Secrets Manager Agent-based Credential Provider (CP) Integration

Secrets Manger Integration – Technical Documentation Template

Name of Company: **Tricentis**
Website: **https://tricentis.com**
Name of Product: **Tricentis Tosca**
Version: **2024.1**
Date: **10/07/2024**

Table of Contents

1. PARTNER SOLUTION OVERVIEW

Tricentis Tosca is a test automation platform that is capable of testing applications of various technologies. It allows to test entire business processes end-to-end. For this, Tosca needs to be able to authenticate to different systems. To store the credentials for these authentications, Tosca can fetch secrets from various authentication providers, such as CyberArk.

Version: **2024.1**

Platform components:

- **Tosca Commander**
- **Tricentis Automation Service**
- **Tosca Cloud**
- **Distributed Execution Agent**

2. KEY BENEFITS

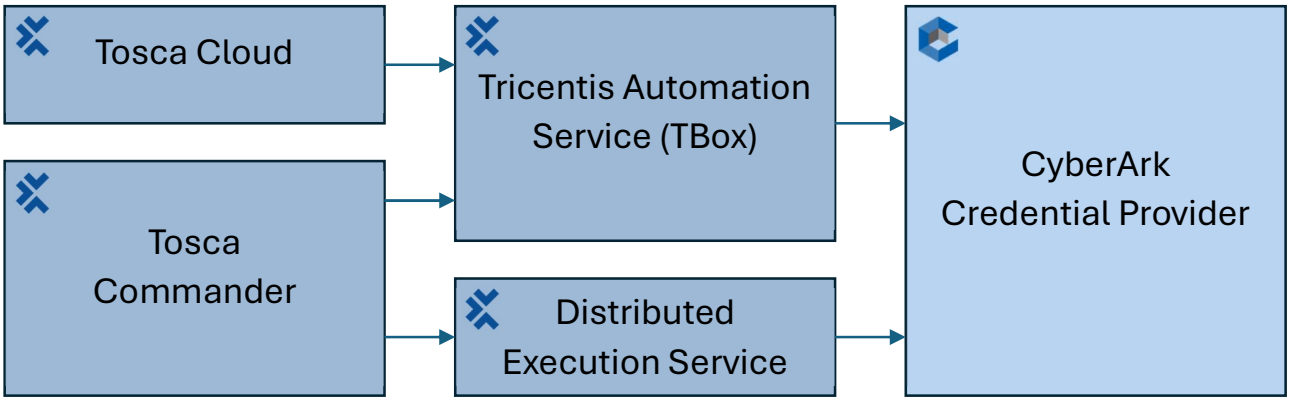
Benefits of **Tricentis Tosca:**

- **Automated testing of entire end-to-end processes across systems**
- **Module-based testing approach that minimizes test case creation effort.**

Benefits of integrating **Tricentis Tosca** with CyberArk Credential Provider:

- **Secure access to applications and environments**
- **Simplification of sharing secrets in organization and avoiding copying of secrets since Tosca can retrieve them right from CyberArk.**

3. PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



3.1 Credential Provider integration

CyberArk is integrated into Tricentis Tosca in several places:

- During execution, secrets from CyberArk can be retrieved using the {SECRET} and {OTP} dynamic values. The {OTP} value allows to generate Timed-One-Time-Passwords from CyberArk secrets. In this scenario, the secrets are retrieved by the Tricentis Automation Service (TBox).
- In Mobile Engine, secrets can be used in capabilities to store credentials. In this scenario, Tricentis Automation Service (TBox) retrieves the secrets.
- CyberArk secrets can be used in DEX Server to provide credentials for Database and Tosca Server connections. In this scenario, DEX Server retrieves the secrets.

3.2 Credential retrieval

In all cases, secrets are retrieved on demand. For execution, this is when TestStepValue in which the dynamic value is used is executed. For DEX and Mobile engine this is during component startup. The credentials are retrieved via an API call to the CyberArk Credential Provider .NET Core API.

