Value-Added Module (VAM)

SecureAuth ADFS Value-Added Module Deployment Guide
Copyright Information

©2019. SecureAuth® is a registered trademark of SecureAuth Corporation. SecureAuth’s Identity Platform software, appliances, and other products and solutions are copyrighted products of SecureAuth Corporation.

Version 3.6

May 2019

Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.5</td>
<td>2019-01-14</td>
<td>Device Recognition (digital fingerprint), MFA supported: email, phone, SMS, help desk, KBQ.</td>
</tr>
<tr>
<td>3.6</td>
<td>2019-03-13</td>
<td>MFA options upgraded: Static PIN, OATH, KBQ</td>
</tr>
</tbody>
</table>

For information on supporting this product, contact your SecureAuth 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

What’s New in Version 3.6 ........................................................................................................................................... 1  
Product Overview .......................................................................................................................................................... 1  
Benefits/Use Cases ......................................................................................................................................................... 1  
MFA/Adaptive Authentication ...................................................................................................................................... 1  
Prerequisites ........................................................................................................................................................................ 2  
  System Prerequisites ....................................................................................................................................................... 2  
  Configuring the SA Identity Platform API Realm ........................................................................................................... 2  
  Icons/Images in SecureAuth Identity Platform ................................................................................................................ 2  
  Installation ............................................................................................................................................................................ 3  
  Setting Up the Properties .................................................................................................................................................. 4  
Deployment & Configuration for the ADFS VAM ................................................................................................................ 5  
  Global-Level Configuration ........................................................................................................................................... 5  
  Per Relaying Party Trust ................................................................................................................................................ 6  
Installation of an Upgraded version of the ADFS VAM .................................................................................................... 6  
  License Considerations .................................................................................................................................................. 6  
  Installing an upgraded version of the VAM ...................................................................................................................... 6  
  Troubleshooting ............................................................................................................................................................. 6  
Release Notes ..................................................................................................................................................................... 6  
  Upgrade Information ....................................................................................................................................................... 7  
  Indemnity ........................................................................................................................................................................ 7
What’s New in Version 3.6

+ Static PIN: User is able to authenticate by entering a static personal pin.
+ OATH: User is able to select up to four registered devices — desktop and/or mobile — and validate with a one-time passcode provided by the SecureAuth Authentication App.
+ KBQ: User will be able to select and answer a certain number of knowledge-based questions in order to authenticate.

Product Overview

This guide contains information on how to install the SecureAuth Active Directory Federated Server (ADFS) VAM and how to configure it for use in an ADFS 3.0 environment. The SecureAuth ADFS VAM is a Multi-Factor Authentication Provider that uses the SecureAuth Authentication Application Programming Interface (API) to send One-Time Passwords (OTPs) for use in authentication by an ADFS application.

The SecureAuth ADFS VAM module enables ADFS customers to add strong authentication to existing ADFS integrations.

Benefits/Use Cases

Many customers have comprehensive ADFS implementations that provide the convenience of Single Sign-On (SSO) access but lack strong security, thereby putting all their applications at risk from a single breach. With this add-on module, over twenty forms of strong authentication can be enabled, as well as advanced IP threat analysis.

Many customers employ this tool when converting their SSO-available applications (using SSO standards such as SAML and WS-Federation) from ADFS to the SecureAuth Identity Platform. ADFS SAML secures their applications before they are migrated to a single SecureAuth platform, which greatly simplifies administration.

Integrating with ADFS using SecureAuth’s 2-Factor Authentication (2FA) can be challenging when pure Federation protocols such as SAML or WS-Federated are employed. The ADFS VAM was created to enable SecureAuth 2-Factor integration, and to enable a migration strategy that moves away from ADFS. In many cases, our clients have a large customer base that currently utilizes ADFS; they quickly discover, however, that ADFS does not provide the security needed in today’s hazardous threat environment. Though needing to migrate away from ADFS, clients soon learn that they have too many applications to migrate all at once. The ADFS VAM overcomes this obstacle by enabling ADFS-dependent applications and data to support SecureAuth 2FA through our API command structure. SecureAuth has created a full 2FA interface directly into ADFS. This gives customers an easy and straightforward path to moving their applications to SecureAuth federation, while still protecting applications behind ADFS.

