



# CYBERARK SECRETS MANAGER

**(Agentless Central Credential Provider CCP)**

## SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: AntWorks Solutions Pte Ltd

Website: [www.ant.works](http://www.ant.works)

Name of Product: ANTstein QueenBOT

Version: Square

Date: 19 September 2018 (Revised 2 October 2020)

## ANTSTEIN QUEENBOT OVERVIEW

ANTstein QueenBOT is a robotic process automation platform which provides tools for automating business processes that are repetitive, mundane and involving rules-based decisions. QueenBOT enables the business user to automate the processes instead of a developer using intuitive BOTbuilder and to publish and deploy to various target machines via Orchestrator.

CyberArk is part of version Square of the product.

Version: Square

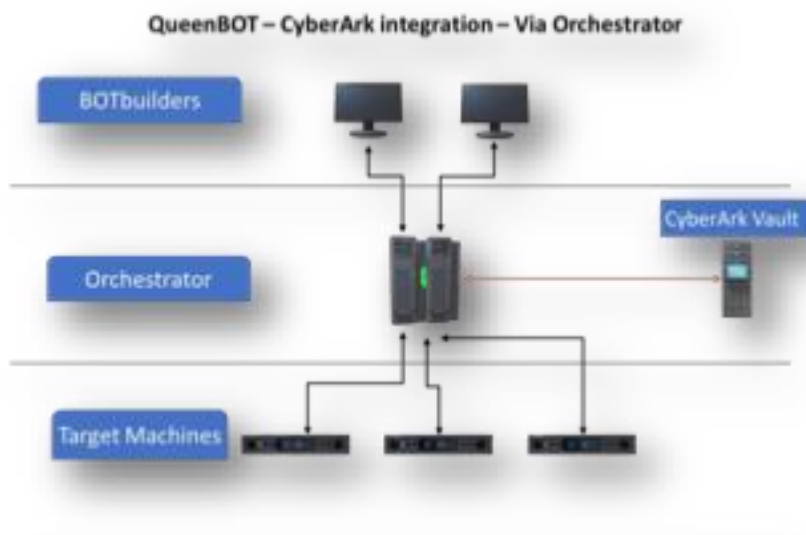
## KEY BENEFITS

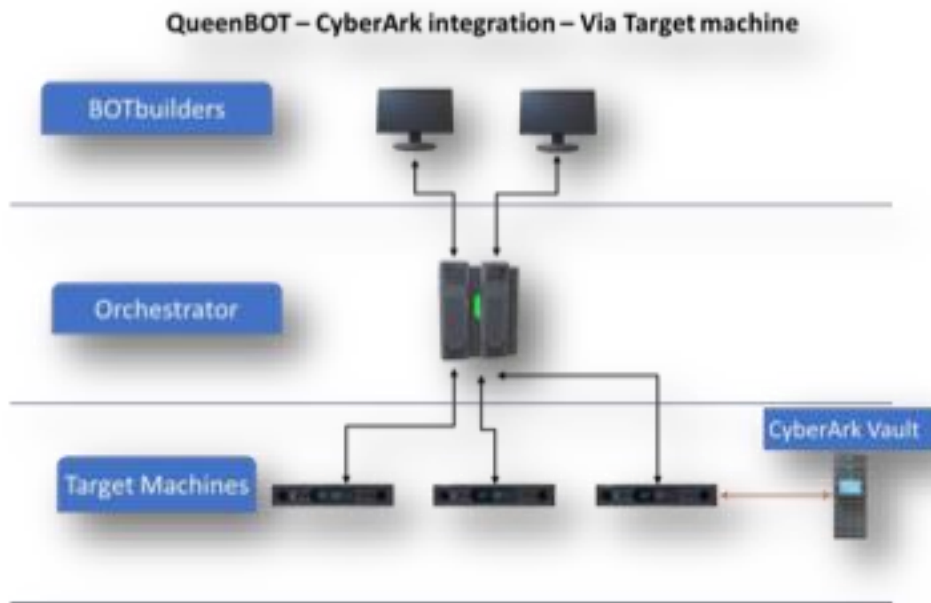
QueenBOT provides the RPA features in a simplistic way so even business user will be able to create Bots instead of only developer. The time taken for creating the automation using QueenBOT is only fraction of other tools in the market.

