



SECRETS MANAGER

TECHNICAL DOCUMENTATION

Transmit Security www.transmitsecurity.com

Name of Product FlexID

Version May 2,

2024

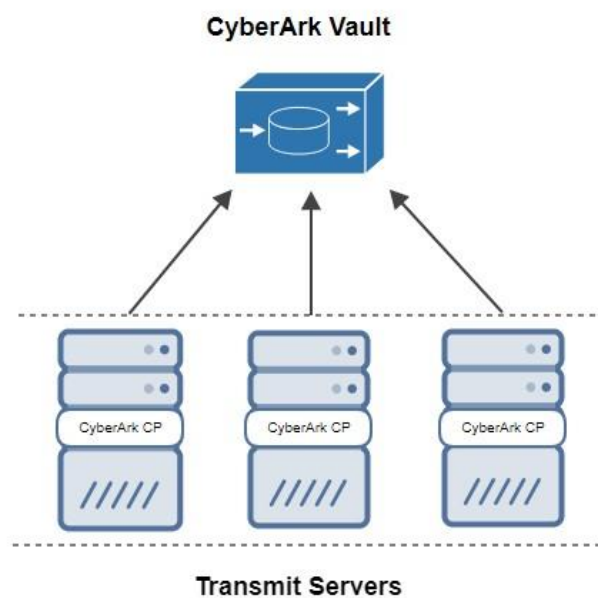
TRANSMIT SECURITY SOLUTION OVERVIEW

Transmit Security is a cross-channel orchestration platform provider that abstracts identity, authentication, authorization, and user-risk decisioning from applications, devices, security systems, infrastructure, and the cloud. An extensible plug-and-play approach reduces deployments to minutes for new and changes to existing business policies, authenticators, risk platforms, and channels. Transmit Security's Over-the-Air Journeys™ and third-party integration consolidates existing authentication and risk solutions into a single console that simplifies programming, reduces management costs, and is more agile to keep pace with new identity-related technologies. Advanced user, device and system profiling is combined with risk data to create a continuously updated user score for real-time authentication and access decisioning at every step, across every system. Learn more at transmitsecurity.com.

KEY BENEFITS

Transmit Security is a cross-channel orchestration platform provider that abstracts identity, authentication, authorization, and user-risk decisioning from applications, devices, security systems, infrastructure, and the cloud. An extensible plug-and-play approach reduces deployments to minutes for new and changes to existing business policies, authenticators, risk platforms, and channels. Transmit Security consolidates existing solutions into a single console that simplifies programming, reduces management, and is more agile to keep pace with new identity-related technologies. Advanced user, device and system profiling is combined with risk data to create a continuously updated user score for real-time authentication and access decisioning at every step, across every system.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



The Transmit Platform supports an agent integration with CyberArk. The CyberArk Credential Provider (including the Java Application Password SDK) is installed and configured on every machine that runs the Transmit authentication server. Transmit Servers are typically deployed as a cluster containing multiple servers.

Credentials are typically used within the Transmit Platform to authenticate against external systems — such as push notification providers, identity stores, and more. For example, credentials may represent

the provider account credentials or API tokens. Instead of storing credentials in the internal Transmit database, credentials may be stored within the CyberArk Password Vault and retrieved as needed, usually as part of an authentication flow.

SECRETS MANAGER INSTALLATION

Refer to the “Credential Provider and ASCP Implementation Guide” or the “Central Credential Provider Implementation guide” for CyberArk Agent based or Agentless installation and configuration.

The following describes how to configure the Secrets Manager Provider with the Transmit Platform.

INSTALLING THE CYBERARK VAULT CREDENTIALS PROVIDER

The *Transmit Platform* provides the option to integrate with a *CyberArk Vault* via a *CyberArk Vault Credentials Provider Local Agent* (version 10.7), to retrieve and cache credentials from the vault in a secure manner.

CyberArk Vault is a third-party paid service. A license must be purchased from CyberArk directly.

This integration assumes that an instance of a *CyberArk Vault* is already installed and accessible.

