Value-Added Module (VAM)

SecureAuth ADFS VAM Deployment Guide

SECUREAUTH

Copyright information

Document revision history

Version	Date	Notes
3.5	2019-01	Device Recognition (digital fingerprint), MFA supported: email, phone, SMS, help desk, KBQ.
3.6	2019-03	MFA options upgraded: Static PIN, OATH, KBQ
4.0	2019-09	Push-to-Accept symbol, No Factors error message
4.0.2	2020-01	Optional radio buttons UI

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

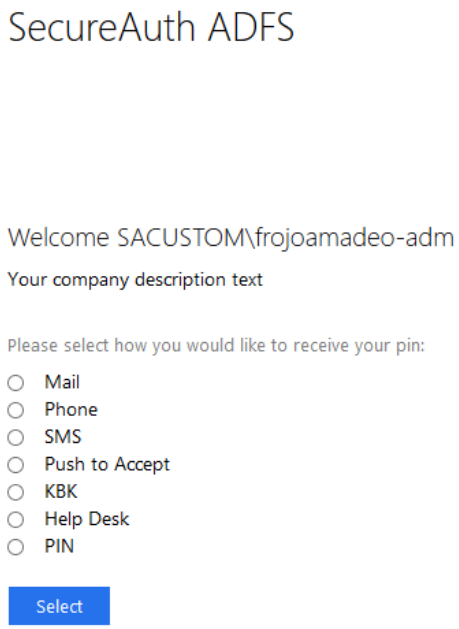
Email: support@secureauth.com
inside-sales@secureauth.com
Phone: +1-949-777-6959
+1-866- 859-1526
Website: https://www.secureauth.com/support
https://www.secureauth.com/contact

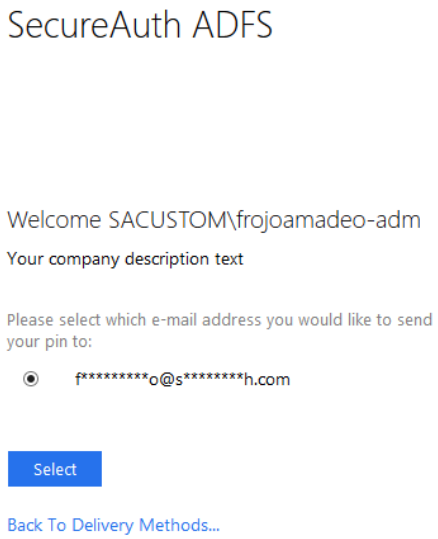
Contents

What's new in version 4.0

Version 4.0.2, released in January 2020, includes an update that enables you to use radio buttons in the user interface. To use radio buttons in the UI, set the **RadioButtonsHTML** property key to `true`, which is described in "Setting up properties" in step 4.

The following images are the new user interfaces that support the radio button change.





Introduction

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 (MFA) 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.

The SecureAuth® Identity Platform, released as version 19.07, was formerly called SecureAuth IdP.

Benefits and use cases

Many customers have comprehensive ADFS implementations that provide the convenience of single sign-on (SSO) access but lack strong security, which puts applications at risk from a single breach. With this add-on module, you can enable over twenty forms of strong authentication and 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 two-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 two-factor integration, and to enable a migration strategy that moves away from ADFS.

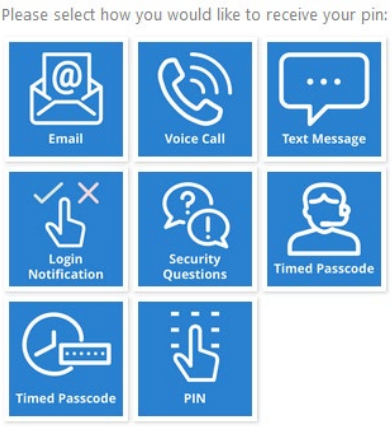
Perhaps your company has a large customer base that currently uses ADFS, and you find that ADFS does not provide the security needed in today's hazardous threat environment. Additionally, although your company might need to migrate away from ADFS, the high number of applications that need to be migrated all at once makes a change difficult.

