Epic ePCS 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.
Version 1.0

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>Features</td>
<td>4</td>
</tr>
<tr>
<td>Process Flow Example</td>
<td>5</td>
</tr>
<tr>
<td>Use Examples</td>
<td>6</td>
</tr>
<tr>
<td>Soft-Token ePCS Second Factor</td>
<td>6</td>
</tr>
<tr>
<td>Soft-Token ePCS with Password</td>
<td>7</td>
</tr>
<tr>
<td>Push-to-Accept ePCS</td>
<td>7</td>
</tr>
<tr>
<td>Installation</td>
<td>10</td>
</tr>
<tr>
<td>Epic Configuration</td>
<td>11</td>
</tr>
<tr>
<td>IdP Configuration</td>
<td>11</td>
</tr>
<tr>
<td>Testing</td>
<td>14</td>
</tr>
<tr>
<td>Best Practices</td>
<td>16</td>
</tr>
<tr>
<td>Update Warning</td>
<td>16</td>
</tr>
</tbody>
</table>
Introduction
SecureAuth’s Epic ePCS Value-Added Module (VAM) enables seamless integration between SecureAuth IdP’s Multi-Factor Authentication (MFA) and Epic’s Hyperspace platform for the E-Prescribing of Controlled Substances (ePCS) system. Using this integrated package, qualified physicians can write prescriptions quickly and securely while meeting DEA requirements for e-prescribing.

This guide also includes instructions on installing and configuring the VAM that enables the link between Epic Hyperspace and SecureAuth IdP.

Why select SecureAuth IdP?

SecureAuth’s flexible authentication framework allows providers to deploy DEA compliant Two-Factor Authentication (2FA) in ways that are not intrusive on physicians; and in many cases SecureAuth can actually optimize workflows by reducing clicks. Its aim is to provide the quickest way to ensure that the accessing physician is the one authorized to approve the prescription, per DEA standards.

Features

+ Seamless integration into preexisting Epic e-prescribing workflows
+ Multiple authentication methods that not only meet DEA regulation but make 2FA easy for physicians – such as push-to-accept, fingerprint, and other DEA-compliant methods
+ Flexible authentication platform that allows providers to select the 2FA method which best conforms to workflow requirements for e-prescribing
Process Flow Example

The process flow using the Epic ePCS VAM is shown in Figure 1.

**FIGURE 1. Process Flow Example Using Epic ePCS**
Use Examples

Soft-Token ePCS Second Factor

The following example illustrates a commonly-deployed 2FA method that utilizes mobile devices featuring FIPS 140-2-compliant One-Time-Password (OTP) tokens. This method is easy for the physicians to use, and because of its FIPS 140-2 compliance, it meets the DEA’s requirement for 2FA.

In this example:

1. The physician enters his/her user name.
   The physician is prompted for a method to receive the required passcode. The passcode is sent by way of the specified device.
2. The physician enters the received passcode then presses Enter.

The physician has entry to the ePCS system.
Soft-Token ePCS with Password

In a variation on the first example, the process requires the physician to perform soft-token ePCS second factor as shown in the following illustration examples (using both a password and a passcode):

1. The physician enters a user name.
   The physician is prompted for a method to receive the required passcode. The passcode is sent by way of the designated device.
2. The physician enters the received passcode then presses Enter.
   The physician is prompted to present their fingerprint at the fingerprint touch reader. The reader can be on an attached dedicated reader, a desktop computer, a laptop, or a smart phone.
3. The physician presents their fingerprint to the reader.
   Reading a fingerprint is compliant with the FIPS 140-2 standard.

The physician is then required to submit their fingerprint to the fingerprint touch screen before entrance to the system is allowed.

The ePCS data is accessible to the physician.

Push-to-Accept ePCS

To comply with DEA requirements while providing the quickest possible access, SecureAuth IdP also features push-to-accept with TouchID for ePCS authentication. Many providers are moving to push-to-accept with TouchID because it not only reduces the number of clicks and character entries a physician has to perform, but also incorporates all three of the authentication factors identified by the DEA:
+ Something you know (username/password)
+ Something you have (mobile device)
+ Something you are (fingerprint for TouchID)

An example of the process required to perform push-to-accept ePCS 2FA is shown in the following illustration example:

Essentially, the path is:

1. The physician opens the application on his/her smart phone or other PC.
   The application prompts the prospective physician for authentication. At the same time, the secondary device is activated.
2. The physician pushes a button on the device to accept the request for entry.

