



SECRETS MANAGER

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Cognizant Technology Solution

Website : www.cognizant.com

Name of Product: Cognizant® Automation Center

Version: 4.1.1

Date: 10/1/2020

PARTNER SOLUTION OVERVIEW

Cognizant® Automation Center is an AIOps platform for automating the datacenter activities for both Infrastructure and applications arena. It also offers Domain-driven solutions to its customers.

Cognizant® Automation Center can integrate very well into the datacenter ecosystem. CyberArk is an industry standard password management tool and widely used by our customers for Credentials management. Cognizant® Automation Center has capability to integrate with CyberArk for retrieval of centrally stored credentials in an automated way while performing its key functionalities.

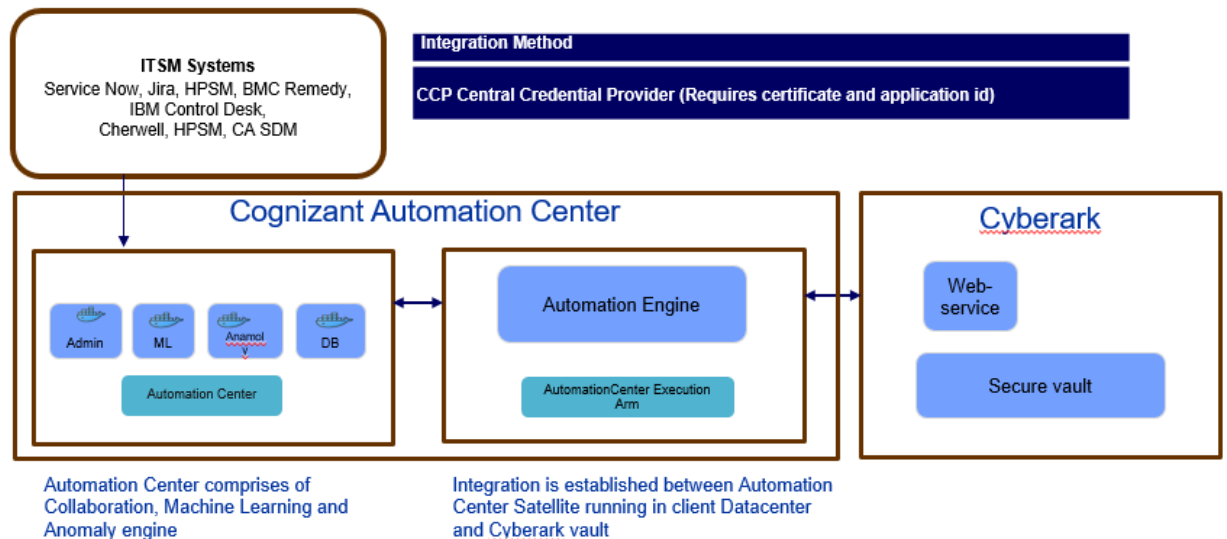
Automation Center supports an API based integration with CyberArk v1 and v2 API versions.

KEY BENEFITS

Key benefits of integrating Cognizant® Automation Center with CyberArk Secrets Manager:

- CyberArk is industry standard password management tool
- CyberArk used across various Cognizant customers
- The integration with CyberArk extends the automation capabilities of Automation Center by providing the customers with a secure and seamless automation experience

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



Cognizant® Automation Center is Cognizant’s AIOps platform for working on IT infrastructure and IT application issues. It is well connected with various ITSM/Events sources to get the feed of proactive and reactive issues/problems as shown in the diagram above. These issues/problems get represented as activities in Automation Center.

SRE can login to Automation Center portal and execute various diagnostic actions to troubleshoot the issue and subsequently resolve issue using resolution actions. To run these diagnostic and resolution action, control is passed on to Automation Engine component, which in turn connects to target CIs/Applications. Automation Engine connects and retrieves account id and password from CyberArk. This information is used to establish connection to target CI and not stored with Automation Center. CyberArk integration is achieved at Mid-tier (using CCP – Central Credential Provider). Credential retrieval is triggered at every action execution level – whenever customer entities are accessed to perform the actions on end CI.

- Linux, Windows
- Databases, network elements
- Other platforms like email, ITSM etc.

