



SECRETS MANAGER

(Agentless Central Credential Provider CCP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION TEMPLATE

Name of Company: TIBCO Software, Inc.

Website: <https://www.tibco.com/>

Name of Product: TIBCO BusinessWorks™ Container Edition

Version: 2.7.1

Date: 13th May' 2022

PARTNER SOLUTION OVERVIEW

Integrate highly reliable, scalable, and secure services and applications that are critical to your business. With TIBCO BusinessWorks™ software, your integration specialists can implement application strategies using both traditional enterprise integration patterns and modern cloud-based API-led approaches built with microservices and containers. A zero-code model-driven environment based on Eclipse simplifies development complexity, helping reduce your costs and speed your time to market.

Version: 2.7.1

Platform components:

- TIBCO Business Studio™ for BusinessWorks™
- Deployment on any supported containerized platform

KEY BENEFITS

Benefits of TIBCO BusinessWorks™ Container Edition:

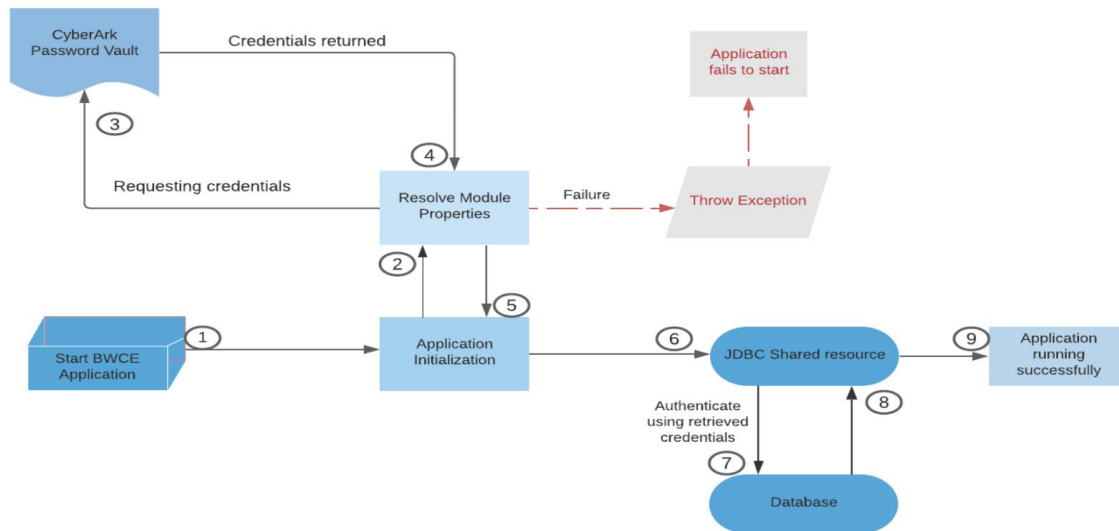
- Design modern enterprise integrations
- Build with control and flexibility
- Rigorously test integration processes
- Deploy portable integrations
- Manage mission critical integrations

Benefits of integrating TIBCO BusinessWorks™ Container Edition with CyberArk Secrets Manager:

- Achieving security in storing the passwords
- Dynamic update of passwords without change required in the application

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

Credential Management in BWCE using CyberArk



SECRETS MANAGER INTEGRATION

TIBCO BusinessWorks™ Container Edition provides the ability to integrate with CyberArk Secrets Manager for customers who want to achieve the security in storing the passwords, automatically replace the passwords, and so on via CyberArk. The CyberArk credential management service is more secure than the passwords in clear text format stored in the configuration files.

Flow of Integration:

- While designing the application, password values are externalized to CyberArk platform along with providing appropriate values for CyberArk custom fields such as Server URL, App ID, query.
- Once an application is designed and ready to be deployed, the application container will initiate connection with the CyberArk server via environment variables provided at the time of application deployment. Environment variables required to initiate connection such as APP_CONFIG_PROFILE and setting the CyberArk integration value to TRUE as depicted in product documentation.

There is no requirement of downloading any third-party tool or service to establish connection between TIBCO BusinessWorks™ Container Edition and CyberArk.

CREDENTIAL RETRIEVAL

The Credential fetching/retrieval is triggered when appropriate environment variables are used while deploying the application on a supported platform.