The application allows entry to the required data.
If Push-to-Accept is used with accounts that have multiple registered mobile devices, a screen appears with a list of mobile devices from which the user can select, as shown below.

SecureAuth Login Device

Press Enter to start the Push-to-Accept request.

- XT1254
- iPhone

Enter
Cancel
Installation

To configure SecureAuth IdP for the Epic ePCS VAM:

1. Designate a realm in your SecureAuth appliance to provide API access to the SecureAuth Epic ePCS VAM.
2. Follow the steps provided in https://docs.secureauth.com/x/sgljAg to enable the Authentication API.
3. Set the realm designated for the Authentication API to enable access to the profile attribute that stores the OATH seed for the OTP.
   Make sure the Data tab of the API realm has the proper profile attributes and the OATH OTP registration method is configured.

To install and configure the Epic ePCS VAM:

1. Copy the provided ZIP file to a temporary location on the server running Epic Hyperspace. This is usually a server that can be accessed using a virtual desktop infrastructure (VDI).
2. Extract the provided ZIP archive to the same temporary location on the server.
3. Copy the SecureAuth folder contained in the extracted ZIP archive to the C: drive root.
4. Open the SecureAuth folder, now located at C:\SecureAuth\, and run the RegisterSALoginDevice.bat as an Administrator.
   This will add SecureAuthLoginDevice.dll to the server’s code base.

   **NOTE:** By executing this .bat file, this SecureAuth Epic ePCS VAM is automatically registered on the Citrix server, enabling you to bypass regsvr32 for this DLL.

5. Open SASettings.xml using Notepad or a comparable text editor and modify the following settings:

<table>
<thead>
<tr>
<th>SecureAuthAPIUrl</th>
<th>The URL used to access the Authentication API realm defined in the SecureAuth Configuration. It must be accessible by HTTPS and the certificate used to serve the SSL connection must be trusted by the Epic Hyperspace server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ePCSUrl</td>
<td>References the local host running Epic Hyperspace. This URL should not be changed.</td>
</tr>
<tr>
<td>AppID</td>
<td>The AppID provided by the Authentication API settings in the SecureAuth appliance as defined by the Authentication API realm defined above.</td>
</tr>
<tr>
<td>AppKey</td>
<td>The AppKey provided by the Authentication API settings in the SecureAuth appliance as defined by the Authentication API realm defined above.</td>
</tr>
<tr>
<td>Retry</td>
<td>Indicates the number of attempts a user has to correctly enter his/her OTP before the Epic ePCS VAM returns to Epic and fails to authenticate the message.</td>
</tr>
</tbody>
</table>

SecureAuth

www.secureauth.com

+1 949-777-6959
Epic ePCS Value-Added Module (VAM) Deployment Guide

<table>
<thead>
<tr>
<th>LogLevel</th>
<th>The default value should be set to 0 which turns off logging. Do not change this value unless instructed to do so by a SecureAuth Engineer.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WindowTitle</td>
<td>Indicates the title text that will display on the Epic ePCS VAM dialog box.</td>
</tr>
<tr>
<td>RequirePassword</td>
<td>If set to 1, the user will be required to enter their password for the configured data store in the Authentication API realm when using the Epic ePCS VAM.</td>
</tr>
<tr>
<td>LogoPath</td>
<td>Specifies the full path on the disk of the custom logo image displayed in the Epic ePCS VAM. For example: C:\SecureAuth\logo.png</td>
</tr>
<tr>
<td>EnablePush</td>
<td>Enables Push-to-Accept as the second factor method as provided by the Epic ePCS VAM. To enable, set this value to 1. The default value is 0 (push-to-accept disabled). If the Push-to-Accept method is used with accounts that have multiple registered mobile devices, the software will display a list of devices from which the user can select. + If no devices are found, the software will notify the user + If only one device is found, it will automatically send the push request without waiting for a selection</td>
</tr>
<tr>
<td>PreferStaticPin</td>
<td>Enables or disables the static PIN feature. If set to 0, it indicates the use of TOTP (OATH) token. If set to 1, it enables the use of a static PIN. If this feature is enabled and the user has a static PIN, it will verify against the static PIN. If no PIN is found for the user, it will default to using a standard TOTP token.</td>
</tr>
</tbody>
</table>


**Epic Configuration**

Follow the Epic documentation for the steps required to add a new authentication provider. Epic will ask for the Login Device Programmatic ID (Pronged). Add this value to that field:

SecureAuthLoginDevice.Receiver.