To install the *CyberArk Vault Credentials Provider Local Agent*, follow the steps below, **for each server node** in the cluster:

1. [Install the CyberArk Vault Credentials Provider](#)
2. [Add the CyberArk Java SDK to the Transmit Server Runtime](#)

Step 1 - Install the CyberArk Vault Credentials Provider

1. Download the relevant *CyberArk Vault Credentials Provider* installation RPM / DEB files onto the *Transmit Server*.
2. Configure the *CyberArk Credentials Provider* according to the *CyberArk Installation Guide*. (This includes for example: configuring the host and port of the Vault in the vault.ini, creating the *credential file* and the *basic_appprovider.conf* file, etc.)
3. Run the *CyberArk Credentials Provider* installation RPM / DEB files. This will install the *CyberArk Vault Credentials Provider Local Agent* and Java SDK.

Step 2 - Add the CyberArk Java SDK to the Transmit Server Runtime Classpath

1. It is recommended to create a symbolic link to the `/opt/CARkaim/sdk/javapasswordsdk.jar` *Java SDK file* on each server.

Command Structure:

```
ln -s [path of the file to be linked] [path of the symbolic link]
```

For example, this command creates a symbolic link on a *Transmit* server:

```
ln -s /opt/CARkaim/sdk/javapasswordsdk.jar /opt/auth-control[standalone|admin]/libs/cyberarksdk.jar
```

2. Add the *CyberArk Java SDK* file to the `TS_CLASSPATH` as follows

- a) Edit the `/bin/start.env` file.
- b) Add the *CyberArk Java SDK* file name and *full path* to the *soft link* (separated by colon ":") to the `TS_CLASSPATH` as shown in this example:

Example

```
TS_CLASSPATH=<some-other-JAR-files>:/opt/auth-control[standalone|admin]/libs/cyberarksdk.jar
```

Note: If you are installing on an *auth-control* server then make sure to repeat the steps on the *auth-control-admin* server as well.

- c) Save the `start.env` file.
- d) Restart all the *Transmit* servers that were updated.

Note: After the re-start, check that there are no *exceptions* in the logs when loading the *CyberArk SDK*.

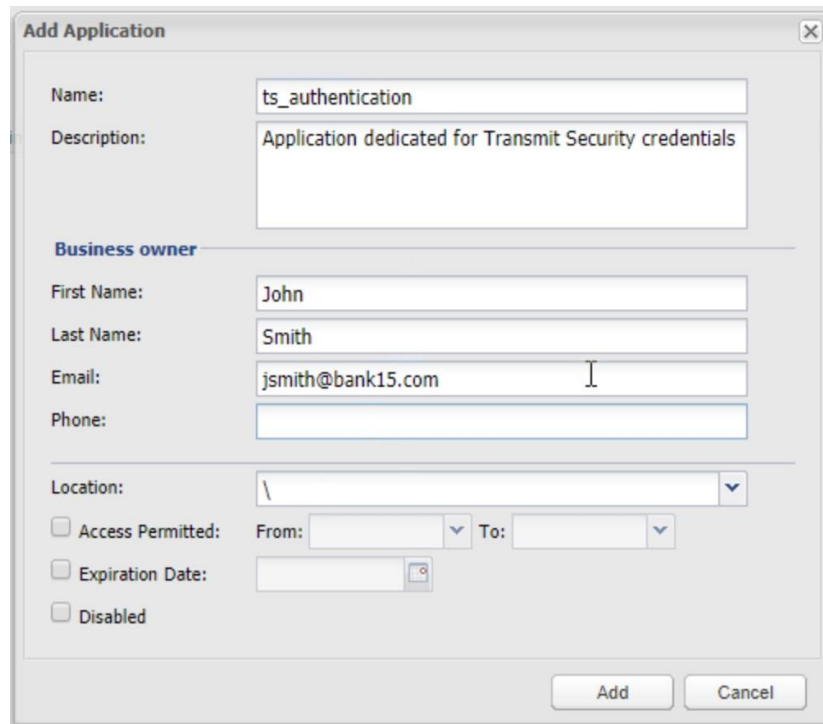
Note: After completing the installation, an option to use the *CyberArk Secure Vault* should be available in the *Keys and Credentials* section of the *Administration Console*.

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.