The environment variables used on any supported OS on docker/kubernetes supported platform. The required environment variables are listed here:

<https://docs.tibco.com/pub/bwce/2.7.1/doc/html/app-dev-guide/using-credential-man.htm>

REQUIREMENTS

- All supported OS, deployment platforms are listed in Product Readme:
https://docs.tibco.com/pub/bwce/2.7.1/TIB_bwce_2.7.1_readme.txt?id=0
- No specific requirements required for CyberArk integration separately, user designing/deploying application can access CyberArk integration as well.

SECRETS MANAGER INSTALLATION

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

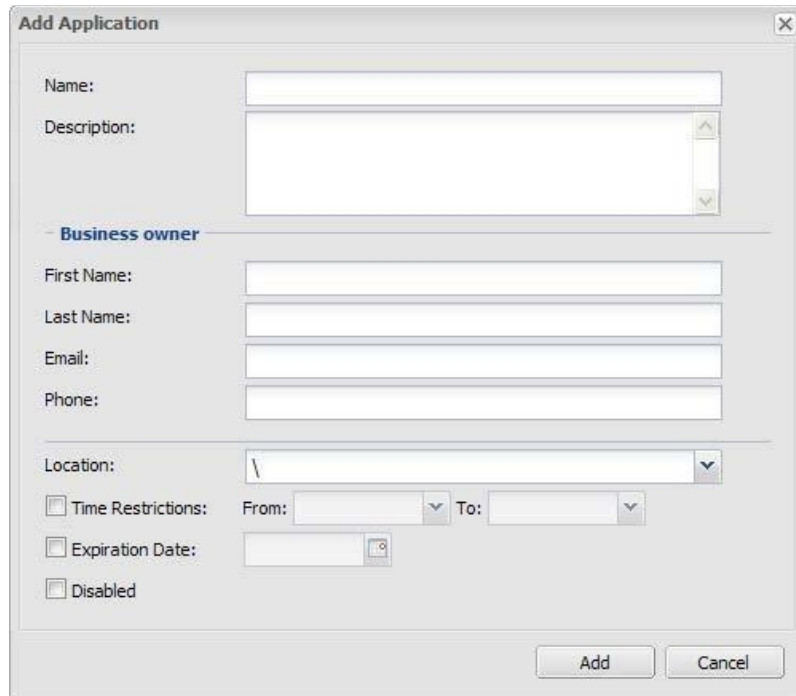
SECRETS MANAGER CONFIGURATION

The following sections provide details on TIBCO BusinessWorks™ Container Edition configuration with CyberArk Secrets Manager: <https://docs.tibco.com/pub/bwce/2.7.1/doc/html/app-dev-guide/using-credential-man.htm>

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.



Add Application

Name:

Description:

Business owner

First Name:

Last Name:

Email:

Phone:

Location:

☐ Time Restrictions: From: To:

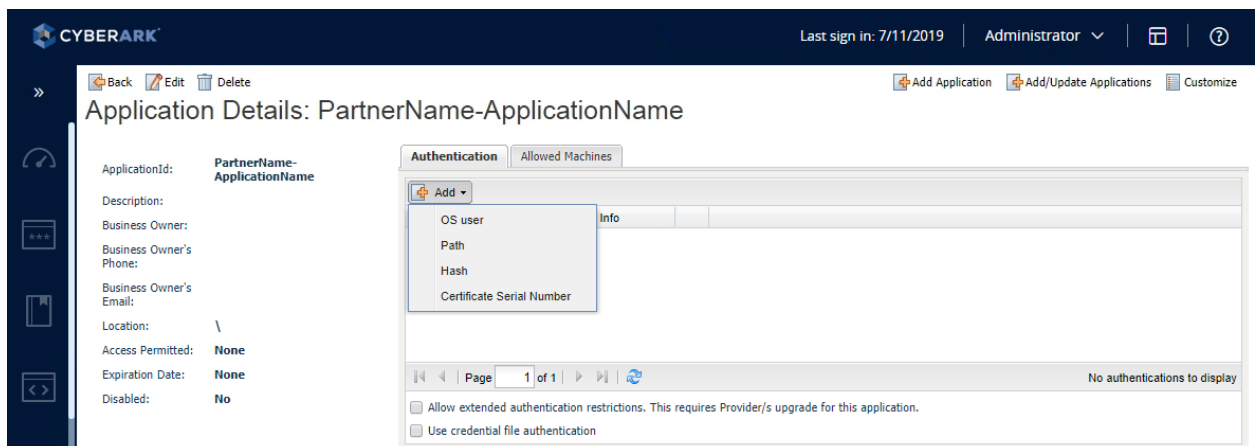
☐ Expiration Date:

☐ Disabled

2 Specify the following information:

- In the **Name** box, specify the unique name (ID) of the application.
- 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.

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



CYBERARK Last sign in: 7/11/2019 Administrator

Back Edit Delete Add Application Add/Update Applications Customize

Application Details: PartnerName-ApplicationName

ApplicationId: PartnerName-ApplicationName

Description:

Business Owner:

Business Owner's Phone:

Business Owner's Email:

Location: \

Access Permitted: None

Expiration Date: None

Disabled: No

Authentication Allowed Machines

- OS user
- Path
- Hash
- Certificate Serial Number

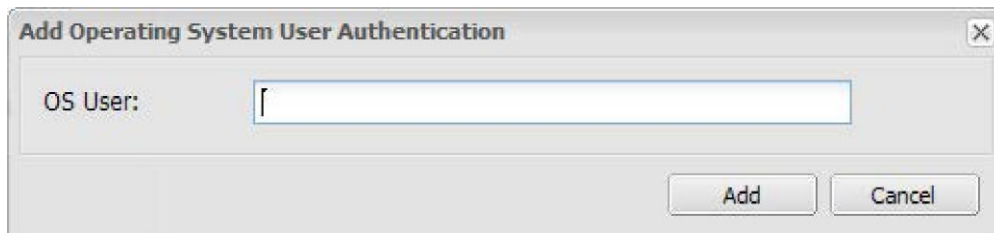
Page 1 of 1

No authentications to display

☐ Allow extended authentication restrictions. This requires Provider/s upgrade for this application.

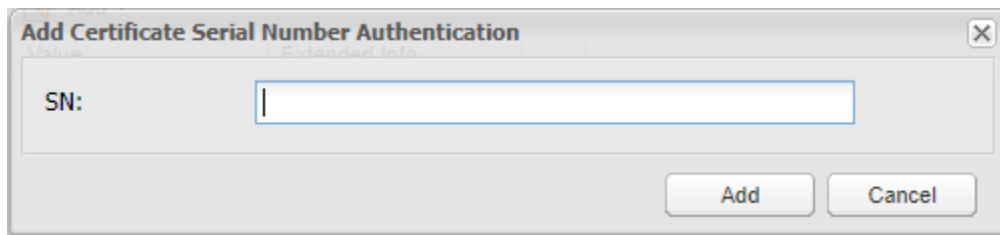
☐ Use credential file authentication

- 2 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.
- 2 Specify the application's **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password.
- 2 In the Authentication tab, click **Add**. A drop-down list of authentication characteristics is displayed.
- 2 Select the authentication characteristic to specify.
- 2 Select **OS user**. The Add Operating System User Authentication window appears.



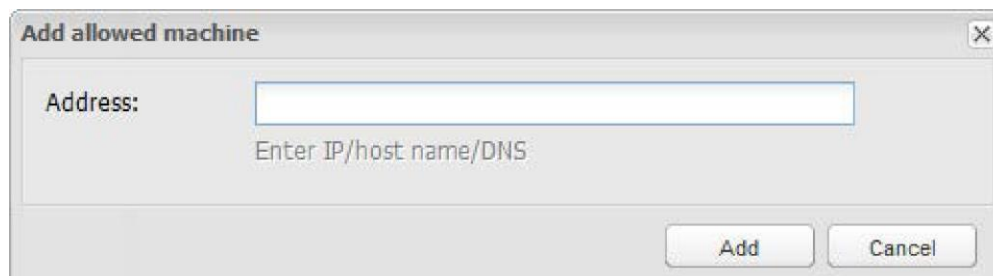
The dialog box is titled "Add Operating System User Authentication". It contains a label "OS User:" followed by a text input field. At the bottom right, there are two buttons: "Add" and "Cancel".

