



CYBERARK SECRETS MANAGER

(Agentless Central Credential Provider CCP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Axonius

Website: www.axonius.com

Name of Product: Axonius

Version: 1.0

Date: Revised 28 October 2020

AXONIUS OVERVIEW

Axonius is a [cybersecurity asset management platform](#) that gives organizations a comprehensive asset inventory, uncovers security solution coverage gaps, and automatically validates and enforces security policies. By seamlessly integrating with [nearly 200 security and management solutions](#), Axonius is deployed in minutes, improving cyber hygiene immediately.

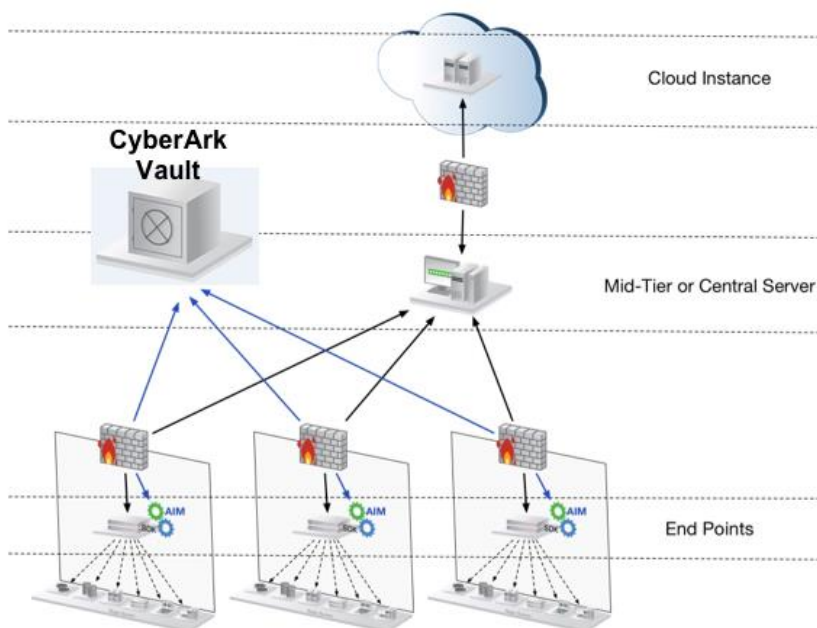
Axonius was named the Most Innovative Startup of 2019 at the prestigious RSAC Innovation Sandbox and was named Rookie Security Company of the Year by SC Magazine in 2019. For more information, please visit Axonius.com.

Version: 1.0

KEY BENEFITS

The integration between Axonius and CyberArk enables Axonius to securely pull privileged credentials from the CyberArk Vault using CyberArk's Secrets Manager. This eliminates the need for Axonius to store or embed these credentials within their solution and the need for the client to rotate these credentials within Axonius. The integration helps ensure that privileged credentials are secured in the Vault, rotated to meet company guidelines and meet complexity requirements.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



SECRETS MANAGER INTEGRATION

Axonius uses the Agentless Secrets Manager method (called Central Credential Provider (CCP)) to integrate with CyberArk. The Agentless Secrets Manager method allows an application (in this case, Axonius) to use a REST API to securely retrieve the credentials from the Vault.

A client certificate is required as it provides protection for the credential while in transit from the agent to the application. The credential is encrypted while in transit from the vault to the Secrets Manager shared agent. The application is authenticated by the client certificate serial number and machine address.

CREDENTIAL RETRIEVAL

In order to securely retrieve credentials from the Vault, the authorized application only requires an Application ID and a Query. The Application ID identifies an application to the CyberArk Vault. It needs to be granted sufficient privileges to retrieve all the credentials it needs.

Axonius uses the Agentless Secrets Manager method (called Central Credential Provider (CCP)) to fetch credentials from CyberArk Vault. Axonius uses the REST API when:

- Creating a new adapter connection
- Updating an existing adapter connection
- During a discovery cycle, to fetch asset information from the various adapters

Axonius does not store the credentials anywhere and deletes any trace of the credential.

SECRETS MANAGER INSTALLATION

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

Axonius uses the Agentless Secrets Manager method (called Central Credential Provider (CCP)) to integrate with CyberArk.

Notes:

- In the below section, the term “Application” refers, in this case, to Axonius.
- No specific steps are required to configure Central Credential Provider (CCP) with Axonius.

SECRETS MANAGER CONFIGURATION

The following sections provide details on Axonius 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.