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 administrators an easy and straightforward path to move 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/Text
- PIN via Helpdesk
- Security Questions (knowledge-based questions)
- OATH
- Static PIN
- Push-to-Accept symbol



Prerequisites

The ADFS 2FA VAM and this documentation were 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 installed and operational.
- SecureAuth IdP version 9.1 and later; SecureAuth® Identity Platform version 19.07 and later

Configuring the SecureAuth Identity Platform API realm

1. Open the SecureAuth Identity Platform **Admin** realm.

   If a realm is not yet set up, set one up before proceeding.
2. Select the **API** tab.
3. In the API Key section, select the **Enable API for this realm** checkbox.
4. In the API Permissions section, select the **Enable Authentication API** checkbox.
5. Click **Generate Keys**.
6. Copy and save for later the following two values: Application ID and Application Key
7. Under the **Multi-Factor Methods** tab, ensure that **KBQ** and **Push-to-Accept** are enabled.
8. Add the following key to web.config.

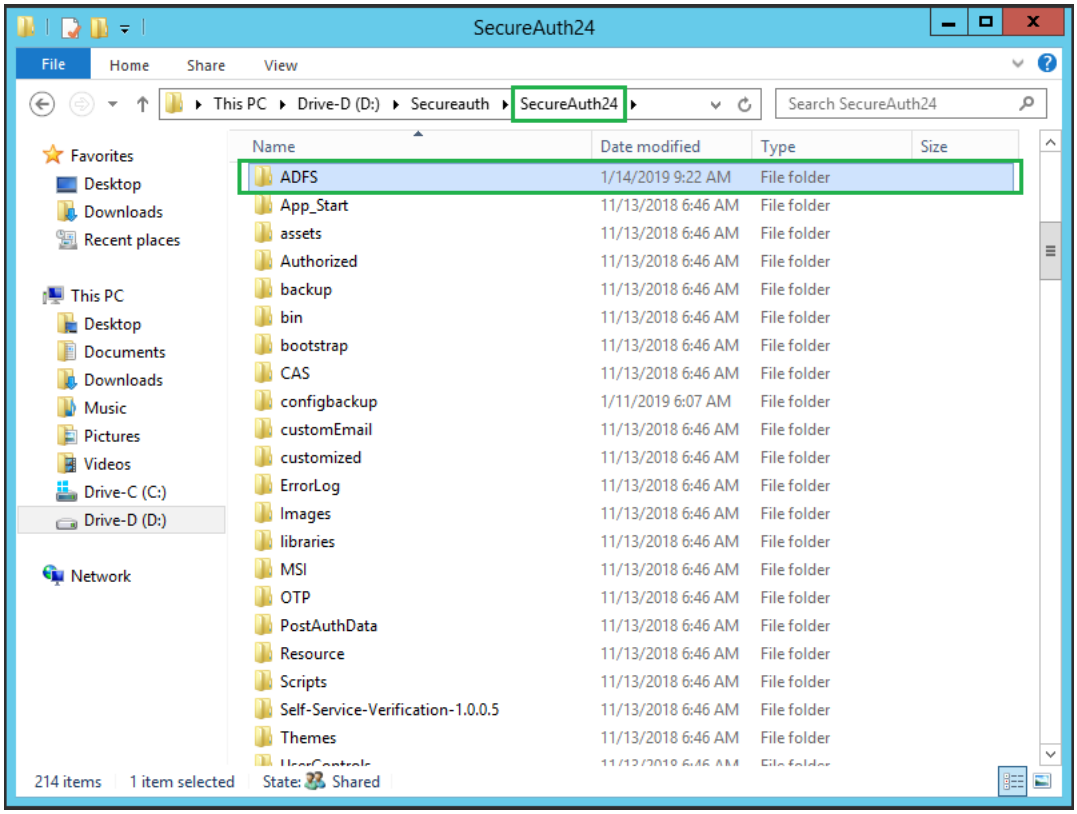
   ```
   <add key="OTPFieldMapping" value="<SecureAuth IdP Profile Property>" />
   ```

   In the **Data** tab, map a new attribute that describes where to save the OTP; for example:

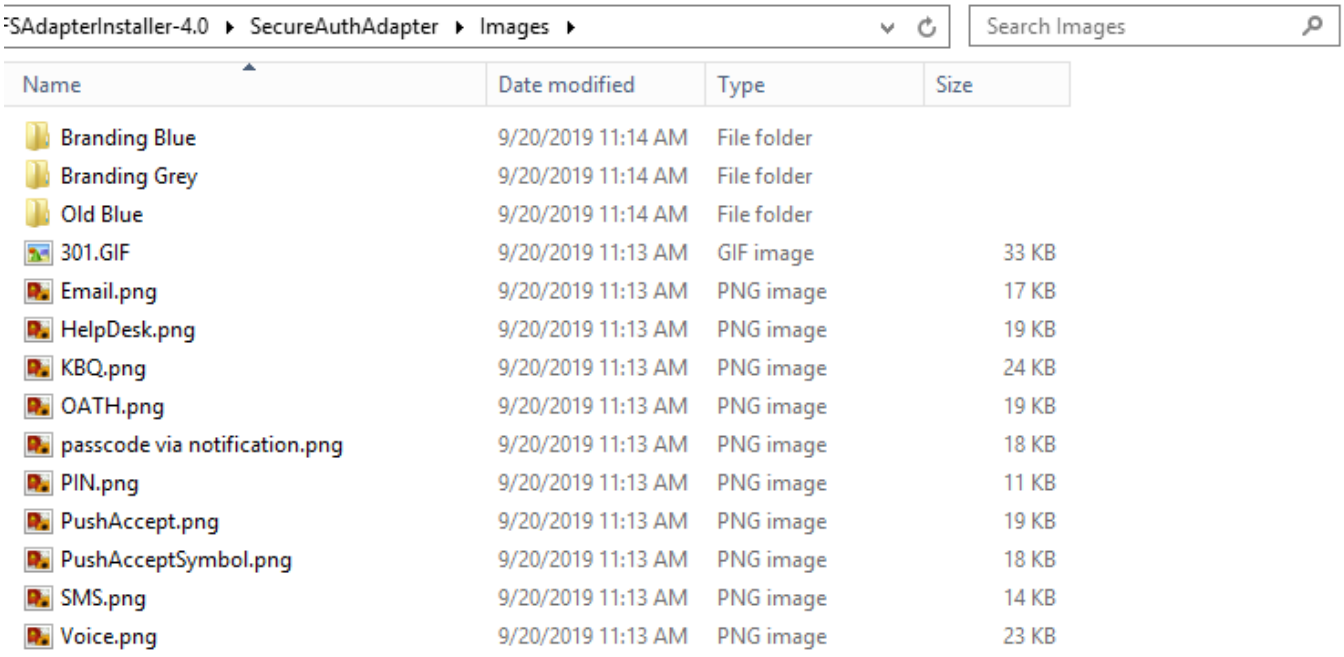
   ```
   <add key="OTPFieldMapping" value="<AuxId1>" />
   ```

Icons and images in SecureAuth Identity Platform

1. Locate the **ADFS** folder inside the **SecureAuthAdapter** installation package.
2. Copy the folder and paste it into the Identity Platform realm that will be used for ADFS.



Note: ADFS should contain two subfolders: **Images** and **Scripts**. The path of those images will be used to set up properties later in the VAM configuration.

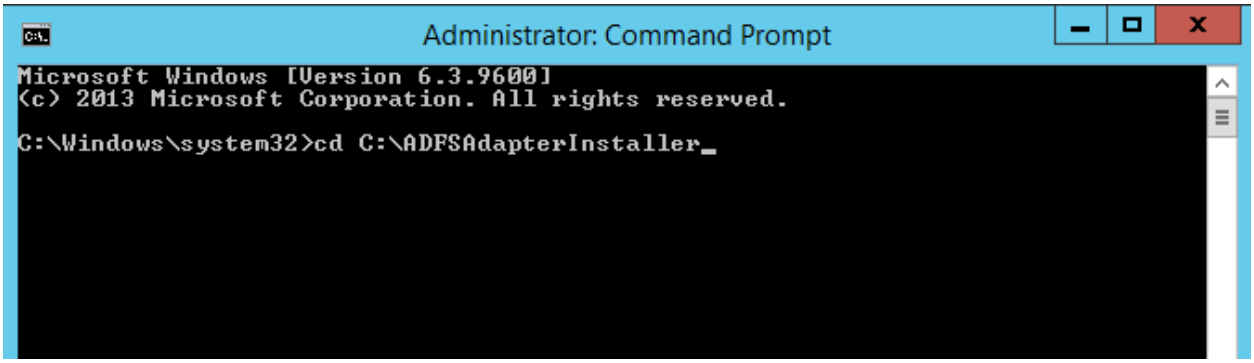


By default, the Images folder contains the SecureAuth Branding Blue icons, but you can copy the branding Grey or Old Blue and replace them in this folder.

