



Secrets Manager integration

(Agentless Central Credential Provider CCP)

Name of Company: Invicti

Website:

- <https://www.invicti.com/>
- <https://www.acunetix.com/>

Name of Product: Acunetix 360

Version: v1.9.4

Date: 24/02/2021

PARTNER SOLUTION OVERVIEW

Acunetix 360 is a best-of-breed enterprise web vulnerability solution designed to be a part of complex environments. It provides multiple integrations as well as options to integrate within custom contexts.

Acunetix 360 is designed to become a part of your complete cybersecurity environment and work with your other solutions. You can deploy Acunetix 360 either on-premises or as a cloud service and use it along with other security tools to get even better protection. Thanks to high performance and extensive integration options, you can improve security without overloading your resources.

Privileged access management (PAM) allows organizations to centrally store, manage, and secure administrative credentials and other high-value secrets. While using a secure central platform to store login credentials can greatly reduce the risk of data breaches, it can also make it harder for automated security testing tools to fully scan web applications. Acunetix 360 integrates with CyberArk to address this challenge.

Acunetix 360 is a complete web application security solution that integrates with dozens of products, including privileged access management solutions. While all data entered into Acunetix 360 and generated during application scanning is well protected, CyberArk integration lets you take security even further and ensure that plain-text secrets never leave your systems. That way, you can fully scan applications that require authentication without ever entering application access credentials into Acunetix 360.

Version: v1.9.4

KEY BENEFITS

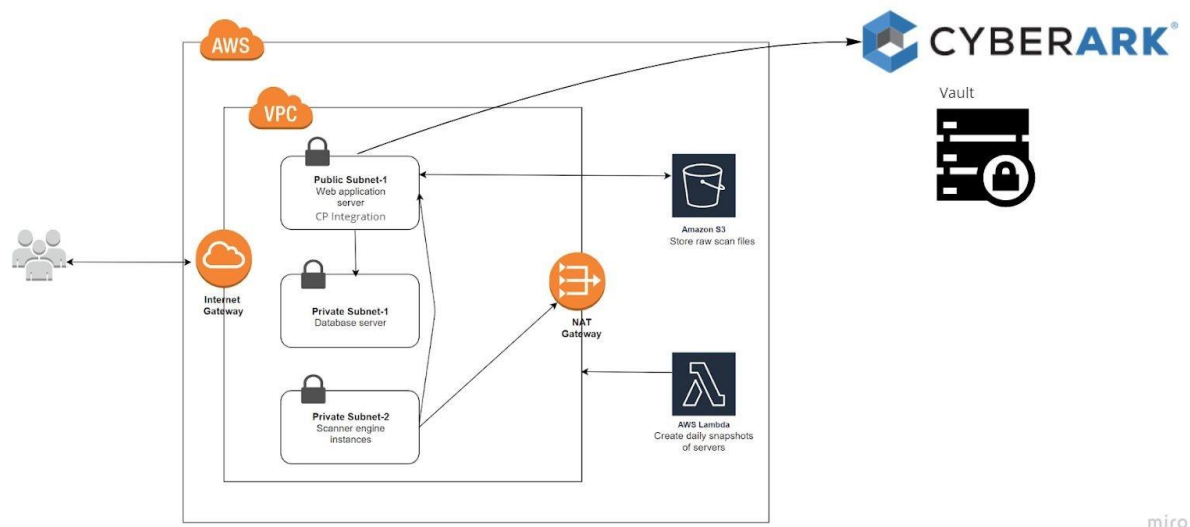
Benefits of Acunetix 360:

- Best-in-Class Web Security Tool
- Unparalleled Visibility with Comprehensive Reports
- Integrations with over 40 tools and systems including;
 - Issue Tracking Systems
 - Project Management
 - Continuous Integration Systems
 - Communication
 - Web Application Firewall (WAF)
 - Single Sign-On (SSO) Providers
 - Privileged Access Management
- Full-featured REST API which allows for easy integration

Benefits of integrating Acunetix 360 with CyberArk SECRETS MANAGER:

- To eliminate the need to share sensitive credentials for vulnerability scanning on password-protected web pages.
- To automate credential retrieval to carry out vulnerability assessment on the target website.
- To manage credentials easily while also ensuring that vulnerability scanning is carried out.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



SECRETS MANAGER INTEGRATION

SECRETS MANAGER integration lies in the integrations module of Acunetix 360. In UI/UXwise, a user activates/deactivates this integration while setting/starting a scan. At the beginning of the scan Acunetix 360 consumes this integration and receives necessary credentials. End Point or Mid-Tier or Central Server (Central Server). Number of mid-tier servers and number of endpoints in a typical installation

CREDENTIAL RETRIEVAL

While setting/starting a scan, a user specifies queries for username and password. The username query is optional, he/she may specify the username directly via the integration panel and may use this integration for only the password field. At the beginning of the scan, the request reaches the CyberArk server which is specified and configured by the user beforehand. If the query is correct, the credentials are returned by CyberArk. This depends on the asset size and the usage (scan count) of the customer.

REQUIREMENTS

The Acunetix 360 server and the CyberArk server should be able to access each other.

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

SECRETS MANAGER CONFIGURATION

The following sections provide details on Acunetix 360 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.