Note: Password write operation to CybeArk vault is not required.

SECRETS MANAGER INSTALLATION

Refer to the “Central Credential Provider Implementation guide” for Agentless installation and configuration.

There is no configuration for Cognizant’s Automation platform to be done in CyberArk. Cognizant Automation Center will connect to CyberArk Central Credential Provider(CCP) component and will retrieve password from CyberArk vault safe.

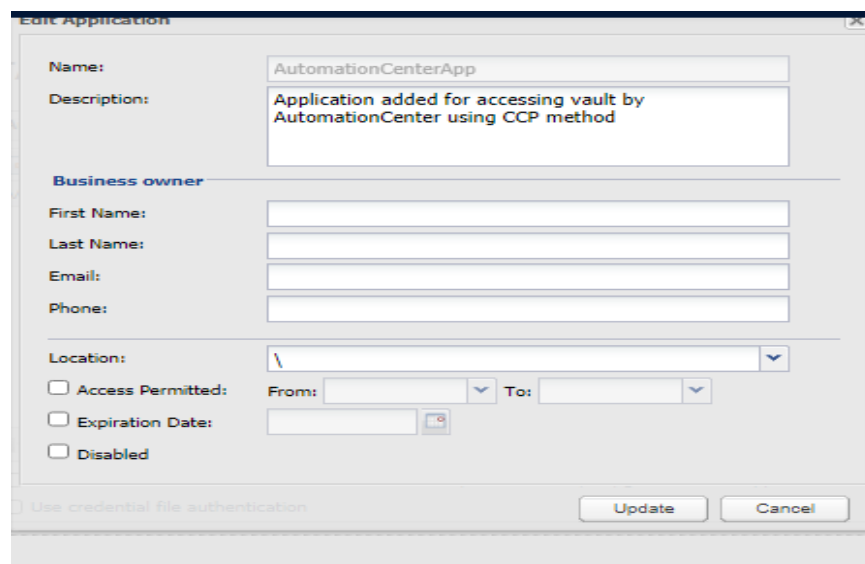
Cognizant Automation Center’s scope is limited to integration with CyberArk for credentials retrieval only. Secrets Manager installation is not included in the scope.

SECRETS MANAGER CONFIGURATION

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

To define the Application, here are the instructions to define it manually via CyberArk’s PVWA (Password Vault Web Access) Interface:

1. Logged in as user allowed to managed applications (it requires Manage Users authorization), in the Applications tab, click **Add Application**; the Add Application page appears.

