



SECRETS MANAGER

(Agentless Central Credential Provider CCP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION TEMPLATE

DOCUMENT PURPOSE: THIS TEMPLATE IS TO BE COMPLETED BY PARTNER AND IS REQUIRED FOR CYBERARK SECURED CERTIFICATION. THE SECRETS MANAGER INTEGRATION TECHNICAL DOCUMENTATION WILL BE MADE AVAILABLE TO PARTNERS, CUSTOMERS AND PROSPECTS. **AS YOU COMPLETE EACH SECTION, PLEASE REMOVE THE DIRECTIONS PROVIDED.**

Name of Company: Venafi, Inc.

Website: <https://venafi.com>

Name of Product: Venafi TLS Protect Cloud

Version: N/A – SaaS

Date: 08/01/2023

PARTNER SOLUTION OVERVIEW

TLS Protect identifies and safeguards all of your TLS certificates and digital keys, delivering the observability, consistency, reliability and freedom of choice you need to protect your company from certificate-related outages and cybercrime in the data center, the cloud and everywhere in between.

Version: N/A - SaaS

Platform components:

- Venafi TLS Protect Cloud Account

KEY BENEFITS

Benefits of Venafi TLS Protect Cloud

- Discover and monitor all TLS keys and certificates (machine identities).
- Define and enforce security policies with ease.
- Reduce downtime with a fast, automated service that scales.

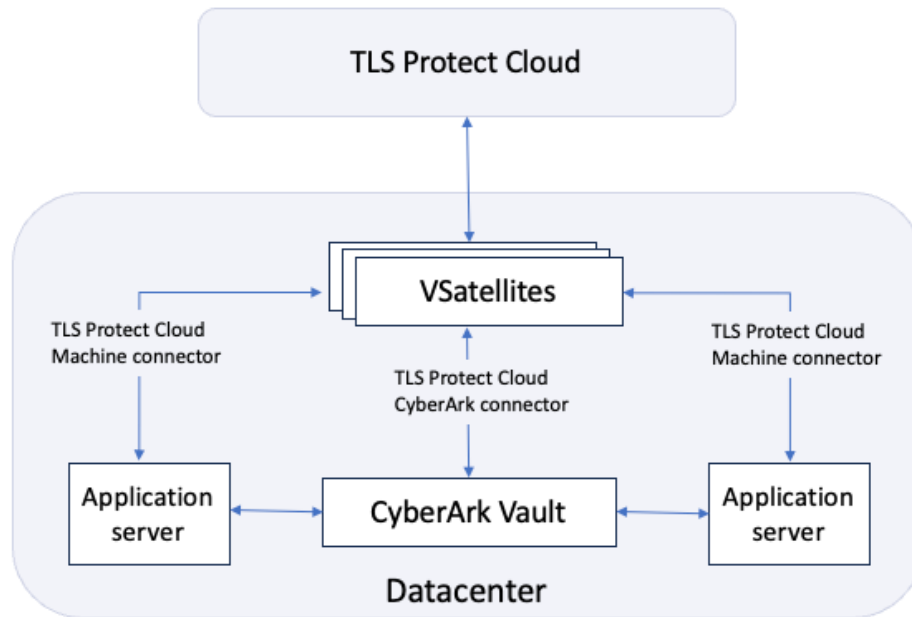
Benefits of integrating Venafi TLS Protect Cloud with CyberArk SECRETS MANAGER:

- Prevents the need to maintain credentials in multiple locations by ensuring they remain securely stored in the CyberArk Vault
- Enables end-to-end automation when provisioning machine identities to target applications without having to worry about manual credential rotation

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

This integration gives Venafi TLS Protect Cloud access to privileged system and application accounts held by CyberArk. This enables organizations to perform sensitive renewal, replacement and rekey operations without an administrator involvement or storing credentials outside of the enterprise vault.

The combined Venafi and CyberArk solution helps organizations strengthen their machine identity management operations by reducing time-consuming administrative tasks that can also increase the risk of exposing private keys to more people. The integration taps the large number of functional integrations, included in the Venafi Marketplace, to automate key and certificate operations. By harnessing the full power of Venafi platform automation, organizations can accelerate the speed of security operations, increase agility to respond to incidents like a CA compromise and reduce overall key and certificate lifetimes.



SECRETS MANAGER INTEGRATION

Rotating credentials that provide machines privileged access is a critical piece of maintaining robust security in your datacenter. The TLS Protect Cloud integration with CyberArk allows TLS Protect Cloud to access credentials stored in a CyberArk vault when performing functions like provisioning certificates to machines.

This allows you to take advantage of TLS Protect Cloud's certificate monitoring and provisioning services while continuing to manage your credentials in CyberArk.

CREDENTIAL RETRIEVAL

TLS Protect Cloud uses the [CyberArk Central Credential Provider](#) service to access credentials stored in CyberArk. Once the connection between CyberArk and TLS Protect Cloud is established, you can create credential references from TLS Protect Cloud to credentials stored in CyberArk.

Credential references can then be assigned to a machine in TLS Protect Cloud. When you want to provision a certificate to that machine, TLS Protect Cloud uses the CyberArk credential to access the machine.

