



CYBERARK SECRETS MANAGER

(Agentless Central Credential Provider CCP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Datamatics Robotics Software Limited

Website: www.datamatics.com

Name of Product: TruBot Robotics Process Automation

Version: 4.3

Date: 23 March 2020 (Revised 29 October 2020)

TRUBOT ROBOTICS PROCESS AUTOMATION OVERVIEW

TruBot is a Robotic Process Automation (RPA) Product based on Windows platform. The current version of TruBot to get certified is Release 4.3. TruBot is available for legacy platforms as well as new age technical platforms and can automate most of the routine tasks performed by human. This eliminates the need for human interaction. It has Visual designer with workflow, drag-and-drop options to easily design the process in TruBot Designer. TruBot provides seamless recording between web, desktop, and SAP. A rich component library of 250+ ready-to-use components, making designing low code and enabling rapid deployment. It has a powerful centrally deployed cockpit for operational monitoring and control of all Bots. The TruBot Analytics module provides ready analytics for the RPA program.

KEY BENEFITS

The key benefits of TruBot are as follows:

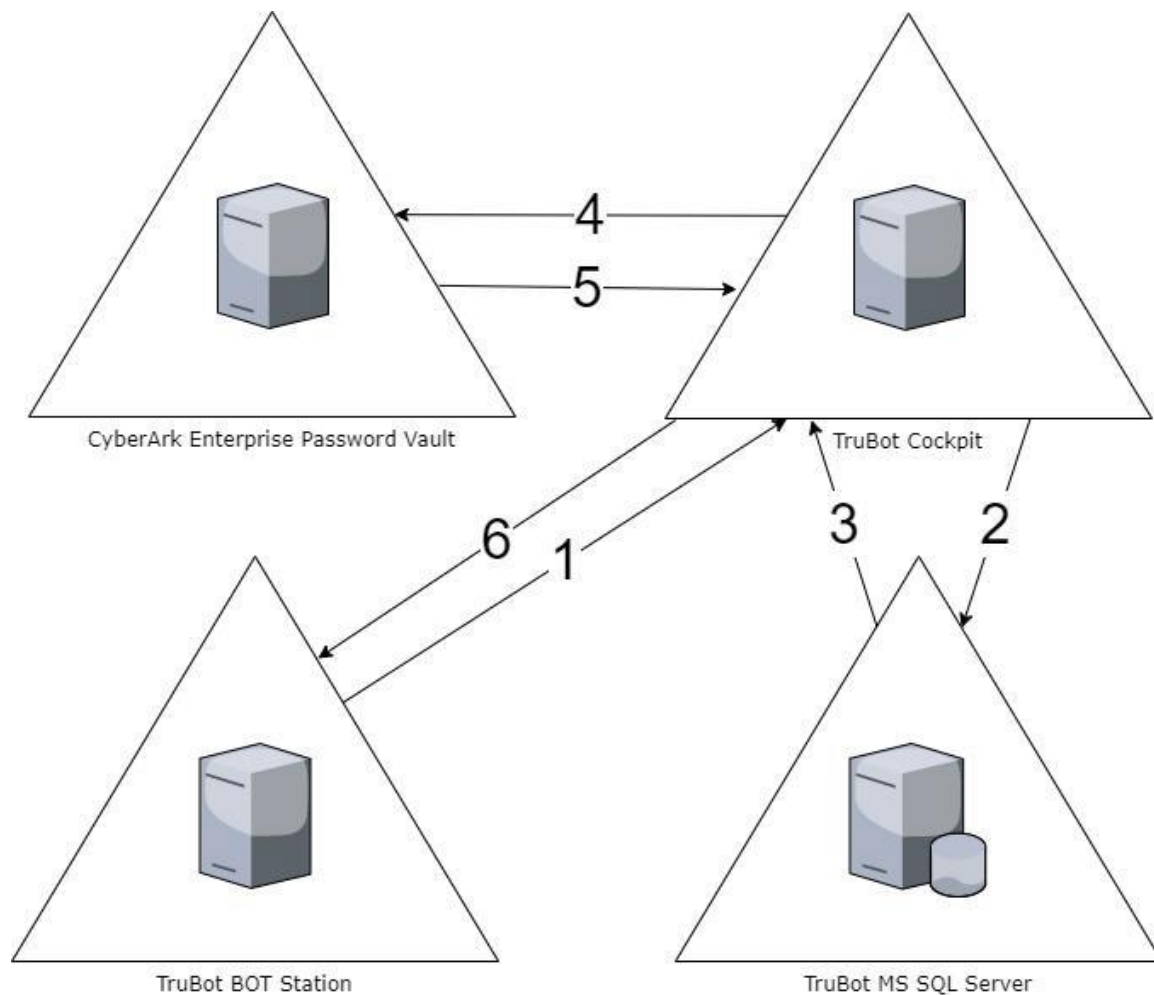
1. Automate routine tasks on systems like SAP, Mainframes, Windows Desktop Application, Web browser-based applications, and more.
2. These BOTs can be attended or unattended.
3. There is a cockpit which can automate and schedule the BOT tasks.

