SECUREAUTH

Welcome to Better Identity.

Best Practices Guide to RSA Migration

Table of Contents

Introduction

The RSA Migration Module provides a migration path for our customers leading away from RSA security tokens and toward more advanced authentication methods. Customers can continue to use their existing RSA tokens when authenticating to SecureAuth IdP, allowing a phased retirement of the legacy hard token technology. This gives SecureAuth IdP the ability to validate RSA soft and hard tokens by using the RSA RADIUS Validation client.

Because the integration utilizes RADIUS, the RSA Migration Module can be used with RSA and other legacy hard token modules.

The RSA Migration Module is one of SecureAuth's value-added modules (VAM), a suite of software components developed by SecureAuth's Tailoring Frontline Services to fit the needs of customers seeking a simple way to adapt their system to the SecureAuth IdP cybersecurity solution.

Benefits

The benefits derived from the use of RSA Migration Module are:

+ Once migrated from RSA, customers enjoy a dramatically lower administration cost, improved user uptime, and greater customer satisfaction

+ Support for RADIUS validation of RSA soft and hard tokens

+ Support for any vendor that currently uses a non-SecureAuth token and supports a RADIUS client validation process

Solution Architecture

The essential architecture of the RSA Migration Module solution is described in this section.

Topology

An illustration of the RSA Hard Token topology is shown in Figure 1.
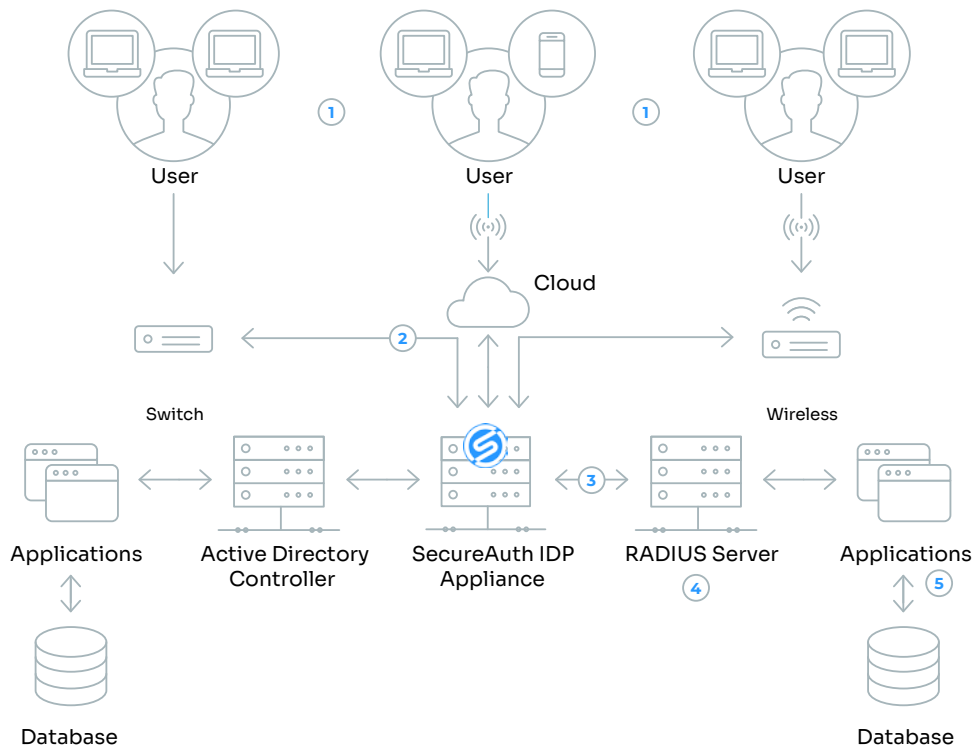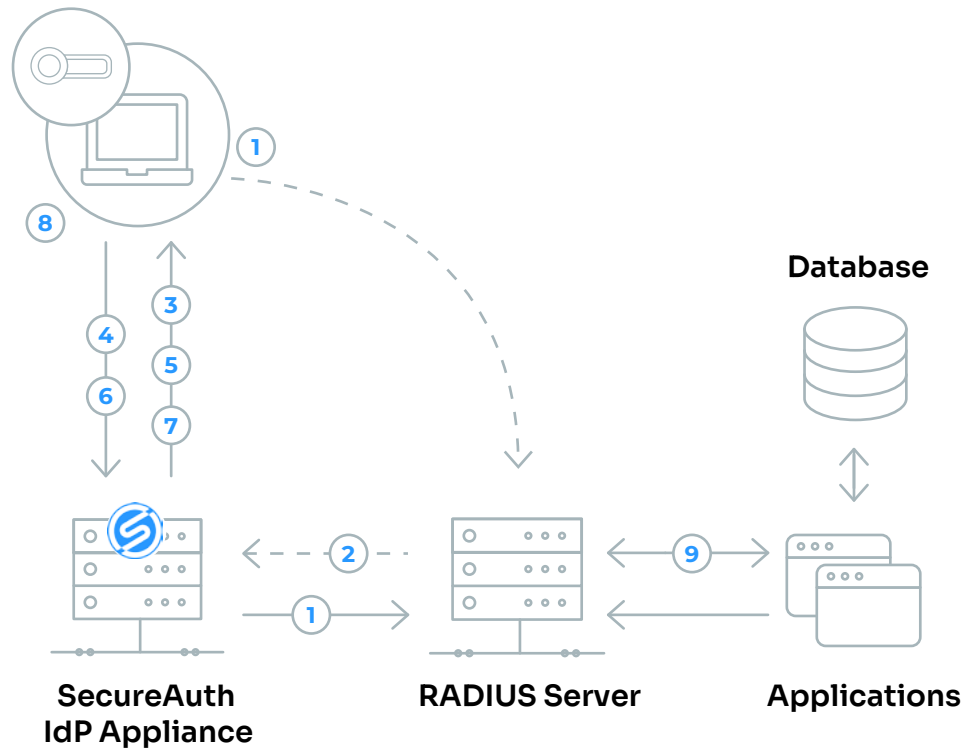

