

Adenza



SECRETS MANAGER INTEGRATION

(Agentless Central Credential Provider CCP)

Name of Company: Adenza

Website: <https://adenza.com/>

Name of Product: ControllerView

Version: 10.14.2

Date: 30-Aug-2023

PARTNER SOLUTION OVERVIEW

Adenza ControllerView is a data-driven enterprise platform used primarily for regulatory reporting that ingests native data from disparate sources to seamlessly and transparently deliver workflow automation and controls, perform validation and calculation, and offer unique dynamic data lineage and audit trail capabilities.

Version: 10.14.2

Platform components:

- The ControllerView Server
- The web application deployed on a web server (Apache Tomcat, for example)

KEY BENEFITS

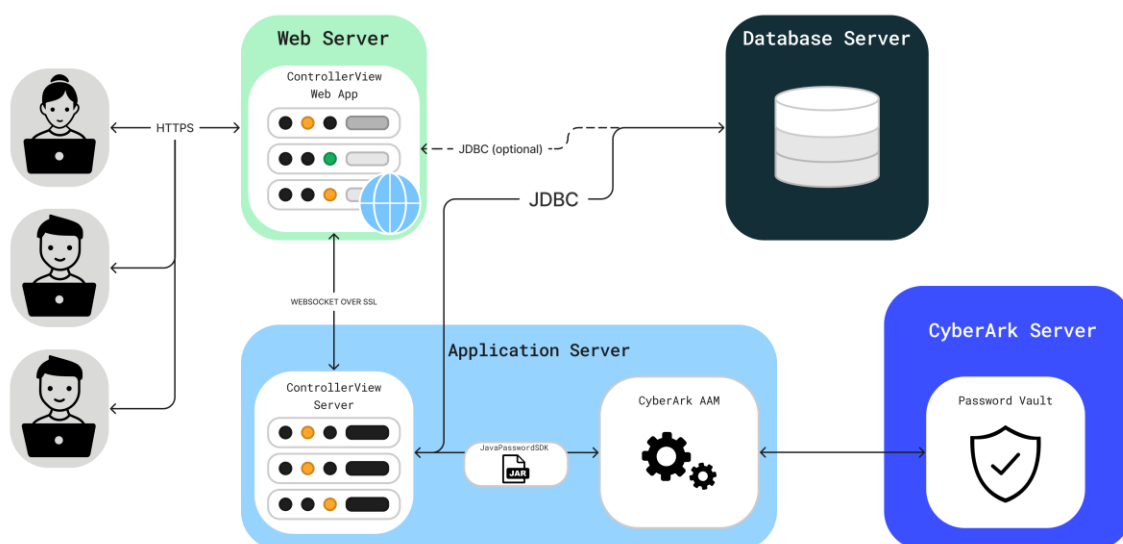
Benefits of Adenza ControllerView:

- Efficiency: automating regulatory reporting processes, which can save time and resources.
- Customization: providing bespoke risk calculation and allowing the development of customized regulatory-reporting solutions.
- Scalability: delivering a scalable solution to address regulatory reporting needs.
- Ease of use: available training courses for the Platform users.

Benefits of integrating the ControllerView with CyberArk SECRETS MANAGER:

- Enhanced Security: credentials are stored in a secure vault.
- Credentials Rotation and Management: SECRETS MANAGER eliminates the need to manage passwords in the ControllerView.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



Note that for simplicity, the diagram shows the minimal working configuration and does not include load balancers or additional Execution Nodes as their presence does not change the integration process with CyberArk SECRETS MANAGER.

SECRETS MANAGER INTEGRATION

The ControllerView communicates with the SECRETS MANAGER installed on the same server where the ControllerView resides using the JavaPasswordSDK.jar which has to be copied to the “server-bin\lib” directory of the installed ControllerView server.

CREDENTIAL RETRIEVAL

Credentials stored in the CyberArk vault are retrieved on demand.
In most cases this happens when establishing a new database connection which requires a username and a password.