The key benefits of integrating TruBot with CyberArk Secrets Manager are as follows:

1. The CyberArk Secrets Manager will store sensitive information like passwords in its vault.
2. TruBot Cockpit will fetch the passwords from cloud instance of CyberArk, before sharing the same with BOTs.
3. No passwords will be stored in the TruBot RPA RDBMS, enhancing the security of the credentials.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

TruBot RPA has three logical entities – Cockpit, BOTs, and RDBMS. BOTs will not directly communicate with CyberArk vault, but they will receive credentials from the Vault via Cockpit. Only TruBot cockpit will access the passwords from the Vault and share them with BOTs running on remote machines. The connection between Cockpit and BOTs are HTTPS based. Therefore, the only integration between TruBot and CyberArk is between Cockpit and the CyberArk vault.



SECRETS MANAGER INTEGRATION

The above diagram is depicted in the steps below:

1. The BOT detects that the BOT requires the sensitive information like password. It sends the request to Cockpit.
2. The Cockpit checks in the RDBMS, where the password is stored
3. The RDBMS responds that the password is stored in the Vault.
4. The Cockpit asks for the password from the Vault.
5. The Vault returns the HTTPS JSON response with the password.
6. The Cockpit shares the password to BOT.

Describe Partner Product and depict where Secrets Manager integration lies. Description might include:

- Where Secrets Manager is integrated in Partner Product
- Location of integration: End Point or Mid-Tier or Central Server
- Number of mid-tier servers and number of endpoints in a typical installation

CREDENTIAL RETRIEVAL

Describe how the credential retrieval plays a role within the Partner product. Describe the flow in detail.

- Describe how the credential retrieval is triggered
- Describe the circumstances / frequency under which the credential retrieval is done
- Describe specific properties required for queries on various platforms
 - Unix
 - Windows
 - Other platforms

SECRETS MANAGER INSTALLATION

Refer to the “Credential Provider Implementation Guide” for CyberArk Agentless installation and configuration.

SECRETS MANAGER CONFIGURATION

The following sections provide details on TruBot Robotics Process Automation configuration with CyberArk Secrets Manager.

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

To define the application, define it manually through the CyberArk Password Vault Web Access (PVWA) interface:

- ☐ Log in as user allowed to manage applications (it requires Manage Users authorization)
- ☐ In the Applications tab, click **Add Application**. The Add Application page appears.

Edit Application

Name: Datamatics-TruBOT

Description: This is for storing sensitive credentials for TruBOT Robotic Process Automation.