Add Application

Name:

Description:

Business owner

First Name:

Last Name:

Email:

Phone:

Location:

☐ Access Permitted: From: To:

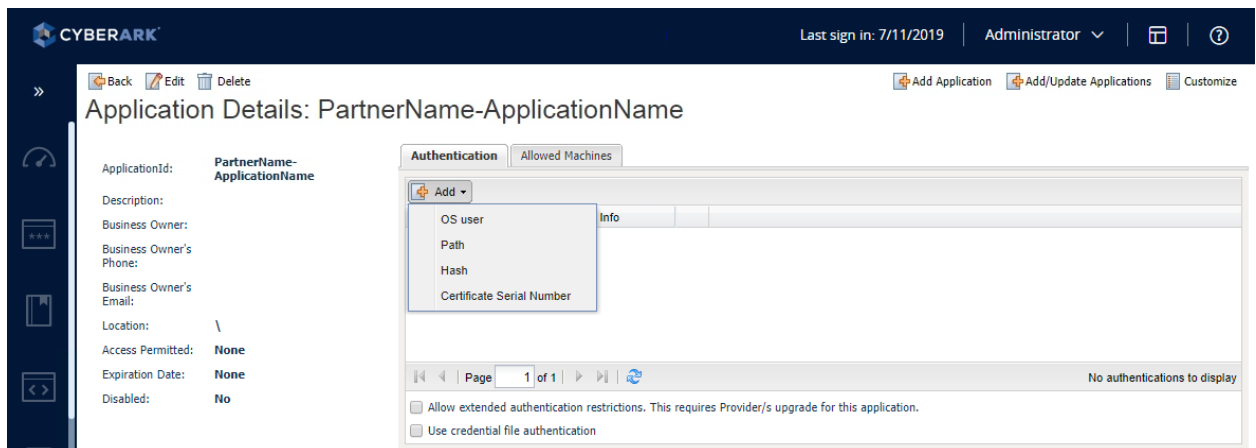
☐ Expiration Date:

☐ Disabled

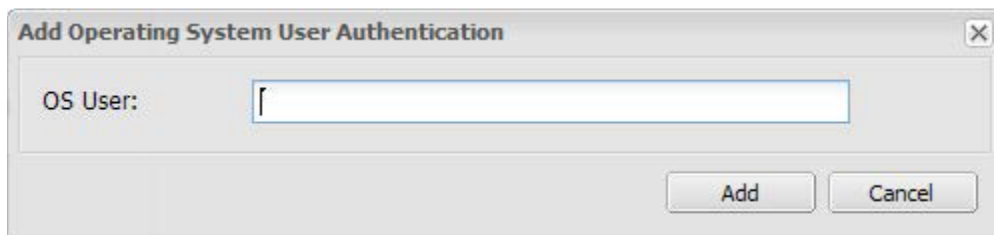
☐ Specify the following information:

- In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: Axionus
- 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.

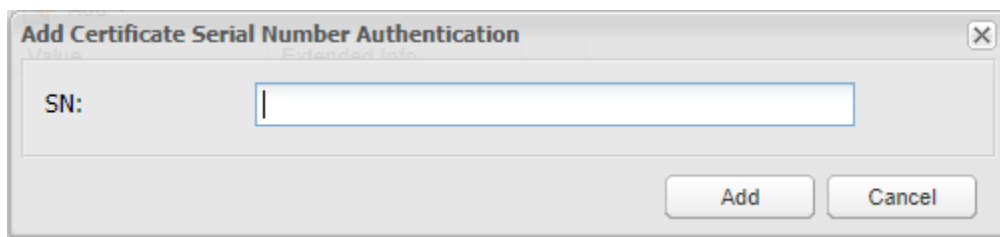
☐ Click **Add**. The application is added and is displayed in the Application Details page.



- ☐ 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 Certificate Serial Number.



Instructions on how to get the Certificate Serial Number:

Windows:

Start -> certmgr.msc (Current User) -> expand Personal -> select Certificates -> double-click on

certificate to open

Start -> certlm.msc (Local Computer) -> expand Personal -> select Certificates -> double-click on certificate to open

If the first two options do not work in your env:

Start -> mmc.msc -> File; Add/Remove Snap-in -> Certificates -> Add -> OK -> you may be prompted to choose Local Computer or Current User -> OK

Expand Certificates -> Personal -> Certificates -> Double-Click on a certificate to open.

Once the certificate is open -> Details tab -> Serial Number is in the list of values shown

Once the certificate is open

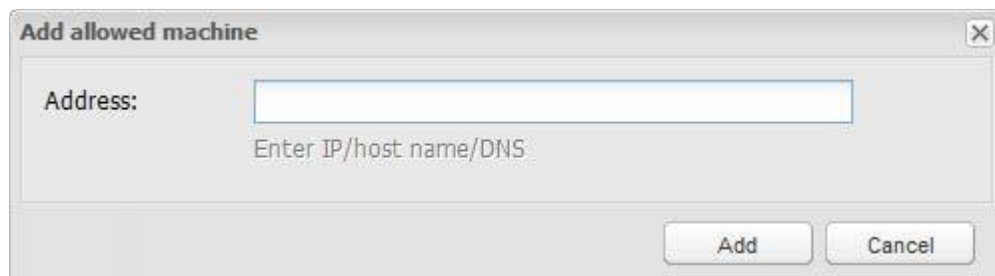
OpenSSL

openssl x509 -in <cert file name> -serial -noout

- This is the most secure way to authenticate the application for CCP
- The following are enhanced ways of authenticating

- ☐ 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.



