



CYBERARK SECRETS MANAGER

(Agentless Central Credential Provider CCP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Aqua Security

Website: www.aquasec.com

Name of Product: Aqua Container Security Platform

Version: 2.5

Date: 19 September 2018 (Revised 15 October 2020)

AQUA SECURITY OVERVIEW

Aqua Security enables enterprises to secure their virtual container environments from development to production, accelerating container adoption and bridging the gap between DevOps and IT security.

Aqua has built a native, architected-for-containers platform for securing containerized applications. It combines a central management and policy engine with host-based enforcers (which are in themselves containers) to power a scalable, easy-to-deploy solution that provides full visibility into container activity and policy enforcement capabilities.

Version: 2.5

KEY BENEFITS

The Aqua Platform was created to tackle the complex challenge of securing containerized applications, while adhering to a set of principles that ensures the effectiveness and usability of the solution.

Full Container Lifecycle Security

Most DevOps and security professionals would agree that it is important to secure containers and easier to secure them as early as possible in their lifecycle. At Aqua we enable this “shift left” methodology, but also view container security as a continuous process. This process starts with image development and CI, followed by deployment and orchestration. It continues even in production, with ongoing monitoring and improvements. Focusing only on the development process is insufficient, and focusing on runtime without understanding the container payload is ineffective. Resolving these two issues with one seamless platform is what ensures effective security while minimizing false positives.

Automation

One reason to choose automation is that manual processes are prone to human error. But in the context of containers, it is the scale and frequency of updates that make automation not only better, but indispensable.

If every change in a container image or its deployment required manual adjustment, security would become untenable. Aqua’s container build-ship-run cycle is typically highly automated, so it is possible to integrate security into it with very little overhead.

Smart Defaults

While everyone wants flexibility and control, Aqua's experience in enterprise security solutions has taught us that customers keep many default settings and features provided by vendors because they cannot be bothered with tweaking them. However, these defaults may have been selected for convenience, rather than security.

Therefore, it is critical to have smart defaults that most customers would find suitable for their requirements. This allows the customer to benefit from enhanced security from day one of using the Aqua Platform. For example, default security profiles for the most popular open-source container images would typically be sufficient for most workloads and would only need to be tweaked for specific use-cases.

Layered Security Model

Providing layers of security is one of the key principles of any security policy – it helps avoid single points of failure and creates defense in depth via fallback solutions, in case one of the layers fails to fulfill its purpose.

We also want to layer passive measures, such as hardening and access control mechanisms, with active measures that monitor for anomalous behavior and generate alerts or preventive action.

Cyber Intelligence

The threat landscape for containers constantly changes, as it does everywhere else in cyber security. But additionally, since containers are a new and evolving technology, there are significant new features and updates with every release that repeatedly change the attack surface.

To keep up with those changes, the Aqua Platform has cyber intelligence updates fed into it daily. Aqua's research team provides threat intelligence based on a variety of open sources, commercial sources, and in-house research.

Actionable Insights

Many security solutions can point out vulnerabilities or create alerts about suspicious behavior, but stop short of providing preventive measures or processes that lead to remediation. It is our objective to make insights actionable, whether automatically as part of the security policy, or by supporting user-driven processes that drive to resolution.

Security at Scale

Some of the largest scale applications in the world run on containers. Containers are used for highly variable workloads that can go from zero to thousands of hosts in minutes, then go back down to zero just as quickly. Security must, therefore, scale to such usage patterns both technically as well as from a usability standpoint.

The Aqua Security CyberArk Integration

In many environments, there is a need to pass sensitive information like passwords, connection strings, or tokens into a container. A sensitive piece of information is called a "secret" and Aqua provides central management and secure distribution of these secrets into running containers. Aqua's integration with CyberArk Enterprise Password Vault ensures that these secrets can be safely distributed through Aqua's control system via containers.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

Aqua CSP can be integrated with CyberArk Secrets Manager.



SECRETS MANAGER INTEGRATION

Aqua integrates with CyberArk Enterprise Password Vault to enable the use of secrets that are already defined in the secret store. The integration allows for distribution of their values to containers through Aqua's access control system.

Aqua users can define access control policies that authorize users or groups to run containers that make use of the secret.

When a secret is used, its value will be automatically injected into the container, either as an environment variable or file. The value of the secret is visible outside the container, is not stored on disk, and is encrypted in transit.

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 Aqua CSP 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: Aquasec

Description: ApplicationID assigned to Aquasec Security

Business owner

First Name:

Last Name:

Email:

Phone:

Location: \

☐ Access Permitted: From: To:

☐ Expiration Date:

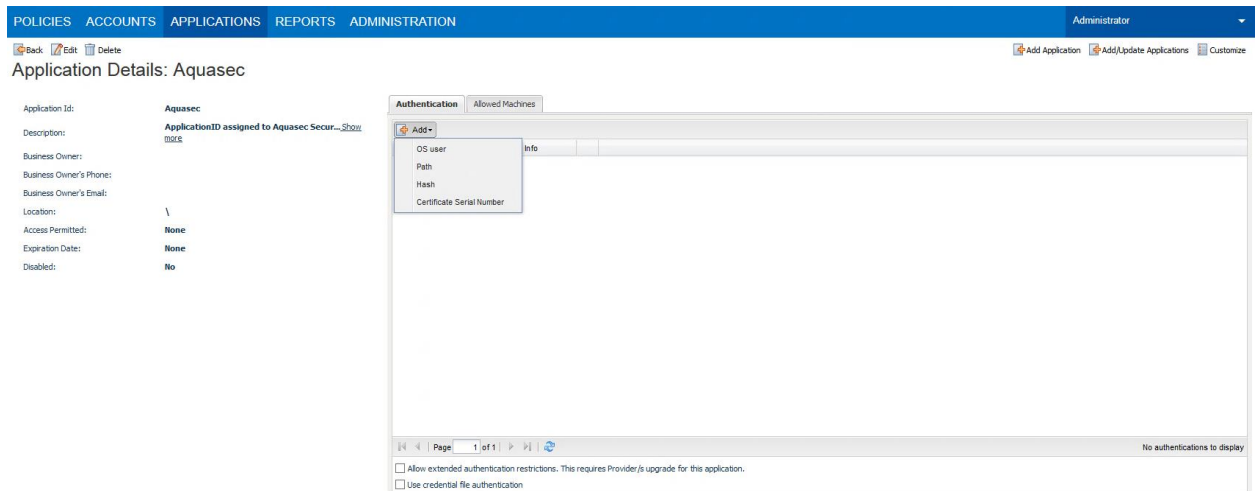
☐ Disabled

Add Cancel

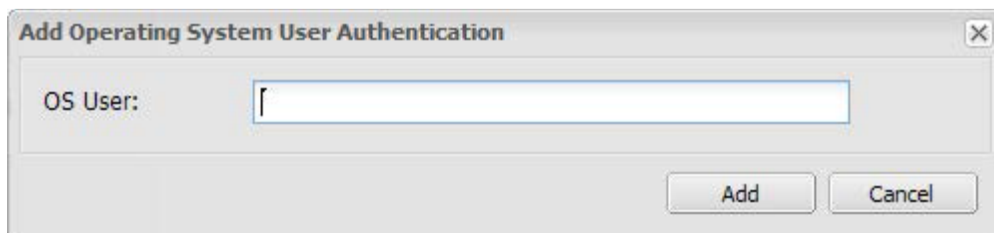
☐ Specify the following information:

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

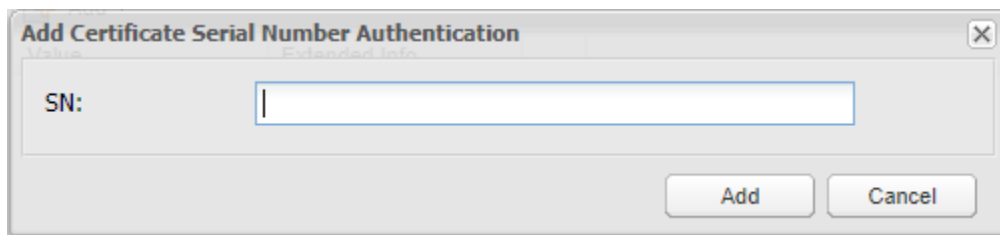
☐ Click **Add**. The application is added and is displayed in the Application Details page.



- ☐ 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

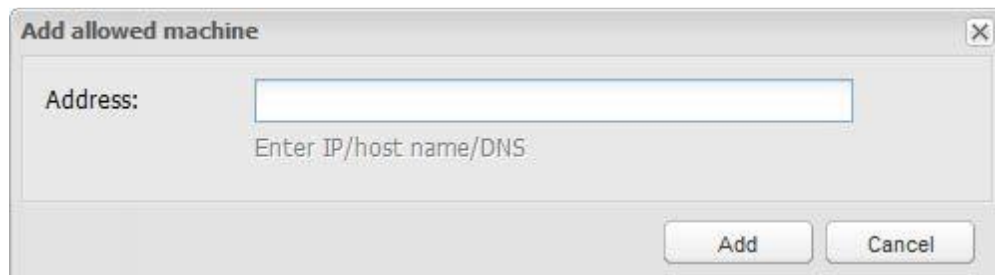
openssl x509 -in <cert file name> -serial -noout

- 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.
- 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.

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:

Selected Search: Vault Display 1 result(s)

Name	Business Email	Full Name
 Aquasec		

☐ Access

- ☐ Use accounts
- ☒ Retrieve accounts
- ☐ List accounts

☐ Account Management
☐ Safe Management
☐ Monitor

- ☐ View Audit log
- ☐ View Safe Members

Aquasec has been added.

- ☐ If the environment is configured for 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.
- ☐ 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**.

AQUA CSP INSTALLATION & INTEGRATION CONFIGURATION

Refer to docs.aquasec.com for Aqua CSP installation.

To configure CyberArk Enterprise Password Vault integration in Aqua server user should follow the steps below:

1. In the Aqua Management Console, go to System, Integrations.
2. Under the Secret Key Stores section, click on the Add Secret Key Store button.

Create New Key Store

* Key Store Name
Key Store Name

* Key Store Type
CyberArk Enterprise Password Vault

☐ Enabled

* Connection URL
Enter Connection URL

* App ID
Enter App ID

* Safe
Enter Safe

Pull Interval (minutes) ⓘ
1

Labels ⓘ
Select labels...

Save Changes Cancel

3. Enter a logical name for the Vault store.
4. Select the CyberArk Enterprise Password Vault from the Key Store Type drop down.
5. Click *Enable to enable the Vault store
6. Enter CyberArk Vault connection URL
7. Enter the Application ID as configured in CyberArk Vault
8. Enter the Safe name as configured in CyberArk Vault

PARTNER CONTACT INFO

Business Contact	Name	Upesh Patel
	Email	upesh@aquasec.com
	Tel	(781) 362-4787
Technical Contact	Name	Tsvi Korren
	Email	tsvi@aquasec.com
	Tel	(781) 362-4787
Support Contact	Name	Dustin Aubrey
	Email	dustin@aquasec.com
	Tel	(415) 946-4058