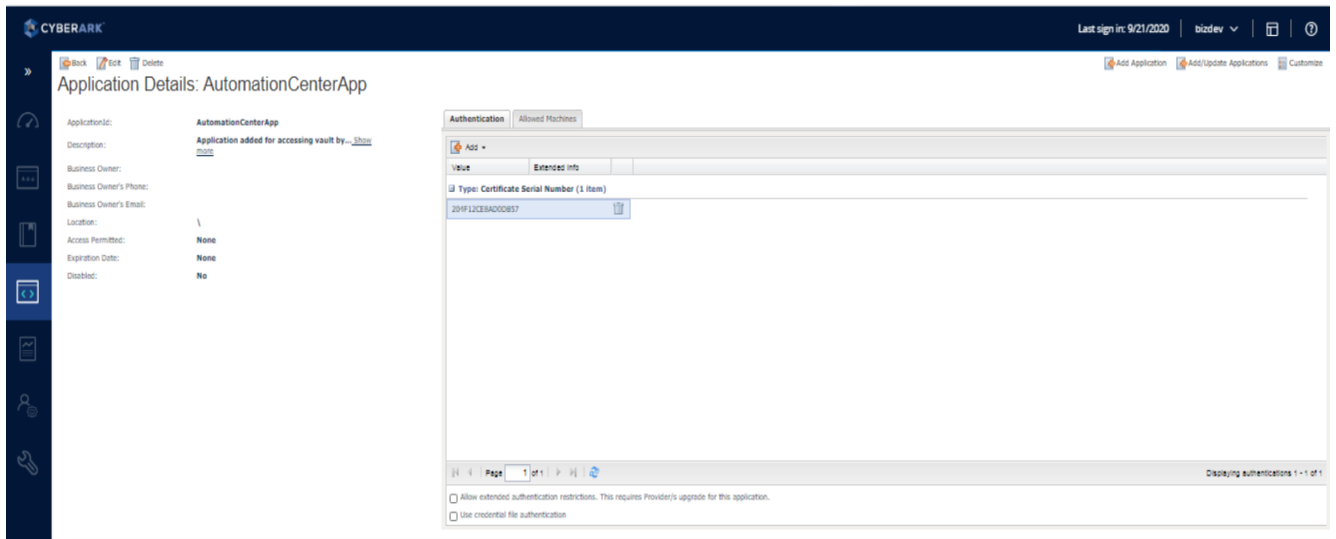


Comment: This Image Specifies the creation of Application inside CyberArk Server.

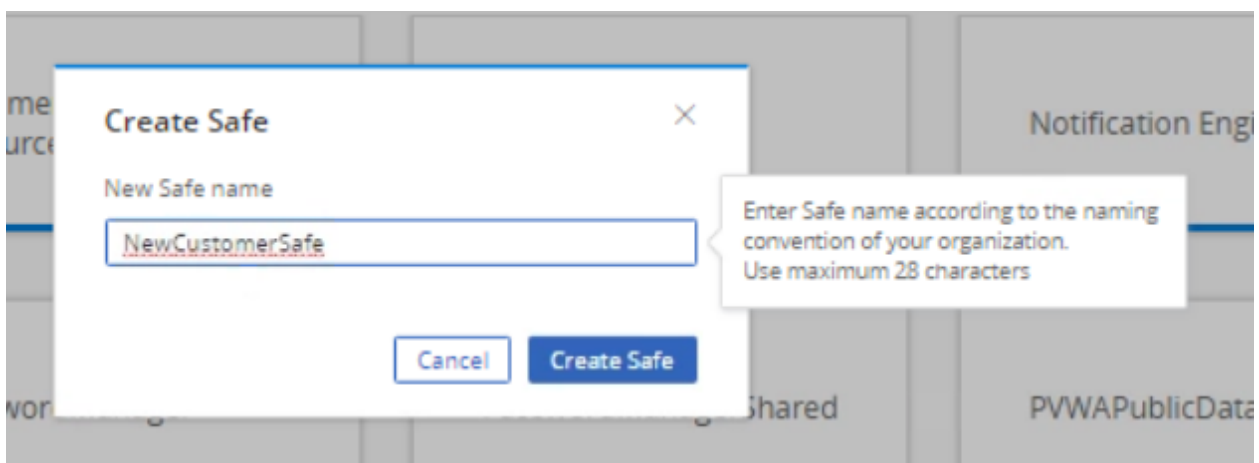
2. Specify the following information:
 - In the Name edit box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: APP ID = AutomationCenterApp
 - In the Description, specify a short description of the application that will help you identify it.

- In the Business owner section, specify contact information about the application's Business owner.
- In the lowest section, 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.