Business owner

First Name: Tejas

Last Name: B

Email:

Phone:

Location: \

☐ Access Permitted: From: To:

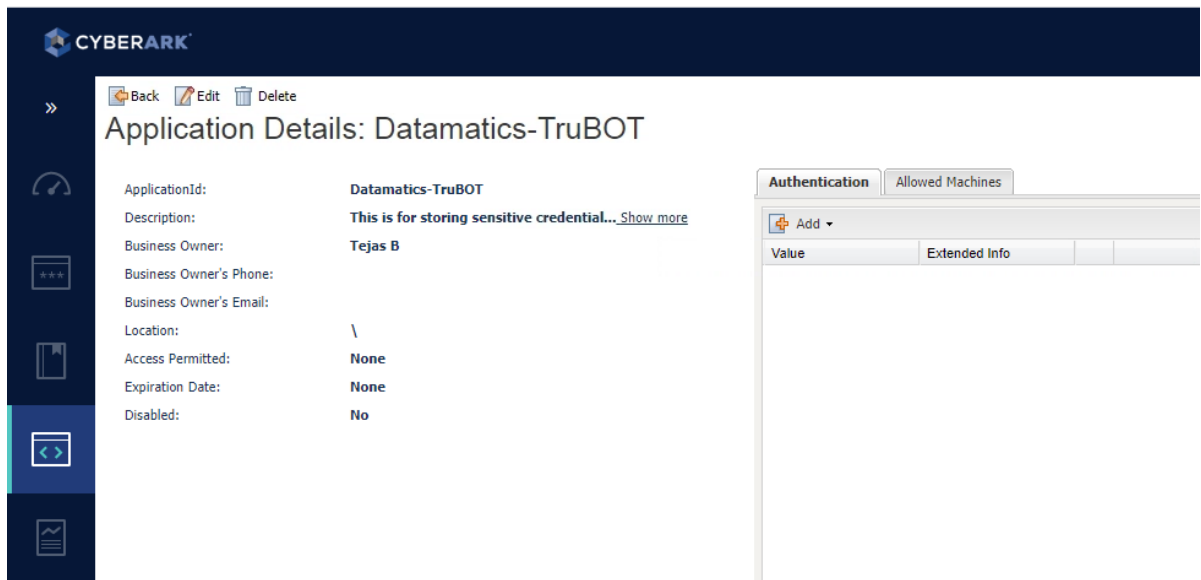
☐ Expiration Date:

☐ Disabled

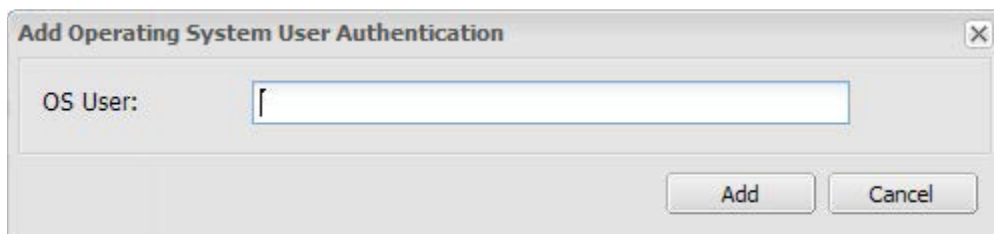
Update Cancel

- ☐ Specify the following information:
 - In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: Datamatics-TruBot
 - In the **Description** box, specify a short description of the application that will help you identify it.
 - In the **Business owner** section, specify contact information about the application's business owner.
 - In the **Location** box, specify the location of the application in the Vault hierarchy. If a location is not selected, the application will be added in the same location as the user who is creating this application.

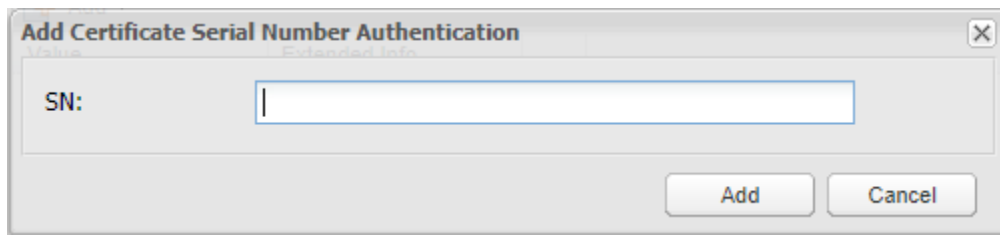
- ☐ Click **Add**. The application is added and is displayed in the Application Details page.