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



The dialog box is titled "Add Certificate Serial Number Authentication". It has two tabs: "Basic" (selected) and "Extended Info". Under the "Basic" tab, there is a label "SN:" followed by a text input field. At the bottom right, there are two buttons: "Add" and "Cancel".

- 2 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.



The dialog box is titled "Add allowed machine". It contains 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, 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**.

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:

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

- 2 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

- 2 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**.

PARTNER PRODUCT INSTALLATION & INTEGRATION CONFIGURATION

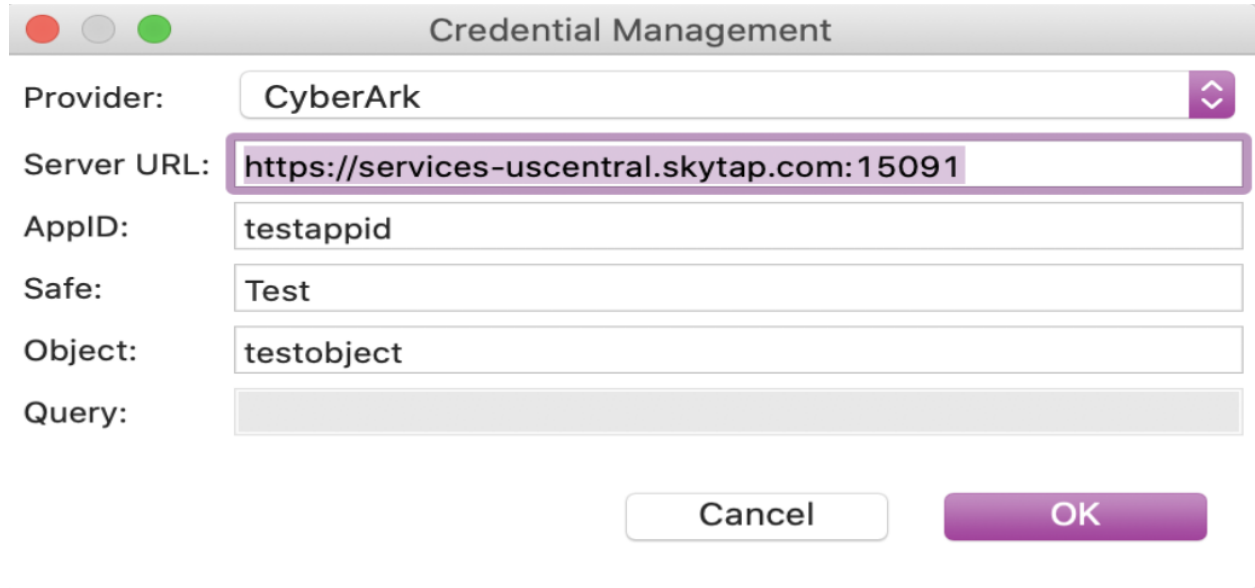
Refer to TIBCO BusinessWorks™ Container Edition for Partner Product installation.

List specific steps to configuring Partner Product to work with Secrets Manager, including:

1. Provide required CyberArk configuration values while designing the application in TIBCO Business Studio™ for BusinessWorks™

2. How to specify credentials for scanning, that are stored in the Vault (instead of providing usernames and passwords) – include screenshots and description of steps

Partner Application UI:



Credential Management

Provider: CyberArk

Server URL: https://services-uscentral.skytap.com:15091

AppID: testappid

Safe: Test

Object: testobject

Query:

Cancel OK

Common use cases:

1. Any type of password required for any third-party connection for application processing:
For example: With BusinessWorks™ applications, for a lot of use-cases customers need to connect to a database to store/fetch data for processing of applications. Data base connection is provided via Shared resource in the application. Passwords can be stored in CyberArk and fetched directly at runtime.

PARTNER CONTACT INFO

Business Contact	Name	Karan Gera
	Email	kgera@tibco.com
	Tel	
Technical Contact	Name	Santosh Kumar
	Email	santkumar@tibco.com
	Tel	
Support Contact	Name	Karan Gera
	Email	kgera@tibco.com
	Tel	