Installation

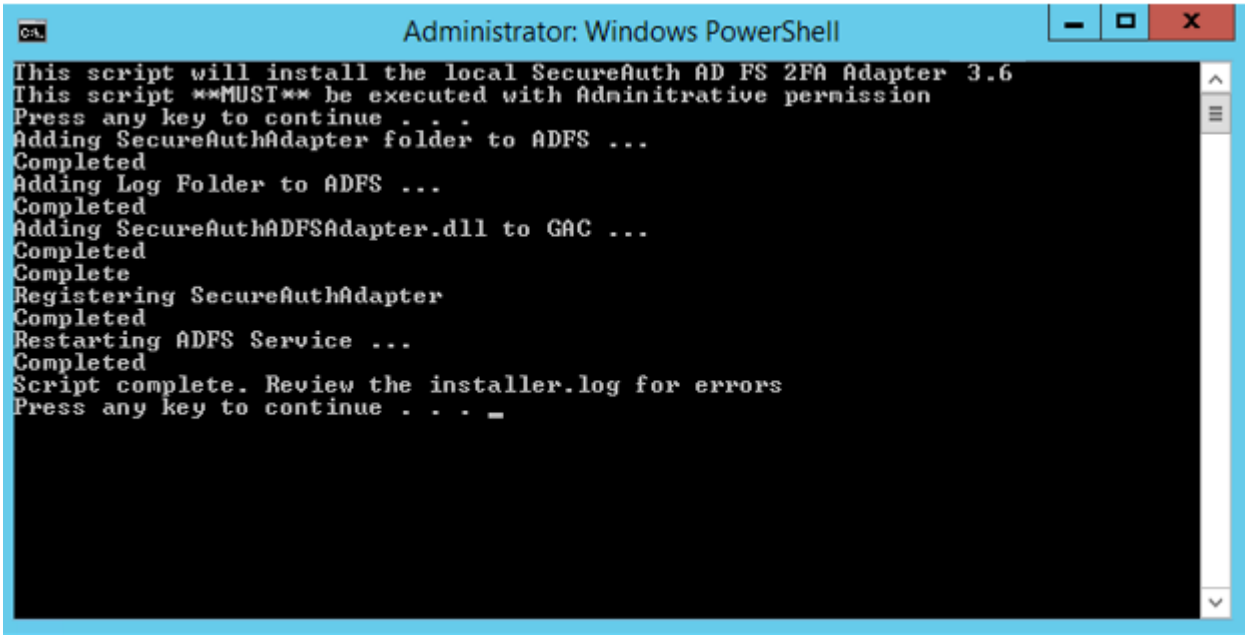
1. Copy the **ADFSAdapterInstaller** into any path (C:).
2. Open a command prompt as an Administrator.
   a. In Windows Start, search for **cmd**.
   b. Right-click **Run as Administrator**.

3. Set the path where the `ADFSAdapterInstaller` is located (e.g., cd + C:\ ADFSAdapterInstaller).



4. Type or paste `.\ADFS-Adapter-Installer.bat` to run the ADFS-Adapter-Installer.bar script.

5. Follow the steps in the Command window.



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

Permissions

Add Adfs service read and write permissions to the following folder and subdirectories or files:

C:\windows\ADFS\SecureAuthAdapter\logs

Setting up properties

1. Open Notepad as **Administrator** (right click -> run as Administrator).

   If you cannot open the .txt file as an administrator, right click the **file | properties | security | edit permissions**.

2. Enable **full control** for yourself to gain editing permissions. (You must have editing permissions or the changes will not be saved in the .txt file).

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

4. Replace the following attributes with appropriate values. (You can copy and modify the following text before pasting it into the 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",

   "EmailImageUrl": "https://[YourSecureAuthHostName]/SecureAuth[API_Realm]/adfs/Images/email.png",

   "KBQImageUrl": "https://[YourSecureAuthHostName]/SecureAuth[API_Realm]/adfs/Images/kbq.png",

"HDImageUrl": "https://[YourSecureAuthHostName]/SecureAuth[API_Realm]/adfs/Images/helpdesk.png",
"OathImageUrl": "https://[YourSecureAuthHostName]/SecureAuth[API_Realm]/adfs/Images/oath.png",
"PushAcceptImageUrl":
"https://[YourSecureAuthHostName]/SecureAuth[API_Realm]/ADFS/Images/adfs/pushaccept.png",
"ProgressGifUrl": "https://[YourSecureAuthHostName]/SecureAuth[API_Realm]/adfs/Images/301.gif",
"ScriptBaseUrl": "https://[YourSecureAuthHostName]/SecureAuth[API_Realm]/adfs",
"KBAQMaxValidCount": Minimum number of correct Knowledge-Based Answers (KBA),
"DisableSSL": "true" for development environment, "false" for production environment
"IDPVersion": "v92",
"NoFactors": "No factors error message",
"NoFactorsLink": "any link to show after no factor error message",
"OTPTimeoutInMinutes": 3
"RadioButtonsHTML": "false"

Deploy and configure the ADFS VAM

Configure the ADFS VAM to apply multi-factor authentication either at a global level or to specific Relaying Party Trusts. The following subsections describe each application.