Figure 1.
RSA Hard Token Topology Example

The following steps describe the process ow (refer to the circled numbers above):

1. An external user enters a well-known application address in a web browser for a federation- or non-federation-aware application utilizing SecureAuth IdP for its main authentication. The application address entered reaches the SecureAuth IdP appliance.

2. The request is mediated by SecureAuth IdP. The user name and password, along with multi- factor authentication, is performed depending on the SecureAuth realm configuration.

    During multi-factor authentication, the SecureAuth IdP application validates using a user's hard token (in the form of a key fob, chip, password + token, password, passcode, or other accepted method).

    The validation of the hard token via SecureAuth IdP is a RADIUS request back to the RSA or other token validation system via RADIUS.

3. The applications and data overseen by the RADIUS server is then made available to the authenticated requester.

4. The applications and data overseen by the RADIUS server is then made available to the authenticated requester.

While the RSA Migration Module was designed for use with the RSA hard token, there are, in fact, other RADIUS server providers, such as Vasco, Defender, and SafeNet, that can be used with this VAM.

RSA Hard Token Process Flow

Figure 2.
RSA Hard Token Process Flow

A more detailed example of the process ow would include the following steps:

1. The user attempts to access an application, such as Salesforce.

2. The RADIUS server overseeing the application redirects the request to SecureAuth IdP.

3. SecureAuth IdP prompts the user for userid and password.

4. The user enters the necessary credentials and presses Submit.

5. SecureAuth IdP prompts the user to provide one of several available options for the second factor.

6. The user selects RSA Token as the second factor.

7. SecureAuth IdP prompts the user to enter a token at the next screen.

8. The user looks at the RSA token on his/her keychain (or other hard token device) and reads the number, then enters that number from the RSA token in the SecureAuth IdP token text box and presses Submit.

9. SecureAuth IdP accepts the token and passes the user along to the RADIUS server with permission to access the required application.

Requirements

Deployment Prerequisites

The requirements for deployment of this module are:

+ SecureAuth IdP version 8.2 or later

+ RADIUS server – such as RSA, Vasco, Defender, or SafeNet – able to validate the token as specified for that hard token deployment

+ Connectivity between SecureAuth IdP appliance and RADIUS server

+ Download the appropriate version of RSA Hard Token package. (There is a version of this package for each supported version of SecureAuth IdP.)

Deployment

While there are several ways to deploy the RSA Migration Module, the procedure detailed on the following pages is the approach recommended by SecureAuth.