REQUIREMENTS

The web server where the ControllerView web application is deployed has the following requirements:

- RAM: 2GB baseline plus at least 400MB per simultaneous user;
- CPU: 2 core minimum total + 0,16 CPU per concurrent user

The application server requires a 64-bit Linux or Windows OS (incl. VM) installed with at least 4 CPU cores, 16GB RAM, 60GB HDD.

Task JVMs spawned on the application server by default are recommended to have 3Gb of RAM or more.

The minimum database server requirements are 4 CPU Cores, 8GB RAM, and 100GB HDD.

Network connection requirements include 1 Mbyte/sec of minimal required bandwidth per user, latency of less than 150 ms, and zero (0%) packet loss.

Client machines must have Google Chrome or Microsoft Edge installed and a screen resolution of 1366x768 or higher.

We recommend that you refer to the up-to-date version of the *V10_Hardware_Software_Requirements.pdf* document to get the most current information.

SECRETS MANAGER INSTALLATION

Refer to [CyberArk Agentless installation and configuration](#).

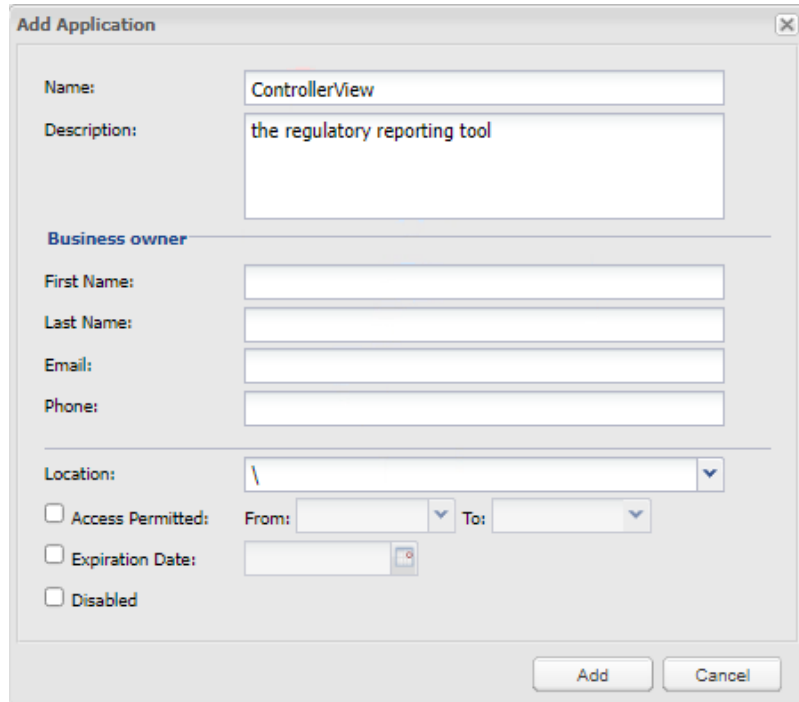
SECRETS MANAGER CONFIGURATION

The following sections provide details on the ControllerView configuration with CyberArk SECRETS MANAGER.

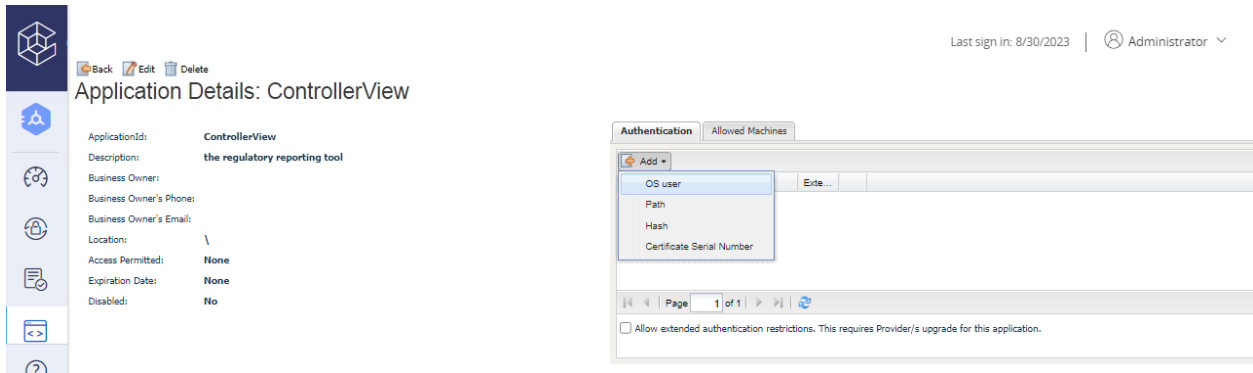
DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