Security is a main tenant of the QueenBOT product to make all the enterprise process automations are well secured and reliable. So integration with CyberArk is a necessary step towards protecting the customer credentials.

## PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

QueenBOT can be integrated with CyberArk Secrets Manager via two ways such as Orchestrator and individual target machine.





## SECRETS MANAGER INTEGRATION

CyberArk connector has been created to integrate the ANTstein QueenBOT with CyberArk vault and to communicate and extract the credential information for the business process.

CyberArk is a leader in credential management platform and provides the security service to major institutions. Seamless integration of ANTstein QueenBOT with CyberArk provides added advantage for the customers in automating secure processes.

Added security is provided for the extracted credential data by encrypting it internally before being used in a business process. This ensures that credential data is not to be seen on a display.



## INPUT PROPERTIES

Input properties are primarily the CyberArk request input parameters. All the required parameters are to be filled for retrieving the credential data.

Mandatory CyberArk parameters

- Application ID - This is app id of the CyberArk request
- Safe - Safe of the credential data
- Folder - Folder of the credential data
- Object - Object of the credential data

Optional parameters for CyberArk request

- Connection Port - Custom port to be supplied in the request
- Reason - Reason to be added in the request for audit
- Other Properties - Any other properties to be added in the credential request to CyberArk

QueenBOT Parameters

- Timeout Duration - Waiting time for the response from the CyberArk in seconds. If it exceeds, the component will throw exception which can be handled in subsequent components.

- Run Local - This indicator is to specify which machine to request CyberArk credential data. This parameter can be added as Run time so it can be modified during deployment of Bots.
  - Local - CyberArk call would be made from current BOTbuilder. Expectation is BOTbuilder has all the CyberArk SDK and setup required to make the call.
  - Orchestrator - This option is relevant when there are multiple machines which require CyberArk credential. In this option, Orchestrator would act as a broker for the remote machines to retrieve password and to transmit it encrypted format in an secured channel.

## OUTPUT PARAMETERS

The following parameters can be extracted from the CyberArk credential request. All these parameters would be available in variables which can be used in subsequent components.

- User Name - User Id of the credential
- Password - Password of the request
- Address
- Content
- Database
- PolicyID
- Result properties

## CREDENTIAL RETRIEVAL

The following components can be used to use the credential data after it is made available by CyberArk connector.

- Email Watcher – for Email account user name and password
- Email Sender – for Email account user name and password
- DB Processor – for Database user name and password
- DB Watcher – for Database user name and password
- Web Runner – for any business process credential
- Windows Runner – for any business process credential
- Remote Runner – for any business process credential

## REQUIREMENTS

CyberArk SDK has to be installed in the machine where QueenBOT Orchestrator or QueenBOT BOTbuilder is present. This is governed by parameter “Run Local” in the component.

There needs to be registered in the CyberArk server for this machine so requests can be serviced from QueenBOT.

## 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 ANTstein QueenBOT configuration with CyberArk Secrets Manager.

### DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

To define the application, configure 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.

The screenshot shows the 'Add Application' dialog box. The 'Name' field contains 'AntWorks\_QueenBOT'. The 'Description' field is empty. The 'Business owner' section has empty fields for 'First Name', 'Last Name', 'Email', and 'Phone'. The 'Location' field is a dropdown menu showing a backslash character. The 'Access Permitted' checkbox is unchecked, and the 'From' and 'To' fields are empty dropdowns. The 'Expiration Date' checkbox is unchecked, and the 'Disabled' checkbox is unchecked. The 'Add' and 'Cancel' buttons are at the bottom right.

