Two Factor Authentication Package

Readme

Version 1.0

04/24/2020

Table of Contents

1. Introduction

This document contains all essential information for the user to make full use of this A2019 Package. It includes a description of the functions and capabilities and step-by-step procedures for setup & configuration of the Package.

1.1 Overview

The Two Factor Authentication package can be used for generating, validating, and distributing access codes to be used for secure bot executions.

1.2 Use cases

The Two-Factor Authentication package is especially useful in the case of attended automation where task processing must be as absolutely secure as possible. Limited individuals could have their mobile devices set up with an Authenticator mobile app (Google Authenticator and Microsoft Authenticator was used for testing this bot) where only they would have the capability to run bots based on their generated codes.

2. Requirements & Prerequisites

2.1 System Requirements

Enterprise A2019 (Cloud deployed) and Community Edition device requirements.
Review the machine hardware specifications, operating system versions, and browser types supported by Automation Anywhere Enterprise for creating and running bots and command packages as an Enterprise A2019 (Cloud deployed) or Community Edition user on your local machine.

2.2 Prerequisites

Google Authenticator App for Android or iOS

While not absolutely required for use, its good to grab this free app for testing the different scenario flows.

3. Getting Started

3.1 Quick Start

3.1.1 Setup

1. Install the package from Bot Store into your Control Room
2. Enable the package named **Two-Factor Authentication** and set as default.
3. Navigate to **Bot Store/Two-Factor Authentication - Automation Anywhere** to examine the 3 installed bots and 1 form. These bots are not required for use, but included to demonstrate how the package can be used.

3.1.2 Configuration and Use

The package includes 4 total actions:

Get Code: which allows for generating a one-time use access code and could be used for situations where an access code needs to be sent to a mobile device/email for validation within the bot.

Get QR Code Image: Used to generate a QR code which can be utilized with the Google or Microsoft Authenticator app (among other 2FA mobile authenticators) to generate valid codes every 30 seconds.

Initialize: The first step in generating a new Secret Key/QR Code image. This action generates a secret key value which is used to build the QR code, and is also used during the Validate and Get Code actions to be sure codes are validated against the correct 2FA model.

Validate: The validate action can be used to validate codes in real time. Supply the secret key and the generated code (likely from mobile for this use case) and determine if the code is valid or not.

To begin using the Two-Factor Authentication bot

1. Run the bot entitled: **1 - Create Secret Key and QR Code.** The use case for this bot is for the initial generation of the 2FA profile. The actions in this bot wouldn't need to run regularly once a profile was established.
   a. You will be prompted for an email address and a company name. No email is actually generated in this bot – the email and company name are only used in the generation of the Secret Key which is needed to build the QR Code and establish a 2FA profile.
2. Upon completion of the bot run – an image will open which is your QR Code. This file is saved to c:\temp along with at txt file which contains your secretKey. Do NOT lose this secret key should you plan to continue using this 2FA profile.
   a. Download and install the Google or Microsoft Authenticator app on your mobile device. Within this app, you should be prompted to scan a QR code. Scan the

QR code that the bot created to add this 2FA profile to your Google or Microsoft Authenticator app.

  b. Notice that the Authenticator App generates a 6 digit key every 30 seconds. This key is unique to the profile which was generated, and is not just random.

3. With the Authenticator App still open, execute the **2A – Validate Code from Authenticator** bot. The use case for this bot is a secure bot execution that requires a user with the 2FA profile on their authenticator app to provide an access code to be validated in real time.
    - **a.** As an input value, this bot will prompt you for the Secret Key (which was generated from running the 1 – Create Secret Key and QR Code bot and was saved in the C:\temp directory as Two-FactorAuthSecretKey.txt)
        - **i.** Note: In a real use case you would store this secret key in your credential vault and always reference it from there, but this sample bot is just for demonstration purposes.
    - **b.** This bot will prompt you for the 6 digit code from your authenticator app.
    - **c.** Provide the 6 digit code from your app and submit.
    - **d.** The bot should show a message indicating that the access code was valid.
    - **e.** Run the bot again and enter a random 6 digits to demonstrate that no
4. The final bot is the **2B - Generate Code to Send for Validation** bot. The use case for this bot is that an access code is generated from the bot itself and sent via email or SMS to a user who will be executing the bot.
    - **a.** The bot will prompt for the Secret Key as well as an email address.
    - **b.** In this example, the bot will attempt to email a generated access code to a user.
    - **c.** Once the access code is sent, the bot will display a form asking the user to provide the access code sent to their email.
    - **d.** If the code entered matches the generated code, bot processing can continue.
    - **e.** If the code does not match, bot processing terminates immediately.

4. Support & FAQs

4.1 Support

Free bots are not officially supported. You can get access to Community Support through the following channels:

- You can get access to Community Support, connecting with other Automation Anywhere customers and developers on APeople – the Bot Building Forum, the Bot Store Support Forum, or the Developers Everywhere Group.
- Automation Anywhere also provides a Product Documentation portal which can be accessed for more information about our products and guidance on Enterprise A2019.

4.2 FAQs

For questions relating to Enterprise A2019: See the Enterprise A2019 FAQs.

Appendix A: Record of Changes

No.	Version Number	Date of Change	Author	Notes

Appendix B: References

No.	Topic	Reference Link
1	Overview of Enterprise A2019	Click here
2	Guidance: Building basic A2019 bots	Click here
3	Guidance: Building A2019 action packages	Click here
4	APeople Community Forum	Click here
5	Automation Anywhere University	Click here