+ Best Practices

+ Installing the Module

+ Configuring the Module

+ Testing the RSA Hard Token VAM Deployment

Best Practices

When planning for deployment, keep in mind the following best practices:

+ Utilize the RADIUS Test Client to streamline the integration. We recommend that you test both the RADIUS server connectivity and token validation using the Test Client before any integration. For more on the Test Client, see "Testing the RSA Hard Token VAM Deployment" on page 10.

+ We have found specific errors arising from RADIUS server policies in Vasco RADIUS servers. Any possible problems can be alleviated by using the Test Tool and examining the server logs.

+ Make sure you download the RSA Hard Token deployment package from the SecureAuth website that matches your version of SecureAuth IdP.

Remember: there are at present multiple versions of SecureAuth IdP that this VAM can support, but each IdP version has its own 'flavor' of the RSA Migration Module. So, check your current version of SecureAuth IdP before going on-line to download the proper VAM version.

Installing the Module

To configure the SecureAuth IdP RADIUS installation for RSA Hard Token authentication, perform the following steps.

1. Download the RSA Hard Token VAM Deployment Package from the SecureAuth site to an appropriate directory on the hard drive where the SecureAuth IdP client program has been installed.

   For the specific location of this deployment package, contact your Custom Development SE
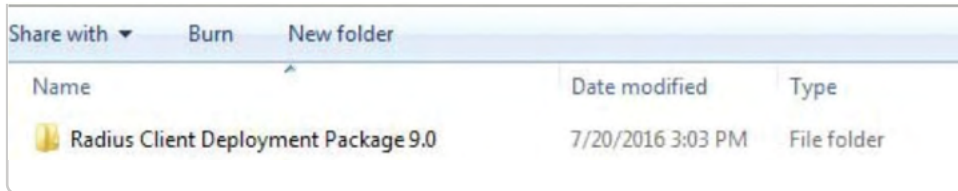
Figure 3. Deployment Package Placement

2. Using a decompression program like WinZip or 7-Zip, unpack the Radius Client Deployment Package. Three sub-folders appear:
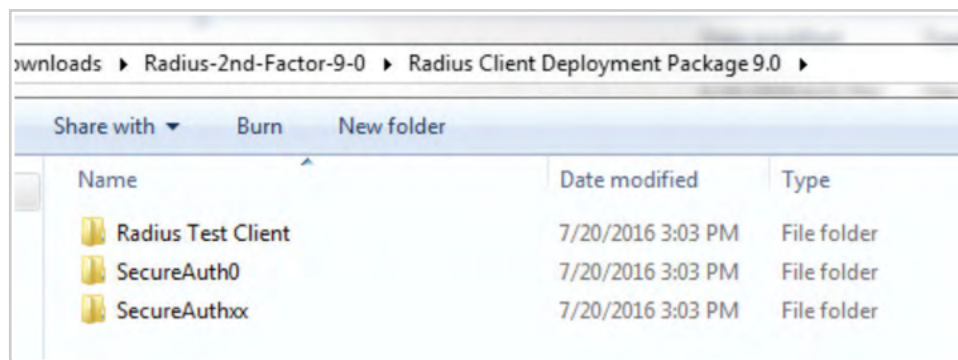

Figure 4. Deployment Package Sub-folders

3. Unpack the SecureAuth0 folder.
4. Copy these files to the corresponding folders in the SecureAuth IdP appliance's /Secure- Auth0 sub-folders.
5. Unpack the SecureAuthxx folder.
6. Copy these files to the targeted realm's bin folder, such as SecureAuth1/bin or Secure- Auth2/bin.

   Repeat this step for each SecureAuth folders that currently exists, except for the Secure- Auth0 folder.