4. REQUIREMENTS

This section lists the requirements for integration.

To retrieve secrets, the relevant component (e.g., Tosca Commander with Tosca Automation Service) needs to be installed on the machine. CyberArk Credential Provider needs to be installed, and its service needs to be running. The Credential Provider's API installation directory needs to be accessible to the Tricentis Automation Service or DEX Server, depending on the component using the integration.

5. CREDENTIAL PROVIDER INSTALLATION

To install a Credential Provider (CP), see the CyberArk Credential Providers documentation.

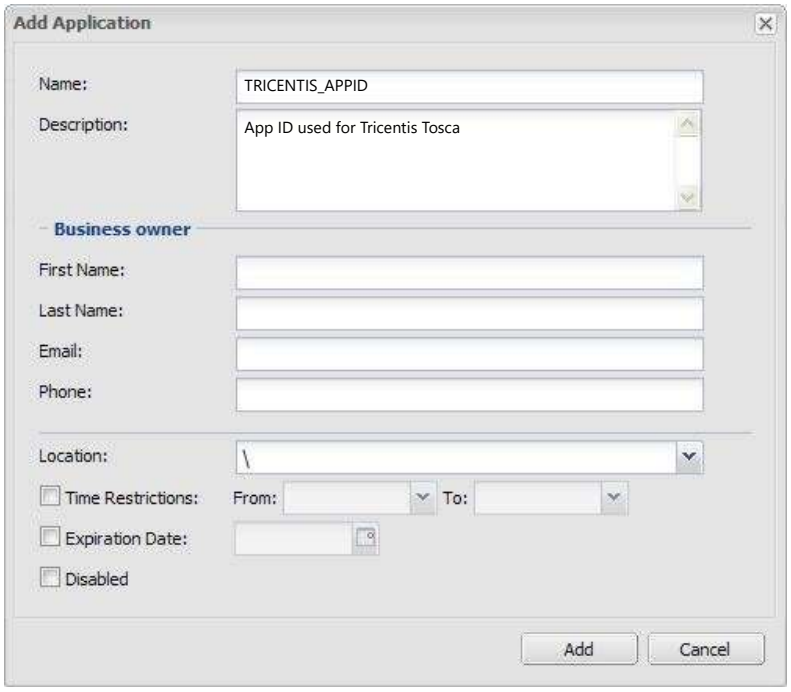
6. CREDENTIAL PROVIDER CONFIGURATION

The following sections provide details on the Credential Provider (CP) configuration with your CyberArk PAM solution (PAM Self-hosted / Privilege Cloud).

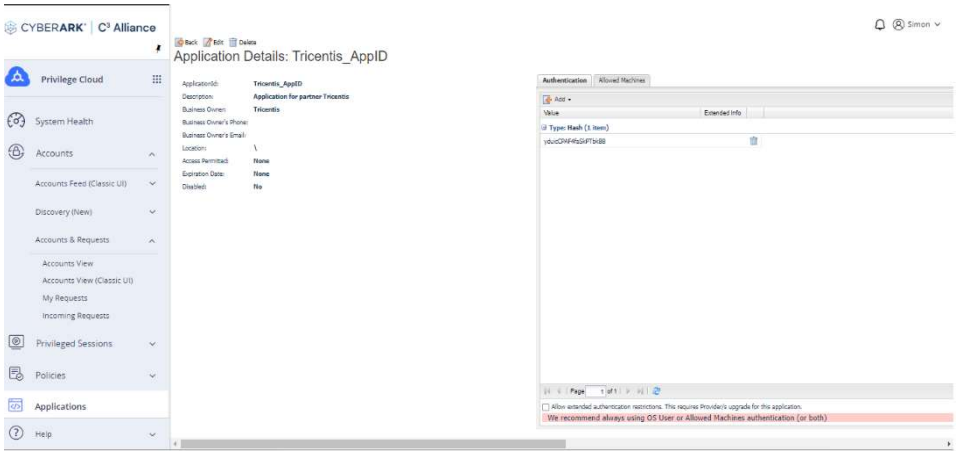
6.1 Define the application identity (app ID) and authentication details