Since TLS Protect Cloud creates a reference to the CyberArk credential, any update to the credential in CyberArk will be automatically used by TLS Protect Cloud when provisioning a certificate to a machine.

REQUIREMENTS

The connection between TLS Protect Cloud and your CyberArk service is established through a [Venafi VSatellite](#). VSatellite is a small piece of software installed on a Linux server in your data center that can access both TLS Protect Cloud and your CyberArk service, thereby becoming the bridge between the two services.

SECRETS MANAGER INSTALLATION

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

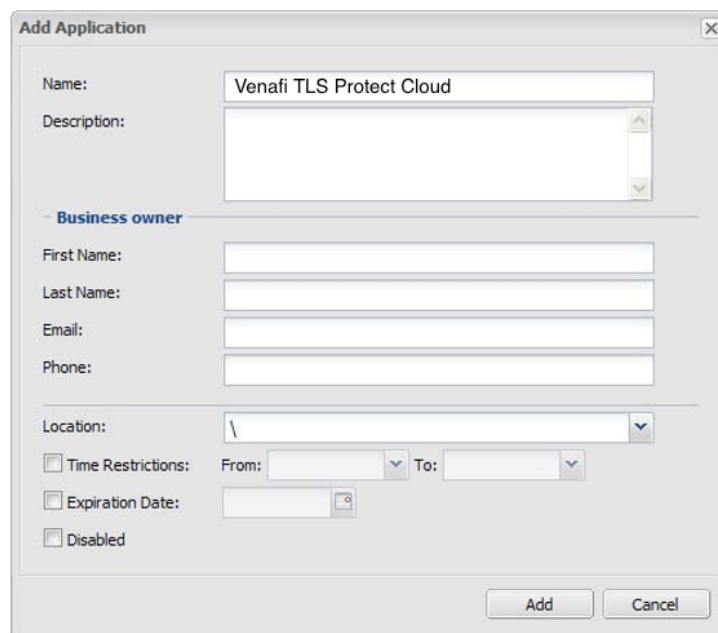
SECRETS MANAGER CONFIGURATION

The following sections provide details on TLS Protect Cloud configuration with CyberArk SECRETS MANAGER.

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

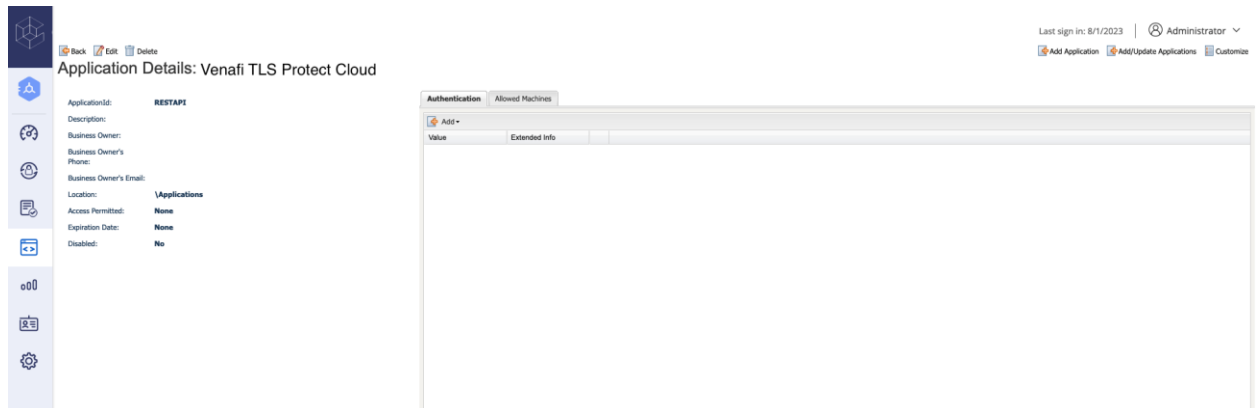
To define the application, define it manually through the CyberArk Password Vault Web Access (PVWA) interface:

- ☐ 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.

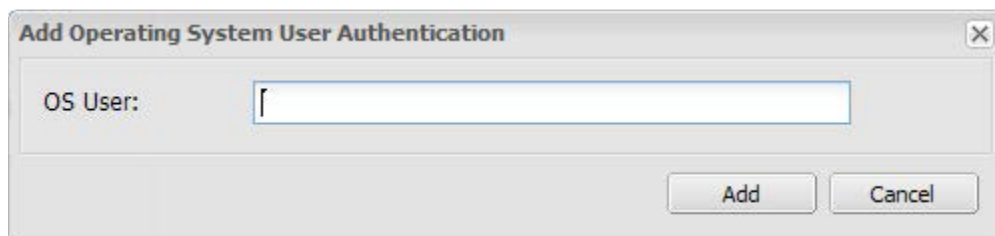


- ☐ Specify the following information:
 - In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: APP ID = Venafi TLS Protect Cloud
 - In the **Description** box, specify a short description of the application that will help you identify 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.

