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

Introduction ................................................................................................................................. 4
Deployment and Setup .................................................................................................................. 5
  Prerequisites ............................................................................................................................. 5
  Configuration ............................................................................................................................ 5
Introduction

This document details the deployment and configuration of the Value-Added Module (VAM) that enables Epic CareLink system applications to access SecureAuth IdP for authentication and authorization.
Deployment and Setup
This section details the steps required to deploy and configure the VAM for Epic CareLink.

Prerequisites
Download the following VAM files to the computer where the SecureAuth IdP appliance resides:
- CareLink.aspx
- CareLink.aspx.cs

These files are supplied by the SecureAuth sales engineer or representative once you have purchased the necessary VAM license.

Configuration
Here are the steps required to integrate this VAM with SecureAuth IdP:

1. In SecureAuth IdP Web Admin console, create a realm to handle Epic CareLink security.
   It is only necessary to specify the name and other basics for this realm. The details come later.
   For more information on creating a new realm, refer to https://docs.secureauth.com/display/91docs/SecureAuth+IdP+Realm+Guide.

2. Create a \Customized subdirectory under the directory containing the IdP data for that Epic CareLink realm.
   For example, if you have created a realm to handle Epic CareLink security and called it SecureAuth23 like this:
   [LocalComputer]\SecureAuth\SecureAuth23
   you would create a subdirectory like this:
   [LocalComputer]\SecureAuth\SecureAuth23\Customized

3. Copy the two downloaded files to this new \Customized subdirectory like this:
   • [LocalComputer]\SecureAuth\SecureAuth23\Customized\CareLink.aspx
   • [LocalComputer]\SecureAuth\SecureAuth23\Customized\CareLink.aspx.cs

4. At the IdP Web Admin console, select the new realm and go to System Info tab page.
5. Scroll down to the Links section and click the Web Config Editor link.
The Web.config file appears like Figure 1.

6. Scroll down to the <appSettings> section like this example:
   
   ```xml
   <appSettings>
   <add key="CareLinkCert" value="4ca3ecc93e45d669105aba5fd12ac8b3ea3f6820"/>
   <add key="CareLinkPost" value="http://epic.com/EpicCareLink/common/epic_check.asp?mode=SAML"/>
   </appSettings>
   
   7. Make changes to the CareLinkCert values as required.
   It is not necessary to remove spaces for the CareLinkCert value; the Post Authentication page handles that automatically. This value is the thumbprint for the certificate to be used.
   To find the thumbprint:
   a. Open CertMgr in Windows on the machine where this realm resides.
   b. Locate the certificate.
c. From the **Details** tab, select the thumbprint entry which then populates the box at the bottom as shown in Figure 2.

![Certificate Details Window](image)

*FIGURE 2. Certificate Details Window*

d. Copy the value from the window then paste that value into the realm’s Web Config Editor file.

If necessary, copy the required text into a text editor, like Notepad or OneNote, to modify it, then paste it back into the Web Config Editor file.

![Web Editor File Section](image)

*FIGURE 3. Web Editor File Section*

e. Save changes and exit the Web Config Editor.

8. From the Web Admin console, go to the Post Authentication page and specify these values as shown in Figure 4 on page 5.

   • Authenticated User Redirect: select **Use Custom Redirect**
   • Redirect To: enter the location and name of the aspx file you copied to the \Customized subdirectory in Step 3.
FIGURE 4. Post Authentication Example

Epic CareLink integration requires a post authentication event (CareLink.aspx) to send a signed XML POST to the Epic CareLink application.

**NOTE:** The certificate must reside on both the SecureAuth appliance in the LocalComputer\Personal Store as well as the Epic CareLink server and be accessible by both applications. The certificate on the SecureAuth Appliance must have a private key.