MFA/Adaptive Authentication

The following options are available on the ADFS Value-Added module:

+ Email
+ Voice Call
+ SMS
+ PIN via Helpdesk
+ KBQ
+ OATH
+ Static PIN
+ Push To Accept
Prerequisites

System Prerequisites

The ADFS 2FA VAM and this documentation have been built using the systems outlined below:

- ADFS 2FA Adapter 3.6 running on Windows Server 2012R2 and Windows Server 2016
- ADFS 2FA Adapter 3.6 should be previously installed and operational.
- SecureAuth Identity Platform Version 9.1 or above

Configuring the SA Identity Platform API Realm

1. Go to the Identity Platform Admin realm, which should already be set up.
2. Navigate to the API tab.
3. Check the Enable API for this realm checkbox.
4. Check the Enable Authentication API checkbox.
5. Click on generate keys.
6. Copy and save for later the following two values:
   - Application ID
   - Application Key
7. Under the Registration Methods tab, if KBQ and Push-2-Accept should be functional, ensure that those options are enabled.

Icons/Images in SecureAuth Identity Platform

1. Locate the ADFS folder inside the SecureAuthAdapter installation package.
2. Copy that folder and paste it into the Identity Platform realm that will be used for ADFS.
**Note:** ADFS should have two subfolders in it: Images and Scripts. The path of those images will be used to set up properties later in the VAM configuration.

![Image Folder Content]

**Note:** By default, the Image folder contains the Branding Blue icons, but you can copy the branding Grey or Old Blue and paste/replace them in this folder.

**Installation**

1. Copy the **ADFSAdapterInstaller** into any path (C:).
2. Open a Command Prompt as an Administrator.
3. Click in Windows Start and Search “cmd.”
4. Right-click **Run as Administrator**.

![Command Prompt]

5. Set the path where the **ADFSAdapterInstaller** is located (e.g., `cd + c:\ADFSAdapterInstaller`).
6. Type/paste "\ADFS-Adapter-Installer.bat" to run the **ADFS-Adapter-Installer.bat** script.

7. Follow the steps in the Command window.

---

**Note:** Check the **installer.log** file for more information if you receive an error message.

### Setting Up the Properties

1. Open Notepad as **Administrator** (right click -> run as Administrator). If the user cannot open the .txt file as an administrator, then right click on the **file | properties | security | edit permissions**. Enable **full permissions** on the current user in order to have editing permissions (if not, changes won’t be saved in the .txt file).

2. Open the file: **C:\Windows\ADFS\SecureAuthAdapter\Props\SecureAuthProperties.txt**

3. Replace the following attributes with appropriate values (below text can be copied/modified before pasting into file):
   
   * "EnableLogs": "detailed",
   * "AppID": "[The previously generated Application ID]",
   * "AppKey": "[The previously generated Application Key]",
   * "SecureAuthRealmUrl": "https://[YourSecureAuthHostName]/SecureAuth[API_Realm]/",
   * "UseSAMAccountName": "sAMAccountName",
   * "PhoneImageUrl": "https://[YourSecureAuthHostName]/SecureAuth[API_Realm]/adfs/Images/voice.png",
   * "SMSImageUrl": "https://[YourSecureAuthHostName]/SecureAuth[API_Realm]/adfs/Images/sms.png"
Deployment & Configuration for the ADFS VAM

The ADFS VAM can be configured to apply multi-factor authentication either at a global level or to specific Relaying Party Trusts. Each of these applications is described in the following subsections.

Global-Level Configuration

By default, the package installation will configure both the Intranet and Extranet zones to use Multi-Factor Authentication (MFA). To do this:

1. Launch the ADFS Microsoft Management Console (MMC).
2. Click on the Authentication Policies container in the navigation pane to the left.
3. Click on the link under Edit Multi-Factor Authentication.
4. Define what requirements will be used to determine whether the authentication request will require MFA. You can define specific users and groups, device types, or locations. By default, the package installation will set both Extranet and Intranet to be protected by MFA.