To define an identity for your application in the Credential Provider, define it manually through the CyberArk Password Vault Web Access (PVWA) / Privilege Cloud interface:

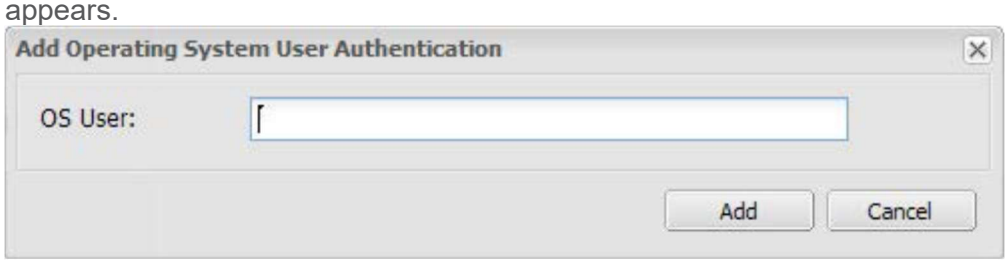
1. Log into the interface with a user that has permissions to manage applications (it requires **Manage Users** authorization)
2. In the Applications tab, click **Add Application**. The Add Application page appears.



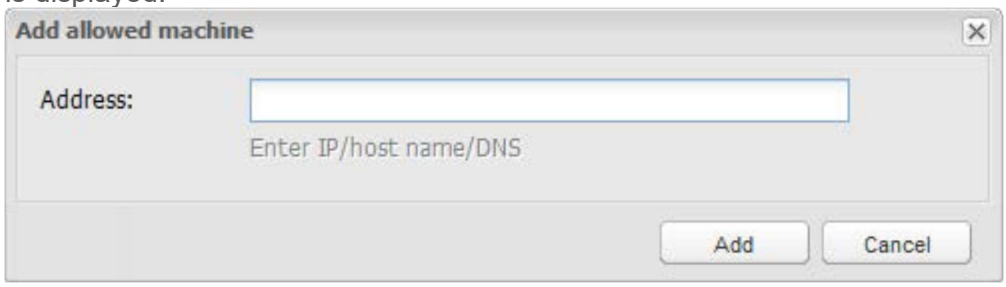
3. Specify the following information:
    - In the Name box, provide the unique name (ID) of the application. The recommended application ID for this integration is: APP ID = **Tricentis_AppID**
    - In the **Description** box, provide a short description of the application that will help you identify it.
    - In the **Business owner** section, provide contact information about the application's business owner.
    - In the **Location** box, specify the location of the application in the Vault / Privilege Cloud hierarchy. If a location is not selected, the application will be added in the same location as the user who is creating this application.
4. Click **Add**. The application is added and is displayed on the Application Details page.



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



   d. Specify the name of the OS user who will run the application, then click **Add.** The OS user is listed in the Authentication tab.
7. Specify the application's Allowed Machines. This information enables the Credential Provider to make sure that applications that run only from specified machines can access their passwords.
   a. In the Allowed Machines tab, click **Add**. The Add allowed machine window is displayed.



b. 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 Credential Providers were installed.

6.2 Provision accounts and set permissions for application access

For the application to perform its functionality or tasks, the application must have access to particular accounts that already exist, or to new accounts to be provisioned in CyberArk Vault / Privilege Cloud.

In the **safe you want Tricentis Tosca to fetch secrets from**, provision privileged accounts that will be required by the application. You can do this in one 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 need **Add accounts** permissions in the **relevant safe**.