- ☐ Check the **Allowing extended authentication restrictions** box. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.
- ☐ Specify the application's **Authentication** details to be set to Client Certificate. This information enables the Credential Provider to check certain application characteristics before retrieving the application password.
- ☐ In the Authentication tab, click **Add**. A drop-down list of authentication characteristics is displayed.
- ☐ Select the authentication characteristic to specify.
- ☐ Select **OS user**. The Add Operating System User Authentication window appears.

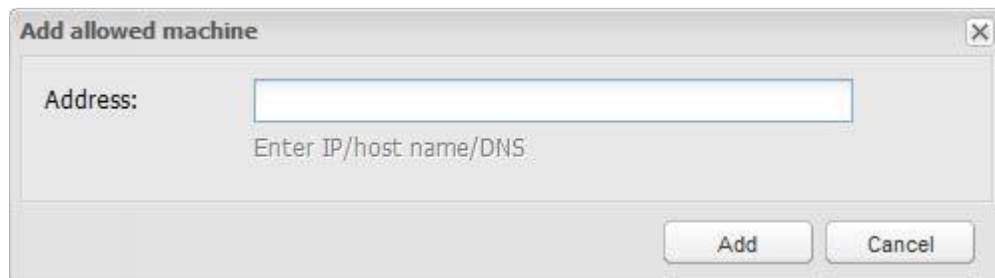


- ☐ Specify the name of the OS user who will run the application, then click **Add**. The OS user is listed in the Authentication tab.
- ☐ Specify the Certificate Serial Number.



- ☐ Specify the application's Allowed Machines. This information enables Secrets Manager to make sure that only applications that run from specified machines can access their passwords.

- In the Allowed Machines tab, click **Add**. The Add allowed machine window is displayed.

A screenshot of a dialog box titled "Add allowed machine" with a close button (X) in the top right corner. Inside the dialog, there is a label "Address:" followed by a text input field. Below the input field, there is a hint text "Enter IP/host name/DNS". At the bottom right of the dialog, there are two buttons: "Add" and "Cancel".

- In the **Address** box, specify the IP/hostname/DNS of the machine where the application will run and will request passwords, then click **Add**. The IP address is listed in the Allowed Machines tab.

PROVISIONING ACCOUNTS AND SETTING PERMISSIONS FOR APPLICATION ACCESS

For the application to perform its functionality or tasks, the application must have access to particular existing accounts, or new accounts to be provisioned in CyberArk Vault.

In the Password Safe, provision the privileged accounts that will be required by the application. You can do this in either of the following ways:

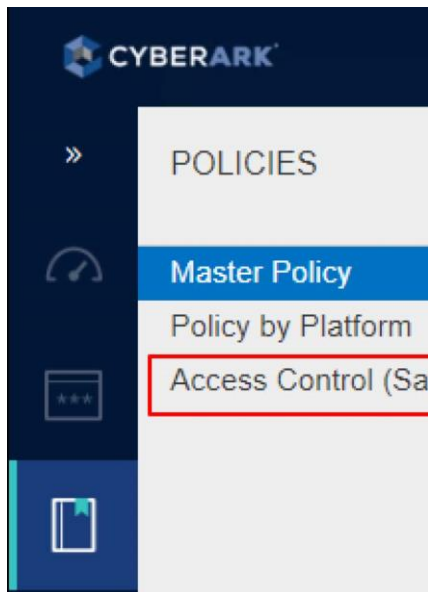
- **Manually** – Add accounts manually one at a time, and specify all the account details.
- **Automatically** – Add multiple accounts automatically using the Password Upload feature.