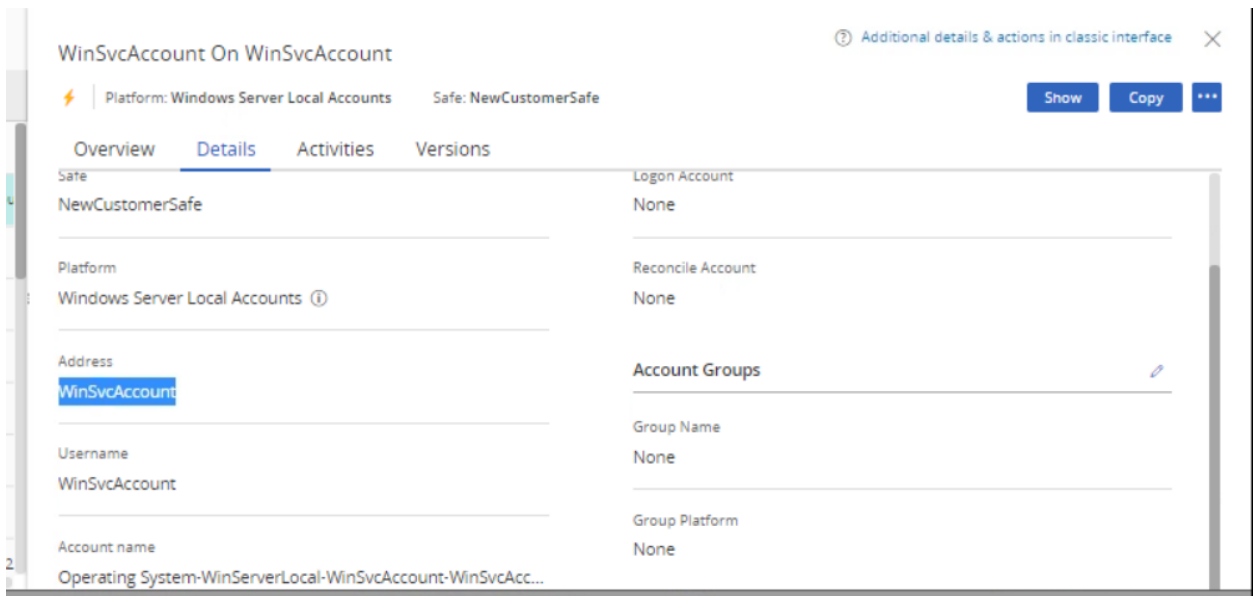
3. Click **Add**; the application is added and is displayed in the Application Details page.



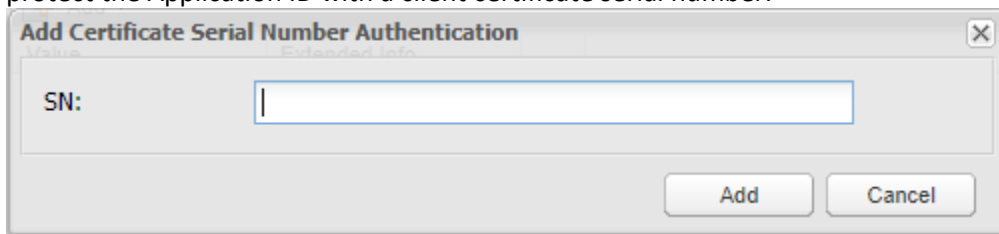
Creating Safe :



Account details:



- **Allowing extended authentication restrictions.** This enables you to specify an unlimited number of machines and Windows domain OS users for a single application. Please check this box.
4. 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.
 5. Specify the Certificate Serial number:
 - a. When using the Agentless Secrets Manager(Central Credential Provider) there's an option to protect the Application ID with a client certificate serial number:



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 (Step 1). 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 (Step 2).

1. 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**.

2. Add the Credential Provider and application users as members of the Password Safes where the application passwords are stored. This can be done either manually in the Safes tab, or by specifying the Safe names in the CSV file for adding multiple applications.
 - i. 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:

Selected Search: Vault Display 1 result(s)

Name	Business Email	Full Name
 AutomationCenterApp		

☐ Access

- ☒ Use accounts
- ☒ Retrieve accounts
- ☒ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

- ☒ View Audit log
- ☒ View Safe Members

☐ Workflow

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

Add Safe Member

Search: AutomationCentr

Search In: Vault

Search

Selected Search: Vault

Display 1 result(s)

Name	Business Email	Full Name
AutomationCenterApp		

☐ Access

☐ Use accounts
 ☒ Retrieve accounts
 ☐ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

☐ View Audit log
 ☐ View Safe Members

☐ Workflow

Add

Close

- iii. If your environment is configured for dual control:
 - In Privileged Account Security solutions , when working with dual control, the Provider user can always access without confirmation, thus, it is not necessary to set this permission.
- iv. 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 CognizantAutomationCenter-Install.doc for Cognizant Automation Platform installation.

Steps to configure Cognizant Automation Center Platform to work with Secrets Manager:

1. In Automation Center, CyberArk vault has to be onboarded giving below information.

This information will be used to connect to CyberArk vault.

- a. CyberArk vault url and port
- b. Application id as onboarded in CyberArk vault
- c. CyberArk vault username
- d. Other details.