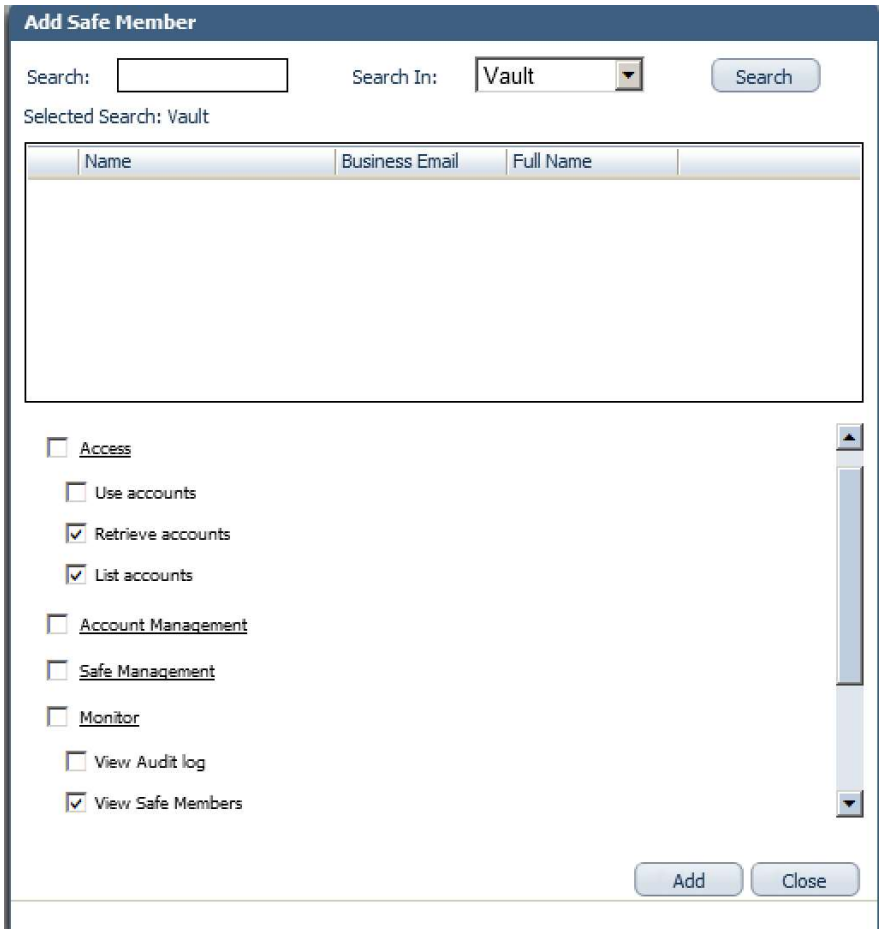
For more information about adding and managing privileged accounts, see the documentation for your PAM solution.

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

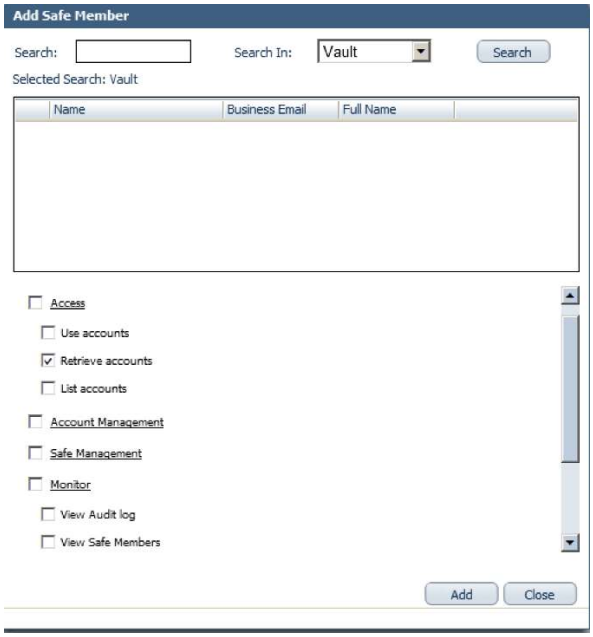
Add the Credential Provider and application users as members of the password Safes where the application passwords (accounts) are stored. This can be done manually in the **Safes** tab, or by specifying the Safe names in a CSV file for adding multiple applications.