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 = ControllerView
 - 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.

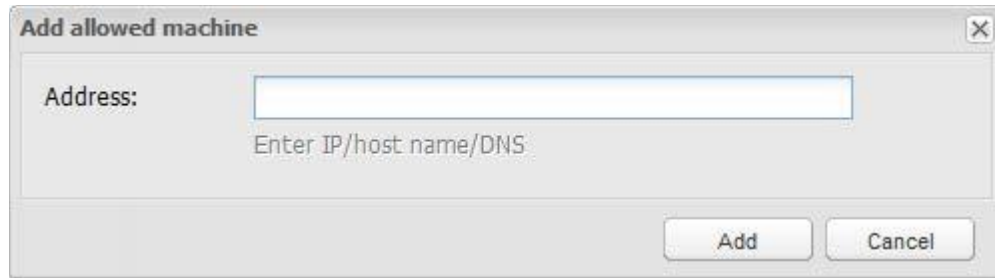


- ☐ Check the **Allowing extended authentication restrictions** box. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.
- ☐ Specify the application's **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password.
- ☐ 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 Hash Authentication.

This field must contain the calculated hash of the core-common-{version}.jar file located in the "server-bin\lib\axiom" directory of the installed ControllerView server.

- ☐ 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.

A screenshot of a Windows-style dialog box titled "Add allowed machine" with a close button (X) in the top right corner. The dialog contains a label "Address:" followed by a text input field. Below the input field is a hint text "Enter IP/host name/DNS". At the bottom right of the dialog are two buttons: "Add" and "Cancel".

Add allowed machine

Address:

Enter IP/host name/DNS

Add 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:

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

1 “2.6.7 Installing CyberArk” and “4.2 Generating a System DB Source Credentials” in
v10_Installation.pdf

9

In brief, the sequence of steps required for the successful integration includes:

- 1 Installing the CyberArk SECRETS MANAGER on the machine where the ControllerView server runs
- 2 Copying the JavaPasswordSDK.jar located in "C:\Program Files\CyberArk\ApplicationPasswordSdk" to "C:\axiom\v10_server\server-bin\lib" (the actual location of the directories may be different)
- 3 Creating a new Application in the CyberArk Privileged Access Manager
- 4 Generating a new System DB Source Credential file following the instructions in the v10_Installation.pdf document if storing passwords in the server file system is not advisable
- 5 Changing the Storage Type to the CyberArk in the ControllerView (for a DB Source, for example) and filling in necessary fields

The image shows a configuration window titled "Credentials for Elevated Access" with a sub-header "Username/Password: CyberArk: Object: postgres". A modal dialog is open in the foreground with the following fields:

- Credential Type:** User Name/Password (dropdown)
- Storage Type:** CyberArk (dropdown)
- AppID:** ControllerView
- Safe:** controllerview-safe
- Folder:** Root
- Object:** postgres
- Reason:** (empty text area)

At the bottom of the dialog are two buttons: "UPDATE" and "CANCEL".

Since the installation and initial configuration of the ControllerView itself is a rather complex process, it

is recommended to refer to the documentation package and service consultants for the latest information.

PARTNER CONTACT INFO

Business Contact	Name	David Attenborough
	Email	communications@adenza.com
Technical Contact	Name	Fedor Ivanov
	Email	core.po@adenza.com
Support Contact	Website	https://adenza.force.com