Add Application

Name:

Description:

Business owner

First Name:

Last Name:

Email:

Phone:

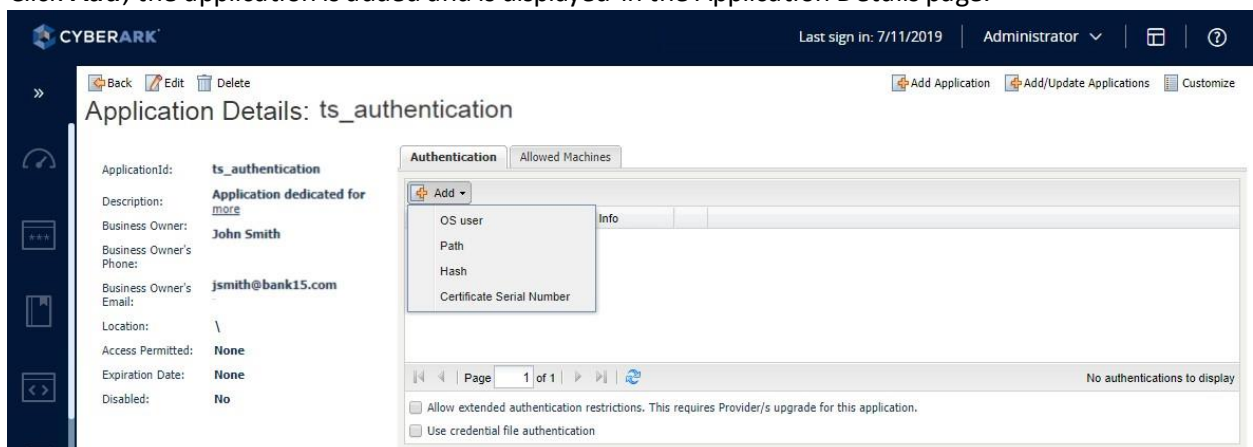
Location:

☐ Access Permitted: From: To:

☐ Expiration Date:

☐ Disabled

2. Specify the following information:
 - In the Name edit box, specify the unique name (ID) of the application. Our solution does not limit this to any particular value.
 - 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.



CYBERARK Last sign in: 7/11/2019 Administrator

Back Edit Delete Add Application Add/Update Applications Customize

Application Details: ts_authentication

ApplicationId: **ts_authentication**

Description: **Application dedicated for** [more](#)

Business Owner: **John Smith**

Business Owner's Phone: **jsmith@bank15.com**

Business Owner's Email: **jsmith@bank15.com**

Location: **\"**

Access Permitted: **None**

Expiration Date: **None**

Disabled: **No**

Authentication Allowed Machines

- OS user
- Path
- Hash
- Certificate Serial Number

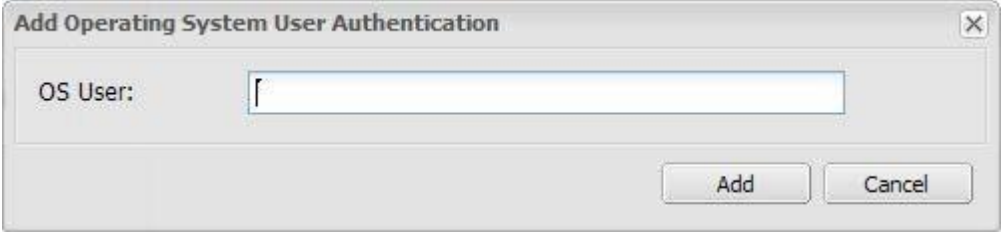
Page 1 of 1 No authentications to display

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

☐ Use credential file authentication

- **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.

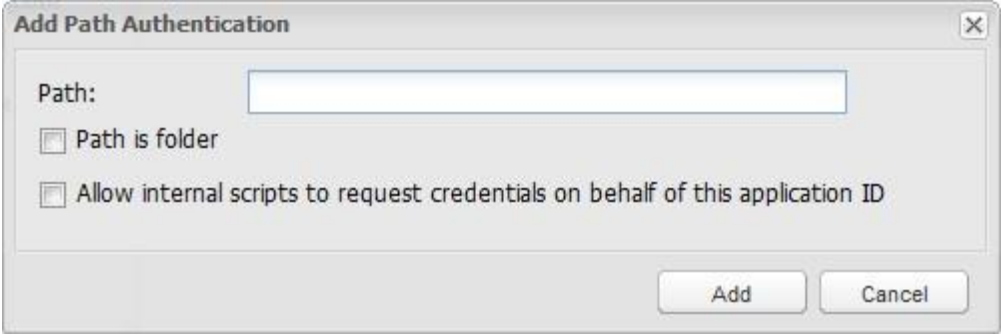
5. Specify the OS user:
 - a. Select **OS user**; the Add Operating System User Authentication window appears.



