inside-sales@secureauth.com

Phone: +1.949.777.6959 or +1-866- 859-1526

Website: https://www.secureauth.com/support  
https://www.secureauth.com/contact
Table of Contents

Introduction ........................................................................................................................................... 4
Benefits .................................................................................................................................................. 4
Prerequisites ........................................................................................................................................ 4
Installing the VAM .............................................................................................................................. 5
Configuring SA IdP for the VAM .......................................................................................................... 7
Use Case: How the VAM Works ........................................................................................................... 8
Introduction
Self-Service Verification provides a method for validating that contact information has been updated properly. While the normal self-service post-authentication page allows the user to update their contact information (such as emails and phone numbers), there is no assurance that the user has updated with a valid phone number or email.

The Self-Service Verification page enforces validity of the updated information. Once a user changes their email address or phone number, they are directed to verify that change with an OTP code sent to either their email or phone.

NOTE: Currently this VAM only supports sending SMS to U.S. phones. Non-U.S. phones are not yet supported.

Benefits

- Acts as a safeguard to make sure the contact information is always valid
- Supports OTP verification of updated account information

Prerequisites
The basic requirement for using the Self-Service Verification VAM is the presence of SecureAuth IdP version 8.2 or later.
Installing the VAM
To install this VAM, perform the following steps:

1. Download the installer for the Self-Service Verification module to the root directory where SecureAuth IdP resides.
2. Double-click the installer to start the VAM installation.
3. Click past the Introduction screen, until the End-User License Agreement screen appears like Figure 1.

![End-User License Agreement](image)

**FIGURE 1.** End-User License Agreement

4. Check the ‘I accept the terms...’ box then click **Next**.
The Product Activation screen appears like Figure 2.

![Product Activation Screen](image)

**FIGURE 2.** Product Activation Screen

1. Enter the Name, Email, and Organization exactly as it was initially entered in SecureAuth IdP. Enter the Serial Key that was given to you and click **Next**.

The Product Setup screen appears like Figure 3.

![Product Setup Screen](image)

**FIGURE 3.** Product Setup Screen

2. From the ‘Realm’ drop-down list, choose the realm you want to install to, and click **Next**.
3. Continue to the Finish screen and click **Finish** to start the installation process.
Configuring SA IdP for the VAM

Once the VAM is installed, you must enter the values in SecureAuth IdP required to make it function properly with the VAM. To do this:

1. In SecureAuth IdP Web Admin console, create a realm to handle this Self-Service Verification VAM integration. Configure the following tabs in the Web Admin Console before configuring the **Post Authentication** tab:
   - **Overview** - the description of the realm and SMTP connections must be defined
   - **Data** - an enterprise directory must be integrated with SecureAuth IdP
   - **Workflow** - the way in which users access this application must be defined
   - **Multi-Factor Methods** - the MFA methods that are used to access this page (if any) must be defined

   **NOTE:** Currently the realm handing the Self-Service Verification page can only be applied to the Light and Dark themes. Future versions of this VAM will accommodate the full range of IdP themes.

   For information on doing this, refer to the *SecureAuth IdP Realm Guide*.

2. In SecureAuth IdP Web Admin Console, select the realm customized for this VAM and click the **Post Authentication** tab page.

3. From the ‘Authenticated User Redirect’ option list, select the **Use Custom Redirect**, then in the ‘Redirect To’ field, enter `Customized/AccountUpdateVerify.aspx` (the file generated by the VAM that directs the interface how to display certain web pages) as illustrated in Figure 4.

   **FIGURE 4.** Post Authentication Page 1

4. Click **Save** to save these changes.
Use Case: How the VAM Works

Once the Post Authentication page is configured for the required realm, any user seeking to change one of their currently listed emails, phone numbers, or other relevant data can do so using a workflow like this.

1. The user proceeds through the steps required to authenticate (according to the workflow previously configured for that). A common workflow is shown in Figure 5.

FIGURE 5. Authentication Pathway
If authentication is successful, the VAM-customized data fields page appears for the requesting user. These contain the current values assigned to the user profile for that user as shown in the example in Figure 6.

**FIGURE 6. VAM-Customized Data Field Page**

Notice that there is a **Send Code** button to the right of each changeable field, two radio buttons indicating the method of sending (**Voice** or **Text**) and an inactive **Update** button at the bottom.

2. If the user needs to update a phone number, for example, they must first enter the new number in the chosen field, then select the method for verifying this change by clicking one of the available radio buttons (**Voice** or **Text**), and then click the **Send Code** button to the right of the changed field as shown in Figure 7.

**FIGURE 7. Sending a New Number Example**
A message appears below the changed field indicating that an OTP code has been sent to the user’s new number via text or voice. A new Validate field appears below the changed field like Figure 8.

3. In the Validate field, enter the OTP code that was sent to the new number, then click Validate.

If this code was correct, a message appears like Figure 9 indicating that the phone number has been verified.

4. Click the Update button to confirm the change and make it permanent.
If the user chooses to update their email address, the steps are identical, as shown in Figure 11.

**FIGURE 11. Email Change Workflow**