1. Add the CP user as a Safe member with the following access:
   - **List accounts**
   - **Retrieve accounts**
   - **View Safe Members**

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



2. Add the application (the app ID) as a Safe member with the following access:
    - **Retrieve accounts**



3. If the Safe is configured for object-level access, make sure that both the CP user and the application have access to the passwords that need to be retrieved.

For more information about configuring Safe members, see the documentation for your PAM solution.

7. TRICENTIS TOSCA: INTEGRATION CONFIGURATION

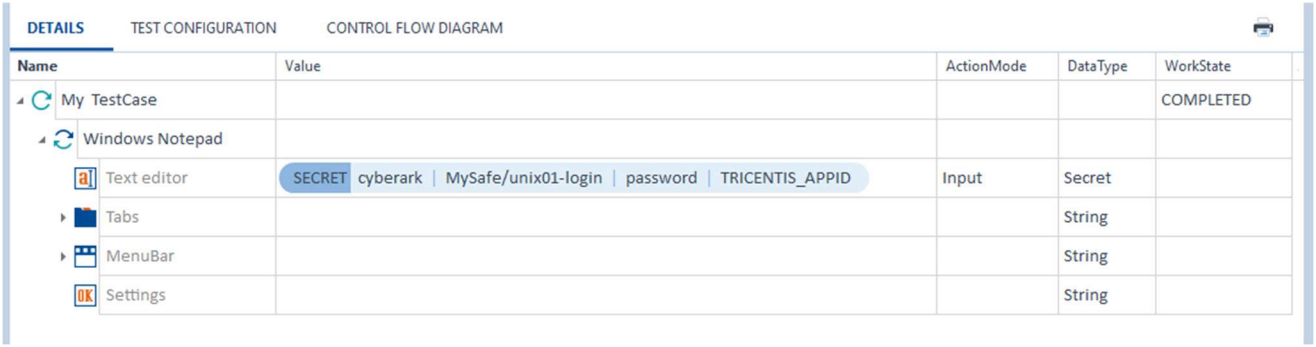
This section describes how to configure the integration between **Tricentis Tosca** and Credential Providers.

1. Prerequisite: Install **Tosca.** For installation instructions, see **https://documentation.tricentis.com/tosca/2410/en/content/installation_tosca/installation.htm**.
2. After successfully installing Tosca and CyberArk Credential Provider, you can create test steps using {SECRET} and {OTP} values.
    - If you installed CyberArk Credential Provider to the default installation location, no further configuration is needed.
    - If you did, you need to create a Test Case Parameter (TCP) called KeyVaultPath that contains the installation path of your CyberArk Credential Provider.

The syntax for the {SECRET} value is as follows:

{SECRET[cyberark][<Safe Name>/<Optional Folder Name>/<Secret Name>][<Secret Property>][<App ID to use]}

Example: {SECRET[cyberark][MySafe/unix01-login][password][TRICENTIS_APPID]}



The supported properties in the secret are password, username and address.

The OTP value uses an identical syntax. For usage in DEX Server and mobile engine, the secret syntax is identical, but not using the curly braces, e.g.:

SECRET[cyberark][MySafe/unix01-login][password][TRICENTIS_APPID].

8. PARTNER CONTACT INFO

Business Contact	Name	Pavlos Mitsias
	Email	p.mitsias@tricentis.com
	Tel	
Technical Contact	Name	Pavlos Mitsias
	Email	p.mitsias@tricentis.com
	Tel	
Support Contact	Name	Tricentis Support
	URL	https://support-hub.tricentis.com/open
	Tel	