The dialog box titled "Add Operating System User Authentication" contains a text field labeled "OS User:" and two buttons at the bottom right: "Add" and "Cancel".

- b. Specify the name of the OS user who will run the application, then click **Add**; the OS user is listed in the Authentication tab.

6. Specify the application path:
 - a. Select **Path**; the Add Path Authentication window appears.



The dialog box titled "Add Path Authentication" contains a text field labeled "Path:", two checkboxes labeled "Path is folder" and "Allow internal scripts to request credentials on behalf of this application ID", and two buttons at the bottom right: "Add" and "Cancel".

- b. Specify the path where the application will run.
 - c. To indicate that the specified path is a folder, select **Path is folder**.
 - d. To allow internal scripts to retrieve the application password for this application, select **Allow internal scripts to request credentials on behalf of this application ID**.
 - e. Click **Add**; the Path is added as an authentication characteristic with the information that you specified.
7. Specify a hash:
 - a. Run the AIMGetAppInfo utility to calculate the application's unique hash.
 - b. Copy the hash value that is returned by the utility.
 - c. In the PVWA, select **Hash**; the Add Hash window appears.

The dialog box is titled "Add Hash Authentication" and has a close button (X) in the top right corner. It contains a label "Hash:" followed by a text input field. At the bottom right, there are two buttons: "Add" and "Cancel".

d. In the Hash edit box, paste the application's unique hash value, or specify multiple hash values with a semi-colon. You can add additional information in a comment after each hash value specified for an application by specifying '#' after the hash value, followed by the comment. For example, OE883B7OD5B6E3EE37D37198049C9507C8383DB6 #app2 **Note:** The comment must not include a colon or a semicolon.

e. Click **Add**; the Hash is added as an authentication characteristic with the information that you specified.

8. 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:

The dialog box is titled "Add Certificate Serial Number Authentication" and has a close button (X) in the top right corner. It contains a label "SN:" followed by a text input field. At the bottom right, there are two buttons: "Add" and "Cancel".

9. Specify the application's **Allowed Machines**. This information enables the Credential Provider to make sure that only applications that run from specified machines can access their passwords. [SEP]

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

The dialog box is titled "Add allowed machine" and has a close button (X) in the top right corner. 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".

- 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 (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 either be done 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:

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

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

- iii. If your 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.
- 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.

10

TRANSMIT SECURITY INSTALLATION & INTEGRATION CONFIGURATION

Refer to the **Transmit Platform Administration Guide** for Transmit Security installation.

From the Transmit Administration Console, use the following steps to specify the details required to retrieve the credentials from the CyberArk Password Vault:

1. From **Keys and Credentials**, click the **Credentials** tab and then click **+ Add Credentials**.
2. Enter the credentials alias and version.

Credentials Alias *	
	This alias is used to identify this credentials across the system. Each alias may have multiple versions.
Credentials Version *	
	Version identifier. The latest version is selected when using a credentials alias.

Field	Description
Alias*	<i>Name</i> used to reference the credentials throughout the platform. Enter the name for new credentials or enter the name of an existing credential to add a new version for it.
Version*	ID of the newly created version.

3. For **Credentials Source**, select **CyberArk Secure Vault**.

Credentials Source	CyberArk Secure Vault
--------------------	--

4. Enter the relevant details described below, then click **Save**.

CyberArk Credentials

Add a remote credentials from CyberArk Credentials Vault

Application ID *

Application id that is defined in CyberArk Vault with appropriate permissions

Safe Name *

Name of the safe within CyberArk Vault where the required credentials exists

Folder

Name of the folder within the safe where the credentials resides. default is 'root'

Account ID *

The credentials unique identifier within the safe

Field	Description
Application ID*	Application ID defined in the CyberArk Password Vault with the appropriate permissions.
Safe Name*	Name of the safe within the CyberArk Password Vault that contains the credentials.
Folder	Name of the folder within the CyberArk safe that contains the credentials. Default is <i>root</i>
Account ID*	ID of the account that contains the credentials. It uniquely identifies the credentials within the CyberArk safe and is used as the credentials ID in the Transmit Platform (e.g., username).

TRANSMIT SECURITY CONTACT INFO

Business Contact	Name	Ravit Aviv
	Email	ravit@transmitsecurity.com
	Tel	+972-79-3003327
Technical Contact	Name	
	Email	
	Tel	
Support Contact	Name	
	Email	
	Tel	