For this step, you require the **Add accounts** authorization in the Password Safe.

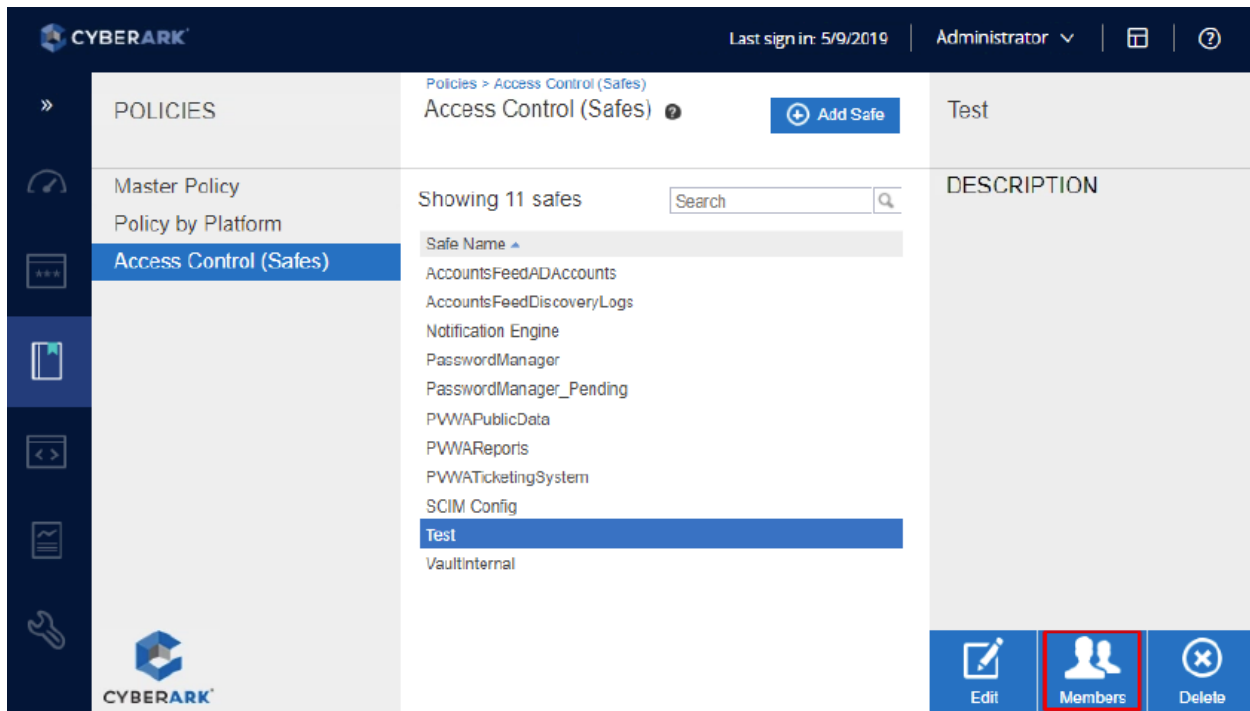
For more information about adding and managing privileged accounts, refer to **the Privileged Access Security Implementation Guide**.

The Safes are created as required, please see the screenshots below:

The following screenshots show how the Safes are created and then mapped to the Application.