Configuring the Module

1. Bring up the SecureAuth IdP Admin Console by entering the URL http://localhost:8088/ configuration on the local machine's browser.
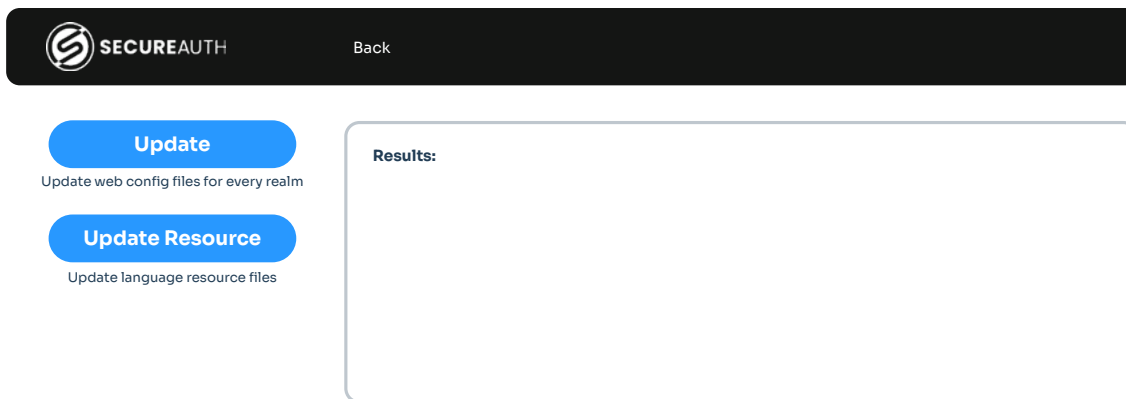
    The admin console user interface can only be viewed on the local machine access.

2. From the admin console's left panel, click the Tools option at the top of the page like Figure 5.
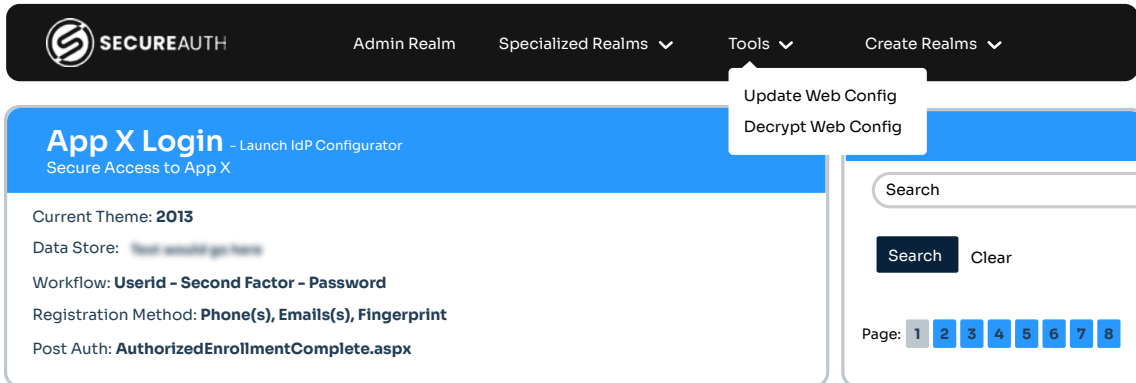
Figure 5. Tools Drop-down Menu

3. Select the Update Web Config option. A screen like Figure 6 appears.

Figure 6. Update Web Config Option Screen

4. Click both the Update and Update Resource buttons.

    The web config files are updated using the new DLLs you copied to the appropriate folders. After the update is completed, the admin UI reappears.

5. From the admin UI, click on the Admin Realm option at the top of the page.
6. From the left pane, click to select the targeted realm, such as SecureAuth1 or SecureAuth2.

7. Click to select the Registration Methods tab.

    Scroll down until you see the newly-created RADIUS Server Settings section as shown in Figure 7.

Figure 7. RADIUS Server Settings Field Selections

The default settings for the attached RADIUS server are displayed.

8. Change the values in these fields as required. These fields include:

RADIUS Server	Select whether a RADIUS server is enabled for this SecureAuth IdP appliance
Host Name	Enter the IP address or the server name of the attached RADIUS server
Authentication Port	Enter the port number this appliance will use to authenticate applications overseen by the external RADIUS server gateway
Authentication Account	Enter the account number needed to verify the RADIUS server authentication
Retries	Enter the number of timeout errors allowed to access this RADIUS server before the server is locked for a specific amount of time
Socket Timeout	Enter the number of milliseconds this RADIUS port is allowed to time out before another try is possible
Shared Secret	Enter the shared secret that enables this appliance to access the RADIUS server

9. If any of the fields are changed in Step 8, update the configuration accordingly.

    SecureAuth IdP should now be able to use a RADIUS-generated hard token as a second-factor authentication.