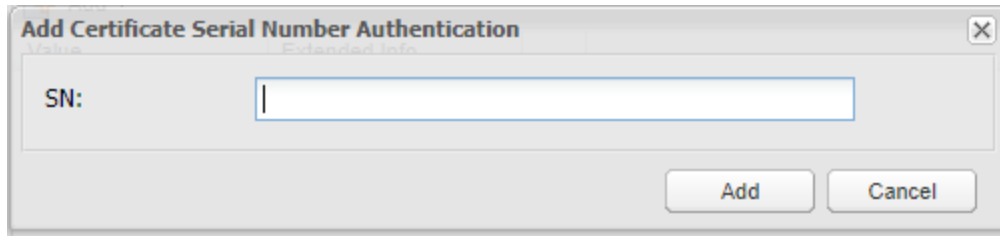
- ☐ Specify the following information:
- ☐ In the Name box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: AntWorks\_QueenBOT
  - In the **Description** box, specify a short description of the application that will help you identify it.
  - In 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. 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.



Instructions on how to get the Certificate Serial Number:

**Windows:**

Start -> certmgr.msc (Current User) -> expand Personal -> select Certificates -> double-click on certificate to open

Start -> certlm.msc (Local Computer) -> expand Personal -> select Certificates -> double-click on certificate to open

**If the first two options do not work in your env:**

Start -> mmc.msc -> File; Add/Remove Snap-in -> Certificates -> Add -> OK -> you may be prompted to choose Local Computer or Current User -> OK

Expand Certificates -> Personal -> Certificates -> Double-Click on a certificate to open.

Once the certificate is open -> Details tab -> Serial Number is in the list of values shown

Once the certificate is open

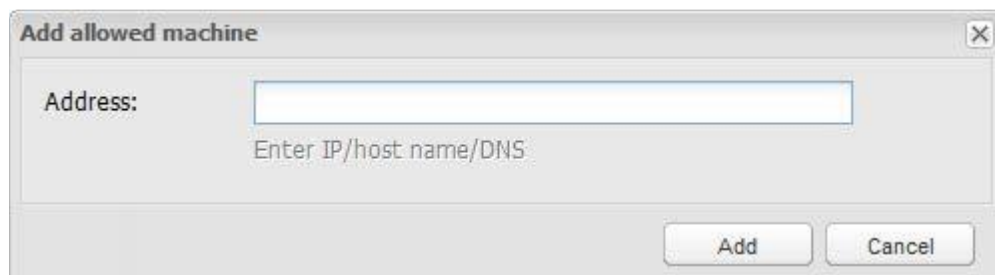
OpenSSL

openssl x509 -in <cert file name> -serial -noout

- This is the most secure way to authenticate the application for CCP
- The following are enhanced ways of authenticating

☐ 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.



- 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. Make sure the servers allowed include all mid-tier servers or all endpoints where the Secrets Manager Credential Providers were installed.



## 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**.

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
- View Safe Members

**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 your environment is configured for dual control:
  - In PIM-PSM environments (v7.2 and lower), if the Safe is configured to require confirmation from authorized users before passwords can be retrieved, give the Provider user and the application the following permission: **Access Safe without Confirmation**
  - 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**.

## ANTSTEIN QUEENBOT INSTALLATION & INTEGRATION CONFIGURATION

CyberArk SDK has to be installed in the machine where QueenBOT Orchestrator or QueenBOT BOTbuilder is present. This is governed by parameter “Run Local” in the component.

There needs to be registered in the CyberArk server for this machine so requests can be serviced from QueenBOT.

## PARTNER CONTACT INFO

|                   |       |                          |
|-------------------|-------|--------------------------|
| Business Contact  | Name  | Leslie Holland           |
|                   | Email | leslie.holland@ant.works |
|                   | Tel   | +1 (650) 798-5061        |
| Technical Contact | Name  | Pandurangan Narasimman   |
|                   | Email | Pandurangan.n@ant.works  |
|                   | Tel   |                          |
| Support Contact   | Name  | Pandurangan Narasimman   |
|                   | Email | Pandurangan.n@ant.works  |
|                   | Tel   |                          |