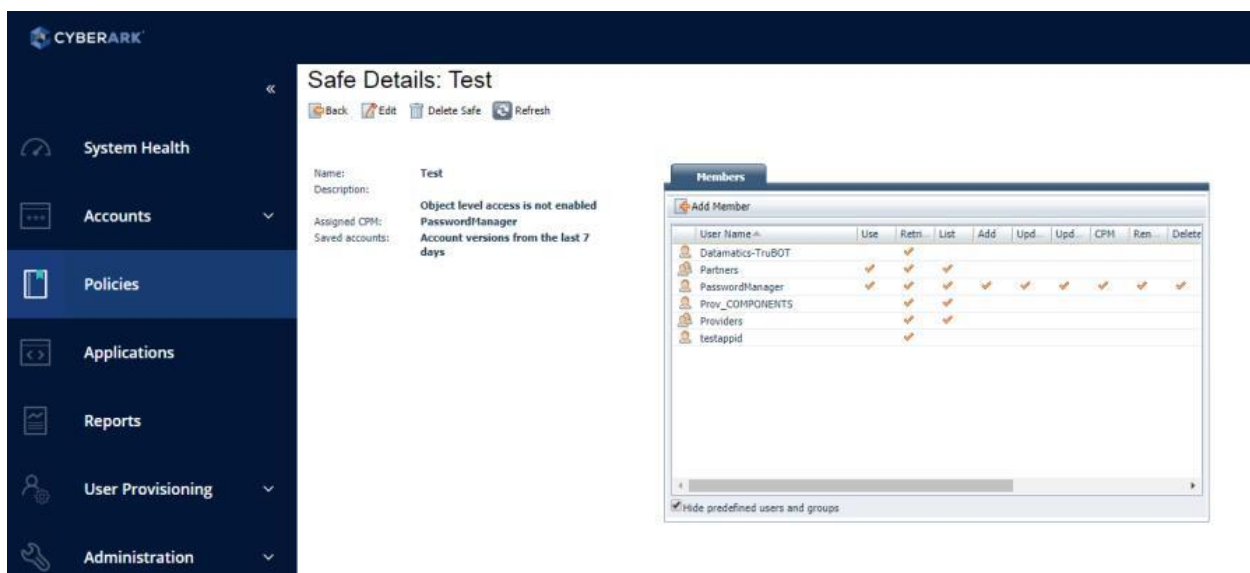


Select the safe as “Test” as per the screen below.



Add the ApplicationID “Datamatics-TruBOT” to the “Test” safe.

Ensure the Provider user for the CCP is added as an owner as well with the permissions outlined Below.



The following screen shows how to add the password to the safe.

CYBERARK

Add Account

- ✓ Select system type
Windows
- ✓ Assign to platform
Windows Desktop Local Accounts
- ✓ Store in Safe
Test
- 4. Define account properties**

Primary properties

Address
trubot1-uk

Username
trubot1-uk-alpha

Password (optional)

Confirm Password

☐ Customize account name ⓘ

CYBERARK

Accounts View

Search for accounts

16 results for: All accounts

Views | Recent | Saved

Status	Username	Address	Platform ID	Safe ↑
☆	Client-user	10.0.1.10	CyberArk	SCIM Config
☆	-	-	-	SCIM Config
☆	-	-	-	SCIM Config
☆	SCIM-user	10.0.1.10	CyberArk	SCIM Config
☆	x_accountA	components	WinDesktopLocal	Test
☆	x_accountB	components	WinDesktopLocal	Test
☆	trubot2	trubot-delhi	GenericWebApp	Test
☆	trubot2	trubot-delhi	GenericWebApp	Test

Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application.

Add the provider user (where the Central Credential Provider is installed) and application users as members of the Password Safes where the application passwords are stored. This can either be done manually in the Safes tab, or by specifying the Safe names in the CSV file for adding multiple applications.

☐ Add the Provider user as a Safe Member with the following authorizations:

- List accounts
- Retrieve accounts

- Note:** When installing multiple Providers for this integration, it is recommended to create a group for them, and add the group to the Safe once with the above authorization.

Add Safe Member

Search:

Search In:

Vault

Search

Selected Search: Vault

Name	Business Email	Full Name
------	----------------	-----------

☐ Access

☐ Use accounts

☒ Retrieve accounts

☒ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

☐ View Audit log

☒ View Safe Members

Add

Close

- ☐ Add the application (the APPID) as a Safe Member with the following authorizations:
- Retrieve accounts

Add Safe Member

Search:

Search In:

Vault

Search

Selected Search: Vault

Name	Business Email	Full Name
------	----------------	-----------

☐ Access

☐ Use accounts☒ Retrieve accounts☐ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

☐ View Audit log☐ View Safe Members

Add

Close

- ☐ If the environment is configured for dual control:
 - In Privileged Account Security solutions (v8.0 and higher), when working with dual control, the Provider user can always access without confirmation, thus, it is not necessary to set this permission.
- ☐ If the Safe is configured for object level access, make sure that both the provider user and the application have access to the password(s) to retrieve.

