Virtru Data Protection Platform Bot

Readme

Version 1.0

20/02/2020

Table of Contents

1. Introduction

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

1.1 Overview

Secure custom workflows to ensure that when sensitive data is extracted and shared within and outside the organization, the appropriate levels of encryption and policy controls were applied. For example, a bot handles the movement of files containing sensitive data from a local storage location (e.g. File server, NAS, desktop, etc.) to Google Drive. Another bot encrypts the data using Virtru, adapts the policy using our access control management capabilities, then downloads and decrypts it where it resides securely in a folder located on-premise or moved to another cloud storage platform.

Benefits:

- Utilize RPA technology while maintaining compliance with laws such as HIPAA, GDPR, CCPA, CJIS, etc.
- Take advantage of the convenience, scale and cost savings of cloud storage with the peace of mind that your data will remain encrypted and invisible to even your cloud provider.
- Eliminate human error when dealing with sensitive data movement across systems
- Streamline the process of collating recording containing sensitive data from disparate systems.
- Enable bots to operate on data that was off-limits previously

1.2 Common Use cases

These are just a subset of the common use cases:

- Report generation workflows that incorporate sensitive data that must be encrypted.
- Moving files from one location to another where it is cloud-based and must remain encrypted.
- Extracting documents from disparate systems while maintaining privacy of the data

2. Requirements & Prerequisites

2.1 System Requirements

For the PC or server where the bot needs to run:

- Ram: 8GB or higher
- Processor: Intel Core i5 or higher and equivalent for any other OS
- Hard Disk: Up to 2GB of overall free space in the AA Client installation drive.

2.2 Prerequisites

Software

- Automation Anywhere Enterprise Agent 11.x
- Automation Anywhere Enterprise Client 11.x
- Automation Anywhere Enterprise Control Room 11.x

Accounts/Licenses

- Automation Anywhere Enterprise License
- Virtru Authentication Token

2.3 Security Measures

There are some security best practice recommendations that you may follow with your bot.

- Use the Credential Locker where possible to store the Virtru Authentication Token

2.4 Disclaimers

Acceptable Use Policy

3. Getting Started

3.1 Skill Matrix

Below is an overview of how the metabots map to these skills:

Skill	Metabots Files
Manage and control the Virtru Encryption policies	Virtru.Automation.AutomationAnywhere.mbot

3.2 Installation Hierarchy

Installation is as simple as adding the Metabot from the Automation Anywhere store

Folder Structure	Description
<Automation Anywhere Application Path>	**< Automation Anywhere Application Path>** is the location where Automation Anywhere files are stored on your machine.
• **Error Folder**	• **Error Folder** is where logs and snapshots of screens will be placed during execution errors.
○ **Logs**	○ **Logs** contains logs in the format: Month-Day-Year Hour Min Sec.txt
○ **Snapshots**	○ **Snapshots** contain screen shots during execution errors
• **Input Folder**	• **Input Folder** is where the input files that the bot needs for execution of the use case is saved
• **My MetaBots**	• **My MetaBots** contains the Developed MetaBots needed for the bot execution

3.3 Quick Start

3.3.1 Setup

Virtru Authentication Tokens – To perform any Virtru operation a user must be authenticated. Virtru supports either:

- AppId – Details
- HMAC – Details

3.3.2 Configuration

INPUT VARIABLES:

Variable Name	Type	Mandatory	Purpose	Example Input
PolicyOwner	Text	Yes	Owner of the Protected Data Policy	user@domain.com
AppId	Text	Yes	Authentication Token: Must match the PolicyOwner	8ae8423c-06b9-46ea-b749-968329b1a23c
HmacId	Text	Yes	Authentication Token: Hmac Id	8ae8423c-06b9-46ea-b749-968329b1a23c@tokens.virtru.com
HmacSecret	Text	Yes	Authentication Token: Hmac Secret	Q2Aww…upl8eeqk=
EncryptedFilePath	Text	Yes	Path to Encrypted File	c:\files\encrypted\encrypted.txt.tdf
PolicyId	Text	Yes	Unique Policy Id of the Virtru Encryption Policy.	49d2aa06-fb78-402a-afbe-8a6d1999d98d
SourceFile	Text	Yes	Path to Source File for specific call	c:\files\file.docx
TargetFile	Text	Yes	Path to Target File for specific call	c:\files\file.docx.tdf

OUTPUT VARIABLES

Variable Name	Type	Mandatory	Purpose	Example Output
PolicyId	Text	Yes	Unique Policy Id of the Virtru Encryption Policy.	49d2aa06-fb78-402a-afbe-8a6d1999d98d
Users	Text/XML	Yes	XML of users on a policy.	<items> <item>user@example.com</item> <item>user@demo.com</item> </items>
Policy	Text/XML	Yes	XML of policy flag	<items> <item>revoke</item> <item>False</item> <item> </item> </items> <items> <item>expire</item> <item>true</item> <item> 2020-02-25T20:43:25</item>

				</items>

4. Reports

There are no Bot Insight Reports generated for this Bot.

5. Logs

5.1 Location

In case of Errors, Error Logs are generated within Error Folder

- Error Folder
    - Logs (Folder)
        - Virtru_Error_Log_yyyy-mm-dd-sec.txt

5.2 Contents

Error Logs will contain:

- Task Name
- Error Line Number
- Error Description
- Generated Timestamp

6. Troubleshooting & Support

6.1 Support

For any issues or questions:

- Submit a support ticket
- Join the Slack Community

6.2 FAQs

- Where do I get my AppId
  - Follow these steps
- Where do I get my Hmac
  - Follow these steps
- How can I get support
  - Submit a ticket
  - Join the Slack Community
- Pricing
  - Details
- What are the Use Cases?
  - Virtru Developer Hub
  - Virtru Technology Blog
- What is an Active Policy?
  - Details

Appendix A: Record of Changes

No.	Version Number	Date of Change	Author	Notes
1	1.0.0	2/28/2020	csigler@virtru.com	Initial Commit

Appendix B: Acronyms

No.	Acronym	Description
1	TDF	TDF is an open data format that provides a protective wrapper that travels with data. https://developer.virtru.com/docs/architecture#section-the-trusted-data-format
2	KAS	The KAS acts as a Policy Decision Point (PDP) https://developer.virtru.com/docs/architecture#section-key-access-server-kas-and-management-infrastructure
3	EAS	EAS provides Identity Management services and returns the attributes associated with an authenticated user. https://developer.virtru.com/docs/architecture#section-entity-attribute-server-eas
4	AA	Automation Anywhere
5	API	Application Programming Interface
6	RAM	Random Access Memory
7	OS	Operating System
8	HMAC	Virtru Authentication Token
9	AppId	Virtru Authentication Token

Appendix C: References

No.	Topic	Reference Link
1	How to Create a Credential in Credential Vault?	Click here
2	Identity Federation	Click here
3	Policy Dashboard	Click here
4	Payload Encryption	Click here
5	Policy Audit	Click here

Appendix D: Open Source Attribution

No.	Library	Link	License
1	Bouncy Castle	Link	MIT
2	Command Line Parser	Link	MIT
3	Flurl	Link	MIT
4	HTML Agility Pack	Link	CC-BY-SA with attribution
5	Log4net	Link	Apache V2.0
6	Microsoft Recyclable Memory Stream	Link	MIT
7	MimeKit	Link	MIT
8	Murmur Hash	Link	Apache V2.0
9	Newtonsoft Json	Link	MIT
10	Polly	Link	New BSD
11	Protobuf.net	Link	Open