**NOTE:** Epic documentation is only available to registered customers. The documents section only appears once the user has signed in.

**IdP Configuration**

Configuring SecureAuth IdP for use with Epic ePCS involves the creation of a realm dedicated to handling the necessary API instructions.

**NOTE:** Configuring SecureAuth IdP for use with Epic ePCS should be handled, at least initially, by the SecureAuth deployment staff and should not be the client’s responsibility.

To create an API-specific realm, do this:

1. Open SecureAuth IdP Web Admin.
   Make sure you have an on-premises directory with which SecureAuth IdP can integrate.
2. Create a new realm in which the API instructions will be enabled.
   For detailed instructions on doing this, refer to the SecureAuth IdP Realm Guide.

3. Click the Data tab, configure the required fields, then click Save.
   A directory integration is required for SecureAuth IdP to pull user profile information during the login process.

4. Click the API tab and scroll down to the API Key section.

5. Check Enable API for this realm box.

6. Click the Generate Credentials button to create a new Application ID and Application Key. The Application ID and Application Key are unique per realm.

   **NOTE:** The API key looks like it is comprised of 64 random characters, but it is actually composed of 32 two-character hexadecimal values. This is important when using the API key to produce the required HMAC hash.

7. Click the Select & Copy button to copy the contents from the fields. These values will be required in the HTTP Header configuration.

8. Scroll down to the API Permissions section.

9. Check the Enable Authentication API box.

10. If required, check one or more Identity Management tools to include in the API.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User management – add, update, and retrieve users and their properties</td>
<td>Use this tool to add new user profiles, and to retrieve and update existing user profiles. Updating a user profile includes setting and/or clearing property values in the user profile.</td>
</tr>
<tr>
<td>Administrator initiated password reset</td>
<td>Use this tool to let an administrator send the end-user a new password requested via an application. Use case scenario: the end-user requests a new password because the current one has been forgotten.</td>
</tr>
<tr>
<td>User self-service password change</td>
<td>Use this tool to let the end-user enter both the current password and create a new password. This tool is used in conjunction with the administrator-initiated password reset option: the end-user enters the password sent by the administrator (the current password) then enters a new password.</td>
</tr>
<tr>
<td>User &amp; group association (LDAP)</td>
<td>Use this tool to enable associations between existing users and groups within the LDAP data store.</td>
</tr>
</tbody>
</table>

11. Click **Save**.

A more detailed discussion of API configuration, HTTP header formation, and optional configurations can be found on-line in the **Authentication API Guide**.
Testing
Epic provides a standalone .NET Testing tool that can be used to verify that the Epic ePCS VAM is working before adding it into Hyperspace’s configuration. The steps below outline how to use the tool.

1. From the SecureAuth folder, open the Test folder.
2. Click to initiate the StandAloneNETTester.exe file. The following window appears:

   ![Testing Window](image)

   Enter the value SecureAuthLoginDevice.Receiver in the ProgID field.

3. In the ProgID field, enter: SecureAuthLoginDevice.Receiver.
4. Click Authenticate.

   A Request Form window like this example appears.
5. In the ‘Key’ field, enter: **UserID**.
6. In the ‘Value’ field, enter the username for the user to be tested.
7. Click the **Add Data** button.
8. Click the **Return True** button.

The Epic ePCS VAM appears. If the device completes successfully, the ‘Results’ field on the Main Form updates with a success; otherwise the ‘Results’ field displays a “Perform Action Failed” condition.
Best Practices
There are only a few points to consider when evaluating best practices for the Epic ePCS tool:

+ Make sure your Citrix server is configured and running properly. For information on doing this, refer to your Citrix user guide.
+ Make sure to run the RegisterSALoginDevice.bat file to automatically register the SecureAuthLoginDevice.dll file.

Update Warning
The process of updating SecureAuth IdP software to a newer version may cause the SecureAuth Epic ePCS module to become invalid and the adapter itself to stop working. Until this feature is included in the main product, these customizations will need to be merged into any future updates.

Please contact tailoringfrontline@secureauth.com before making any updates.