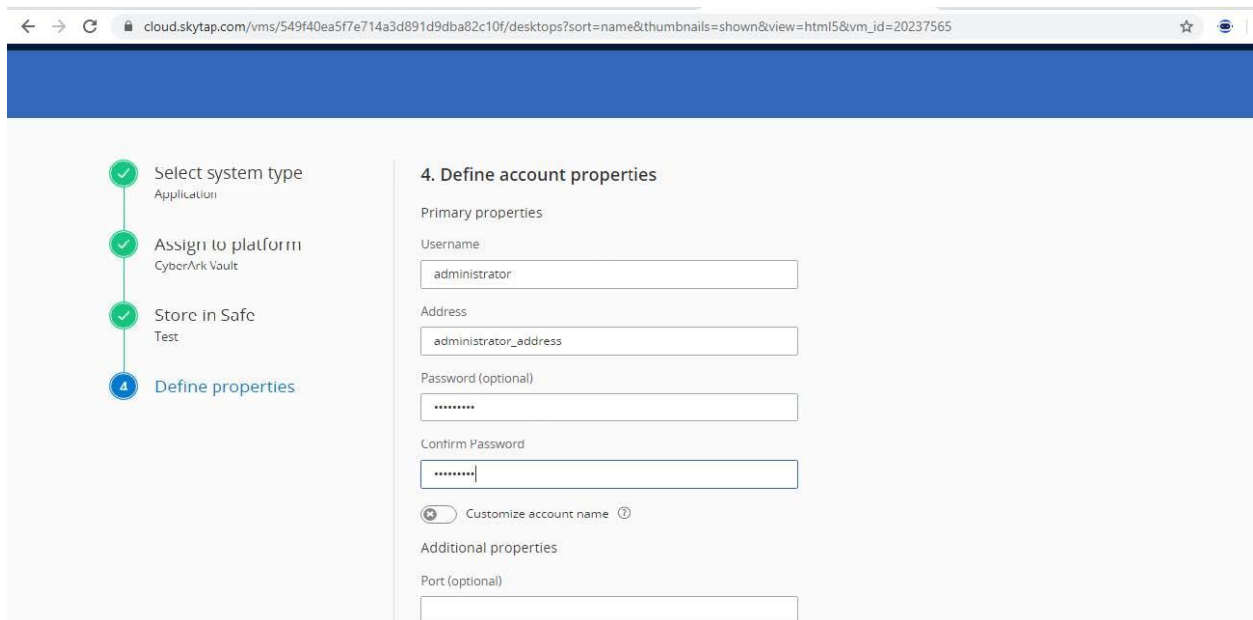
For more information about configuring Safe Members, refer to the **Privileged Access Security Implementation Guide**.

Refer to [TruBot Installation](#) for TruBot Robotics Process Automation installation.

Vault an account to connect to the WebServices SDK

The following image depicts creating the account TruBot will use to authenticate to the CyberArk WebServices SDK.

TruBot will use the WebServices SDK to locate credentials to be retrieved and create accounts that are needed for various RPA tasks.



The screenshot shows a web browser window with the URL `cloud.skytap.com/vms/549f40ea5f7e714a3d891d9dba82c10f/desktops?sort=name&thumbnails=shown&view=html5&vm_id=20237565`. The interface displays a four-step process on the left: 1. Select system type (Application), 2. Assign to platform (CyberArk Vault), 3. Store in Safe (Test), and 4. Define properties (highlighted with a blue circle). The main area is titled '4. Define account properties' and contains two sections: 'Primary properties' and 'Additional properties'. The 'Primary properties' section includes fields for 'Username' (containing 'administrator'), 'Address' (containing 'administrator_address'), 'Password (optional)' (masked with dots), and 'Confirm Password' (masked with dots). There is a checkbox for 'Customize account name' with a help icon. The 'Additional properties' section includes a field for 'Port (optional)'.