Global-level configuration

By default, the package installation will configure both the Intranet and Extranet zones to use MFA. Complete the package installation by using the following steps:

1. Start the ADFS Microsoft Management Console (MMC).
2. Click the **Authentication Policies** container in the navigation pane on the left side.
3. Click the link under Edit Multi-Factor Authentication.
4. Define the requirements to use 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: Ensure that **SecureAuthAdapter** is checked in the authentication providers field at the bottom of the Properties window.
5. Click OK to save the settings for ADFS.

Per Relaying Party Trust

Use the following steps to remove global settings for MFA requirements to set specific Per Relaying Party Trust methods.

Note: Do not clear the SecureAuthAdapter checkbox from the authentication providers field when removing requirements

1. Start the ADFS Management MMC.
2. Expand the container and click the navigation pane on the left side.

3. Authentication Policies Per Relaying Party Trust: Click the specific Relaying Party Trust to add MFA to.
4. Click **Edit Custom Multi-Factor Authentication** in the Action pane on the right side.
5. Define the requirements to be used to determine if the authentication requests for this Relaying Party Trust will require multi-factor authentication.

Upgrade considerations for ADFS VAM

License considerations

If you are adding additional ADFS servers for MFA to a server farm or cluster, you will need to have the VAM installed on all servers in the farm or cluster. One license covers all servers added to the ADFS farm; secondary ADFS servers do not require additional licensing cost, no matter how many servers you add to your farm or cluster.

Upgrade information

Before upgrading SecureAuth Identity Platform appliances, open a Support ticket. When your site is ready to upgrade, get started by creating a support ticket and selecting **I have a question or issue regarding SecureAuth Value-Added Modules (VAMs)** from the "Submit a request" dropdown. A SecureAuth Tailoring engineer will contact you and evaluate and ensure that the VAM can be upgraded.

When installing the upgraded version of the VAM, first completely uninstall the original product, then run the installation script for the new version.

To uninstall, you need to run the uninstall script. If you installed the VAM with an .msi installer, uninstall the VAM by using the uninstall wizard, available from the **Control Panel** > **Uninstall or change a program** > **Uninstall**

Troubleshooting

In ADFS Server 2019, Microsoft changed the HTML header security policy. For example, by default, you cannot load scripts from other domains. If the SecureAuth appliance resides on another domain, it must be added in the policy. The following documentation is available on the Microsoft website:

https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/customize-http-security-headers-ad-fs

The following is the recommended configuration:

Set-AdfsResponseHeaders -SetHeaderName "Content-Security-Policy" -SetHeaderValue "default-src `https://domain1.com https://domain2.com 'unsafe-inline' 'unsafe-eval'; img-src https://domain1.com https://domain2.com data:;"`

Set-AdfsResponseHeaders -SetHeaderName "X-Frame-Options" -SetHeaderValue "deny"

Set-AdfsResponseHeaders -EnableResponseHeaders $true

Release notes

The following release versions catalog the changes to the SecureAuth ADFS VAM.

Version 4.0.2 — 2020-01

Version 4.0.2 includes an update that enables administrators to use radio buttons in the UI by changing the **RadioButtonsHTML** property key to `false` or `true`.

Version 4.0 — 2019-09

Version 4.0 includes the following updates:

- **P2A symbol**: End users can authenticate by accepting a pushed symbol.
- **No factors message**: Administrators can specify a message and redirect link in the properties.txt file that is displayed on the login page when end users do not have multi-factors enabled.
- **Unistaller.bat**: This file generates a backup on the C:\SecureAuthBackup drive.

Version 3.6 — 2019-03

Version 3.6 includes the following updates:

- **Static PIN**: End users can authenticate by entering a static personal PIN.
- **OATH**: End users can select up to four desktop and mobile registered devices and validate them with a one-time passcode provided by the SecureAuth Authentication API.
- **KBQ**: End users can set up and answer knowledge-based questions to authenticate.

Version 3.5 — 2019-01

The VAM supports digital fingerprint device recognition. MFA support includes email, phone, SMS/text, help desk, and KBQ.