Testing the RSA Hard Token VAM Deployment

A third component included in the RSA Hard Token VAM deployment package is the RADIUS Test Client. This command line tool enables you to test the deployment and ascertain whether the VAM configuration is working properly prior to any integration.

To do this, perform the following procedure:

1. Place the RADIUS test tool into a directory of your choosing and extract the files. Notice that one of the files is an executable.
2. Open the command line prompt by typing cmd. The command prompt dialog box appears.
3. Use cd to navigate to the directory where you placed the executable, then enter: SecureAuth. RadiusServerTestClient [hostname] [sharedsecret] [username] [password] where:

[hostname]	Enter the name of the host where the RADIUS server resides
[sharedsecret]	Enter the shared secret that enables the RADIUS server to communicate with the client
[username]	Enter the name of the user
[password]	Enter the password associated with this user

> **NOTE:** If you enter only the executable name, a list of all parameters supported by this executable appear.

The test client runs and indicates whether the deployment was successful or not, as shown in the example in Figure 8 on page 11.
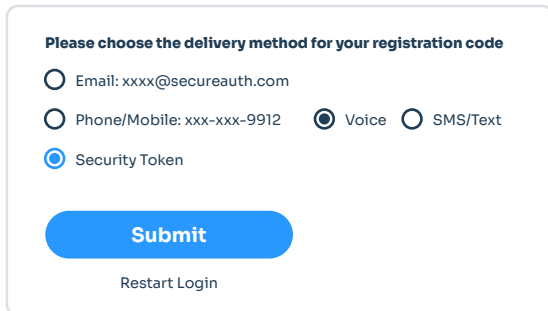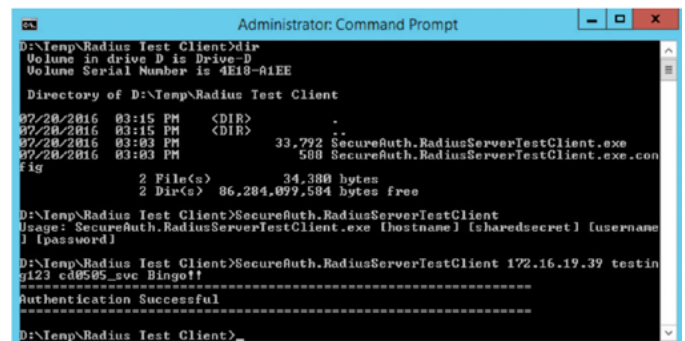

Figure 8. RADIUS Test Client Example Screen

Use Case

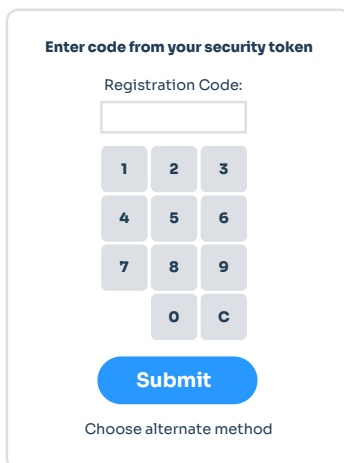This section provides a brief use case example for the RSA Hard Token after its deployment.

Once this VAM has been installed and configured, you can enter a user name and password in the normal manner, then a screen like Figure 9 appears:

Please choose the delivery method for your registration code
- ○ Email: xxxx@secureauth.com
- ○ Phone/Mobile: xxx-xxx-9912   ◉ Voice ○ SMS/Text
- ◉ Security Token

Submit

Restart Login

Figure 9. Workflow Example Screen 1

Once you click the Secure Token radio button and click the Submit button. A screen like Figure 10 appears:

Enter code from your security token

Registration Code:

1	2	3
4	5	6
7	8	9
	0	C

Submit

Choose alternate method

Figure 10. Workflow Example Screen 2

Click the buttons to specify the correct security token code then click Submit.

After the token is validated, the applications protected by SecureAuth IdP through the RADIUS server are now available to the user. In one possible example of this, a company possesses both legacy RADIUS servers and Windows servers. Prior to the introduction of this VAM, only the applications connected to the Windows servers would have been available for the advanced authentication techniques offered by the SecureAuth IdP; however, with the deployment of the RSA Hard Token VAM, the RADIUS servers and their allied applications can now use SecureAuth IdP as well as illustrated in Figure 1 on page 4.

SECUREAUTH
Welcome to Better Identity.