Note: Make sure that SecureAuthAdapter is checked in the authentication providers field at the bottom of the Properties
5. Click OK to save the settings for ADFS.

**Per Relaying Party Trust**

1. Remove any Global settings for MFA requirements to set specific Per Relaying Party Trust methods.

**Note:** When removing requirements, be sure not to uncheck SecureAuthAdapter from the authentication providers field. To do this:

2. Launch the ADFS Management MMC.

3. Expand the container and click on in the navigation pane to the left.

4. **Authentication Policies Per Relaying Party Trust:** Click the specific Relaying Party Trust to which is added MFA.

5. Click on **Edit Custom Multi-Factor Authentication** in the Action pane to the right.

6. Define what requirements will be used to determine if the Authentication requests for this Relaying Party Trust will require Multi-Factor Authentication.

**Installation of an Upgraded version of the ADFS VAM**

**License Considerations**

1. If you are adding additional ADFS servers for MFA to a server farm/cluster, you will need to have the VAM installed on all servers in the farm/cluster.

2. Additionally, secondary ADFS servers will not require additional licensing cost (no matter how many servers you add to your farm/cluster). One license covers all servers added to the ADFS farm.

**Installing an upgraded version of the VAM**

1. When installing the upgraded version of the VAM, you must totally uninstall the original product, then run the installation script for the new version.

2. To uninstall, you need to run the uninstall script; or for clients that have installed the VAM with an .msi installer should uninstall the VAM from the uninstall wizard; or go to Control Panel -> Uninstall program -> Uninstall.

**Troubleshooting**

In ADFS Server 2019, Microsoft has changed the html header security policy. For example, for default, is not possible to load scripts from other domains. If the SecureAuth appliance is in other domain, it has to be added in the policy. Linked is the official documentation:


**Release Notes**

**Version 3.6 — 03/13/2019**

- Upgraded in Version 3.6:
  - **Static PIN:** User is able to authenticate by entering a static personal PIN.
+ **OATH:** User is able to select up to four registered devices — desktop and/or mobile — and validate it with a one-time passcode provided by the SecureAuth Authentication API.
+ **KBQ:** User may select and answer a certain amount of knowledge-based questions in order to authenticate.

**Version 3.5 — 01/12/2019**

+ The VAM supports device recognition (digital fingerprint) and MFA support includes email, phone, SMS, help desk, and KBQ.

## Upgrade Information

Prior to upgrading your SecureAuth Identity Platform appliances, please open a Support ticket so that SecureAuth may evaluate and ensure the Value-Added Module’s availability for that upgrade.

## Indemnity

This document is for informational purposes only. SecureAuth Corporation (SecureAuth) makes no warranties, express or implied, in this document. This document may contain flaws, omissions, or typesetting errors; no warranty is granted nor is liability assumed by SecureAuth. Information contained in this document is periodically updated and changes will be incorporated into subsequent editions. If you have encountered an error, please notify SecureAuth.

Any attempts to alter or modify the code base of this Value-Added Module will create an unsupportable version due to alterations outside of SecureAuth’s control.

SecureAuth reserves the right, without prior notice or liability, to make changes in equipment design or specifications. All specifications are subject to change without prior notice. SecureAuth assumes no responsibility for the use thereof nor for the rights of third parties, which may be affected in any way by the use thereof.

The information contained in this document, or any addendum or revision is proprietary of SecureAuth and is subject to all relevant copyright, patent, and other laws and treaties protecting intellectual property, as well as, any specific agreement protecting SecureAuth’s rights in the aforesaid information. Any use of this document or the information contained in this document for any purposes other than those for which it was disclosed is strictly forbidden.

SecureAuth is a registered trademark of the SecureAuth Corporation in the United States and/or other countries. The names of other companies and products mentioned may be the trademarks of their respective owners.