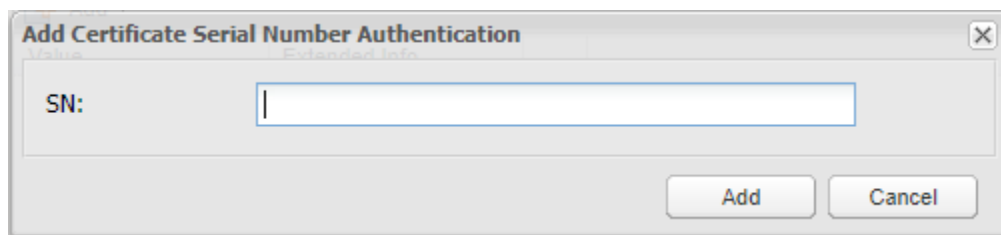
- ☐ Click **Add**. The application is added and is displayed in the Application Details page.



- ☐ 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.
 - Venafi recommends entering the IP addresses of each VSatellite to the "Allowed Machines" tab
- ☐ 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.



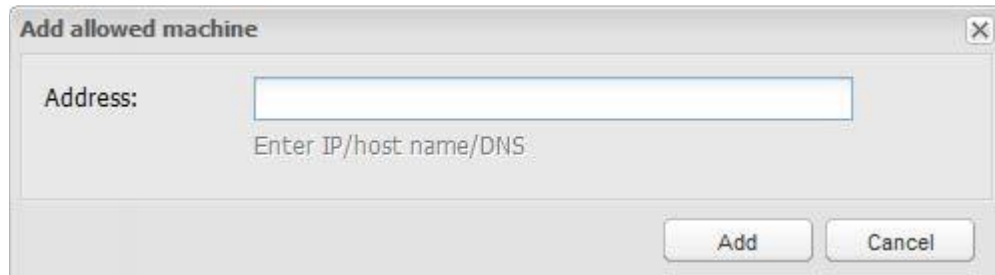
- ☐ Specify the name of the OS user who will run the application, then click **Add**. The OS user is listed in the Authentication tab.
- ☐ Specify the Certificate Serial Number.



- ☐ 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.

[1]
[SEP]

- In the Allowed Machines tab, click **Add**. The Add allowed machine window is displayed. [1]
[SEP]



- 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:

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

☐ 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.

PARTNER PRODUCT INSTALLATION & INTEGRATION CONFIGURATION

List specific steps to configuring Partner Product to work with SECRETS MANAGER, including:

- 9

- b. The VSatellites need to be able to access CyberArk in your datacenter. Before proceeding with the next step, make sure to have the IP addresses of the VSatellites readily available.
 - c. Follow Venafi online documentation to [deploy VSatellites](#).
- 2. Set up the CyberArk connection in TLS Protect Cloud
 - a. In TLS Protect Cloud, click Settings > Credentials Connectors.
 - b. Under CyberArk Configuration, complete the fields according to the following guidelines:

Field	Description
Central Credentials Provider Web Service URL	The URL to the CyberArk Central Credential Provider service
Application Name	The name of the application in CyberArk that this connector is allowed to connect to
Certificate Credential	(Optional) The certificate credential required to authenticate to the CyberArk service
Choose a VSatellite	The list of VSatellites that are allowed to connect to CyberArk – These VSatellites must be whitelisted on the CyberArk application

- c. Click Test Access. If your access is unsuccessful, check the [troubleshooting tips](#).
 - d. Click Save.
- 3. Import credentials from CyberArk
 - a. In TLS Protect Cloud, click Settings > Credentials.
 - b. Click New > CyberArk Credential. Complete the fields on the Add a new credential screen according to the following guidelines.

Field	Description
Name	The name for this credential to be displayed in TLS Protect Cloud
Owning Teams	One or more TLS Protect Cloud teams that have permission to use this credential – These same teams should be assigned to the machine you'll create in Step 4.
CyberArk Access Type	The type of credential that TLS Protect Cloud will receive from CyberArk – The type you select determines if TLS Protect Cloud will reference only the password, or both the username and password from an account in CyberArk.
Account Name	The name of the Account in CyberArk that contains the credential you want to import
Safe	The CyberArk safe
Folder	(Optional) The folder in CyberArk where the credential is located

- c. Click Save. The Credentials page opens with your new credential listed.

- d. You can now test the credential you just created. Click the vertical ellipses icon image of the vertical ellipses icon on the row of the new credential, and select Test Access.
 - e. If TLS Protect Cloud was unable to access the credential, see the [troubleshooting tips](#).
4. Assign the CyberArk credential on a TLS Protect Cloud machine

Partner Application UI:

Credential Connectors

CyberArk Configuration

^

Password Retrieval
Create credentials provider

Central Credentials Provider Web Services URL *

Application Name *

Certificate Credential


 Drag and drop or [browse](#)

Choose a VSatellite *

Test Access

PARTNER CONTACT INFO

Business Contact	Name	Jing Xie
	Email	jing.xie@venafi.com
	Tel	
Technical Contact	Name	Paul Cleary
	Email	paul.cleary@venafi.com
	Tel	
Support Contact	Name	Venafi Support
	Email	support@venafi.com
	Tel	+1.801.676.6900