The screenshot shows the 'Add Application' dialog box with the following fields and values:

- Name:** AcunetixApp
- Description:** Acunetix Application Description
- Business owner:**
 - First Name:** Ogulcan
 - Last Name:** Erduran
 - Email:** ogulcan.erduran@invicti.com
 - Phone:** +10000000000
- Location:** \
- Access Permitted:** ☐ From: [dropdown] To: [dropdown]
- Expiration Date:** ☐ [calendar icon]
- Disabled:** ☐

Buttons: Add, Cancel

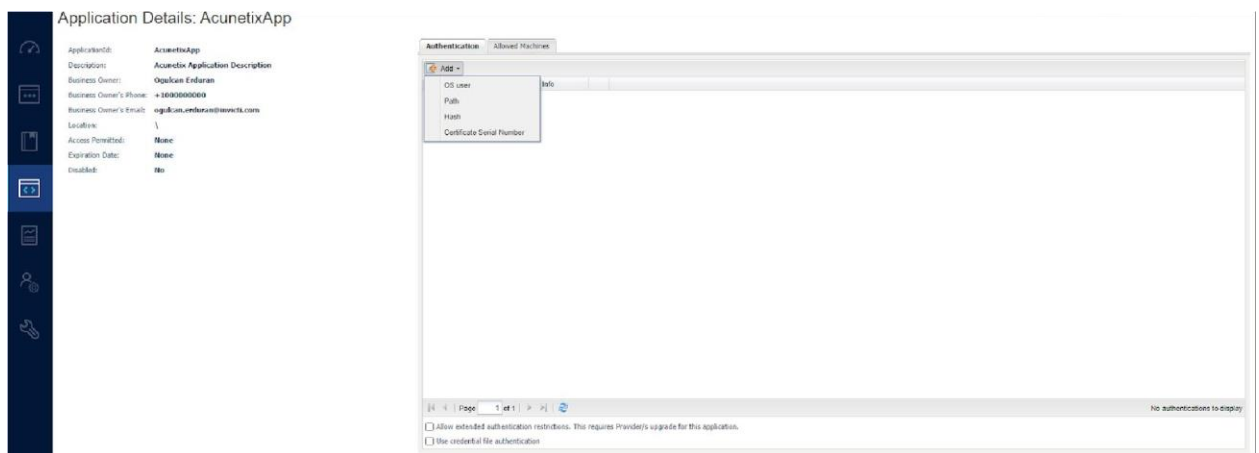
Specify the following information:

- In the **Name** box, specify the unique name (ID) of the application. The recommended

Application ID for this integration is: **APP ID = AcunetixApp**

- 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.

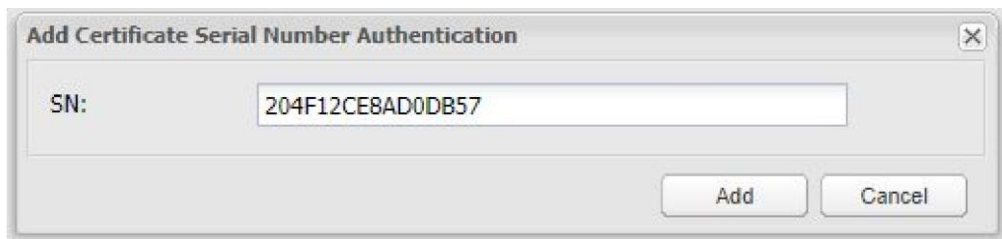


Check the **Allowing extended authentication restrictions** box. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.

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. 

Specify the Certificate Serial Number.



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:

Selected Search: Vault Display 1 result(s)

	Name	Business Email	Full Name
	AcunetixApp	ogulcan.erduran...	Ogulcan Erduran

☐ Access

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

☐ Account Management

☐ Safe Management

☐ Monitor

- ☐ View Audit log
- ☒ View Safe Members

☐ Workflow

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
 AcunetixApp	ogulcan.erduran...	Ogulcan Erduran

☐ Access

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

☐ Account Management

☐ Safe Management

☐ Monitor

- ☐ View Audit log
- ☐ View Safe Members

☐ Workflow

If the Safe is configured for o

bject 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**.

PARTNER PRODUCT INSTALLATION & INTEGRATION CONFIGURATION

Refer to [Integrating Acunetix 360 Enterprise with CyberArk](#) for Partner Product installation.

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 Please refer to the documentation mentioned above. **Partner Application UI:**

New CyberArk EPV Integration

Name ?

URL ?

Certificate File

Certificate File...

Certificate File

Certificate Password ?

Save

CyberArk EPV Settings

Integration

Cyberark

☐ Use static username

Username Query

Username Query

AppID=TestAppID&Query=Safe=TestSafe;Folder=Root\Secret;Object=TestObject&QueryFormat=Exact

Password Query

Password Query

AppID=TestAppID&Query=Safe=TestSafe;Folder=Root\Secret;Object=TestObject&QueryFormat=Exact

Test Vault Settings

Save

Cancel

CyberArk EPV Settings



Integration

Cyberark



☒ Use static username

Static Username

Static Username

Password Query

Password Query

AppID=TestAppID&Query=Safe=TestSafe;Folder=Root\Secret;Object=TestObject&QueryFormat=Exact

Test Vault Settings

Save

Cancel

PARTNER CONTACT INFO

Business Contact	Name	Yalin Yorulmaz
	Email	yalin.yorulmaz@invicti.com
	Tel	905054525089
Technical Contact	Name	Gokhan Tuylu
	Email	gokhan.tuylu@invicti.com
	Tel	905556285277
Support Contact	Name	Erman Ates
	Email	erman.ates@invicti.com
	Tel	905066893876