Main CyberArk configuration screen in the TruBot interface:

The following image depicts the TruBot interface that is used to set up the retrieval of privileged credentials.

CyberArk Configuration

Enable CyberArk Vault: ☒

Server: Port No.: Application Name:

Safe Name: Product Name: Encoded URL:

Serial No. for the Digital Certificate: Client Name on the Digital Certificate: Issuer Name:

Platform Name: Auth Endpoint: Account Endpoint:

AIM web service url:

Partner Application UI for Storage of the password in Vault:

Add Parameter-Value Set

Name: Description:

Category: Status: ☒

Parameter values

NAME	VALUE	Secure in vault
FlipkartPassword		☒
FlipkartID	987645212	☐

When the password is entered and the Save button is clicked, the following steps are carried out inside the Vault:

1. Store the credential used to authenticate to the WebServices SDK outlined in prior steps.
2. In the AAMWebService URL field
3. The Base URL – Provide the baseURL for the CCP AAMWebService
4. The AAMWebService is called with an ApplicationID to retrieve the credentials that will authenticate to WebServicesSDK.
5. Once these credentials are fetched, the Webservice SDK is called to either search for or create the Vault account object needed to continue the process.
6. Once the proper credential has been identified for the RPA Process, the AAMWebService will be called to retrieve the credential.

7. The JSON response received contains the ID and unique key which will be stored as metadata inside the Cockpit RDBMS. This also means that the password is stored successfully above. Please note that password is stored in the vault and not in the Cockpit RDBMS.

Sequence No	Feature Action	SDK	API	Params	Questions
Manual Step	First add the details on the REST API on the known URL in the CyberArk Vault.	Manually in CyberArk	Manually	https://practicaltesla.cyberark.skytapdns.com/AIMWebService/api/Accounts?AppID=Datamatics-TruBOT&Safe=Test;Object=Application-CyberArk-administrator_address-administrator	This request will return administrator and cyberark1 as a credentials, when called in the next step.
1	Store the Object Base URL. The username and password are stored in Vault and the hard coded URL AAMWebservice, is stored in the CyberArk config screen. This URL is a known URL, which means that even the initial password is not stored in the Cockpit RDBMS.	AAMWebservice	Auth / Returns the REST Token for subsequent requests. (Webservice Password)	Administrator and password	(1) This request will return administrator and cyberark1 as credentials.
2	Call the AUTH service.	Webservice	AUTH	The user ID and password in step 1.	Returns the token for the webservice.
3	Create Account Object with Provided Info in step 1 above.	Webservice	Accounts POST	Create Account object in the vault.	Use the token received from earlier step.

Web service calls:

Webservice requires token; and AAMWebservice requires digital certificates. Get final password is always using AAMWebservice.

No passwords, including the initial password, are stored in the Cockpit RDBMS. All passwords are always stored in the Vault.

Digital certificates:

The Digital certificates are stored in the client IIS server, which hosts the Cockpit Entity. Only then will the C# .Net code running on the Cockpit be able to talk to the CyberArk Vault for storing and retrieval of the password.

The component certificate has to be installed in the Personal Store. The scope should be machine level for these digital certificates.

PARTNER CONTACT INFO

Business Contact	Name	Shashi Bhargava
	Email	Shashi.Bhargava@datamatics.com
	Tel	+91 (226) 102-0000
Technical Contact	Name	Tejas Bavishi
	Email	Tejas.bavishi@datamatics.com
	Tel	+91 (226) 102-0000
Support Contact	Name	Hemraj Sadhnani
	Email	Hemraj.Sadhnani@datamatics.com
	Tel	+91 (226) 102-0000