Cognizant[®]
Automation Center
I&O

All Modules Home Entities x Entity - crv-1592305418213 x

Entity Attributes Entity View

Refresh

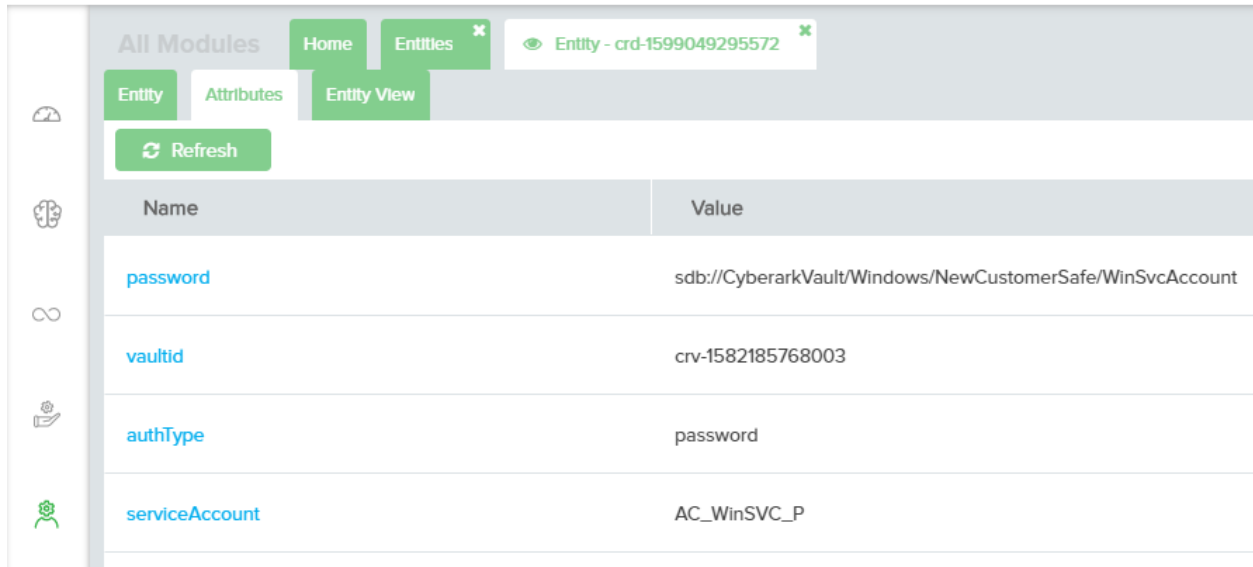
Name	Value
username	Administrator
Folder	Root
driver	automationcenter_cyberarkvault
url	https://services-uscentral.skytap.com:14776
Type	ccp
AppID	AutomationCenterAppid

2. Using this vaultID, onboard a credential entity for the password that is stored in the CyberArk vault. Here we use sdb url to denote the location of password in the vault.

This url will be used as location map inside CyberArk vault to retrieve the password

e.g

sdb://<vault_name>/<Technology>/<Safe_name>/<Keyword(or)Account_name>



Name	Value
password	sdb://CyberarkVault/Windows/NewCustomerSafe/WinSvcAccount
vaultid	crv-1582185768003
authType	password
serviceAccount	AC_WinSVC_P

Common use cases:

1. Windows domain credentials or other standard credentials
 - a. The user will specify: username, address, platform
 - b. Safe name – optional but recommended for increasing performance
2. Local accounts (windows/Unix)
 - a. The user will specify: username & platform
 - b. Safe name – optional but recommended for increasing performance
 - c. When scanning, need to request in the API these username and platform, and add the address of the current machine being scanned
3. Non-standard credentials (can't be unique with username+address+Platform)
 - a. The user will specify: Safe and object name (folder is usually root by default)

PARTNER CONTACT INFO

Business Contact	Name	Gopal Krishnan
	Email	Gopal.krishnan@cognizant.com
	Tel	+919384015939
Technical Contact	Name	Manish Ansingkar
	Email	Manish.Ansingkar@cognizant.com
	Tel	+917720029382
Support Contact	Name	Kalyan Das
	Email	Kalyan.Das@cognizant.com
	Tel	+918336988446