- 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

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

- ☐ 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**.

AXONIUS INSTALLATION & INTEGRATION CONFIGURATION

Refer to [Axonius documentation](#) for Axonius installation and configuration.

Axonius uses the Agentless Secrets Manager method (called Central Credential Provider (CCP)) to fetch credentials from CyberArk Vault. Axonius uses the REST API when:

- Creating a new adapter connection
- Updating an existing adapter connection

- During a discovery cycle, to fetch asset information from the various adapters

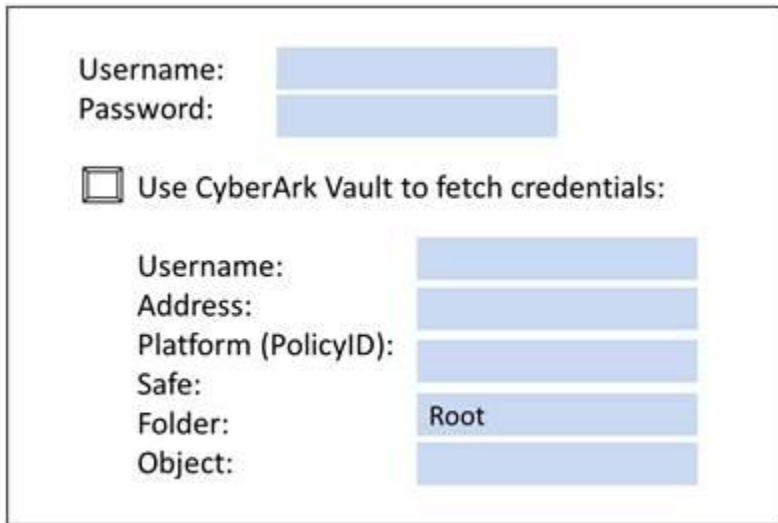
Axonius does not store the credentials anywhere and deletes any trace of the credential.

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

1. Any special configurations within or outside the product
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

>>Replace this screenshot with your actual integration configuration screenshots:

Partner Application UI:



The screenshot shows a configuration form with the following fields:

- Username:** [Text input field]
- Password:** [Text input field]
- ☐ **Use CyberArk Vault to fetch credentials:**
- Username:** [Text input field]
- Address:** [Text input field]
- Platform (PolicyID):** [Text input field]
- Safe:** [Text input field]
- Folder:** [Text input field with "Root" pre-filled]
- Object:** [Text input field]

>>Replace this with your actual configuration options.

Common use cases:

1. Windows domain credentials or other standard credentials
 - a. The user will specify: username, address, platform
 - b. Safe name – optional but recommended for increasing performance
2. Local accounts (windows/Unix)
 - a. The user will specify: username & platform
 - b. Safe name – optional but recommended for increasing performance
 - c. When scanning, need to request in the API these username and platform, and add the address of the current machine being scanned
3. Non-standard credentials (can't be unique with username+address+Platform)
 - a. The user will specify: Safe and object name (folder is usually root by default)

ENABLING CYBERARK

To enable CyberArk integration:

1. Open the **Global Settings**. From the top right corner of any screen, click . The System Settings screen opens. Then click the **Global Settings** tab.
2. Under **CyberArk Settings**, check the **Use CyberArk** checkbox to enable fetching credentials from CyberArk Vault.
3. Once enabled, specify:
 - a. **CyberArk Domain** – The base URL of the Central Credential Provider (CCP).
 - b. **Port** – The port the Central Credential Provider (CCP) is listening to.
 - c. **Application ID** – The Application ID which identifies the Axonius application created in CyberArk.
 - d. **Certificate Key** – The certificate which will be authenticated against the Certificate Serial Number defined on the Application.

CyberArk Setting

Use CyberArk



CyberArk Domain

Port

Application ID

Certificate Key

No file chosen

Choose file

ADAPTER CONFIGURATION

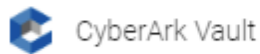
Once CyberArk integration is enabled in Axonius, while configuring adapters, a new CyberArk icon will appear in all password fields, allowing you to enter a password manually or to fetch the password from CyberArk Vault.

AWS Access Key Secret optional



To fetch the password from CyberArk Vault:

1. In a password field, click the CyberArk icon. A CyberArk popup opens.



Query:

Cancel

Fetch

2. In the popup, specify a query. This query represents a location of the Password Object within a Safe in a Vault (e.g. Safe=Test;Folder=root\OS\Windows;Object=windows1).
3. Click Fetch.
 - a. If the fetch is successful, a green indication will be displayed. Hovering over the CyberArk icon will show the Query defined.

AWS Access Key Secret optional

- b. If the fetch is unsuccessful, a red indication will be displayed. Hovering over the CyberArk icon will show the error.

AWS Access Key Secret optional

Note: Typing or deleting any character in the textbox will change the password field back to a manual password input.

PARTNER CONTACT INFO

Business Contact	Name	
	Email	
	Tel	
Technical Contact	Name	
	Email	
	Tel	
Support Contact	Name	
	Email	
	Tel	