



CYBERARK SECRETS MANAGER

(Agent Based Credential Provider CP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Cavirin Systems, Inc.

Website: www.cavirin.com

Name of Product: Cavirin

Version: 8.4

Date: 30 September 2020 (5 November 2020)

CAVIRIN OVERVIEW

Cavirin ARAP (Automated Risk Analysis Platform) is a software appliance that helps ensure the security and compliance of IT infrastructure on a continuous basis across private, public, and hybrid cloud environments. With its agentless architecture, it is capable of running trusted, deep discovery of resources such as bare metal hosts, virtual machines, network appliances, and containers to collect configuration information and evaluate the settings against a rich set of security hardening rules, as well as regulatory standards such as PCI, HIPAA, SOC, ISO, and more. Through its on-demand and scheduled security and compliance scanning ability, ARAP can provide comprehensive risk assessment in the form of a high level score, detailed policy failures, and remediation recommendations.

The current version ARAP is 8.4.

It is supported on Linux platform, and available as Amazon AMI, VMWare OVA, Docker Container, and Microsoft Hyper V images.

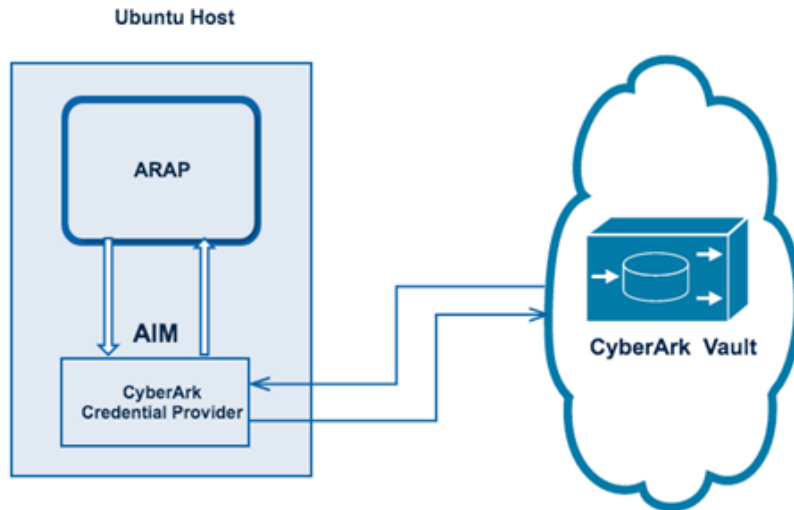
KEY BENEFITS

Cavirin ARAP (Automated Risk Analysis Platform) can provide comprehensive risk assessment of IT infrastructure based on its trusted deep discovery ability of various resources. For this, ARAP's low-footprint, agentless architecture relies on the availability of credentials to hosts and virtual machines in the form of username and passwords or security keys.

Commonly, many security-conscious enterprises prefer to store and manage the credentials to key infrastructure systems through password vaults such as CyberArk. The integration of ARAP with Secrets Manager, provides a mechanism for retrieving the credentials directly out of CyberArk Password Vault for security and compliance scanning of IT resources. The key benefits are that credentials for resources need not be setup on ARAP, and that credentials can be managed from the central password vault without having to duplicate them on the ARAP server.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

Integration Architecture Diagram



SECRETS MANAGER INTEGRATION

Cavirin ARAP never directly communicates with Vault server. It always talks to Secrets Manager provider which in turn talks to the Vault to get the password information. Therefore, Credential Provider must be installed in the system where Cavirin ARAP runs.

CREDENTIAL RETRIEVAL

Cavirin ARAP never stores credentials in the database. It always makes a call to the Secrets Manager Credential Provider whenever necessary during discovery phase.

SECRETS MANAGER INSTALLATION

Refer to the [“Credential Provider and ASCP Implementation Guide” for CyberArk Agent based installation and configuration.](#)

SECRETS MANAGER CONFIGURATION

The following sections provide details on Cavirin 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: Cavirin_ARAP

Description: Application ID for Cavirin's Automated Risk Analysis Platform (ARAP)

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: Cavirin_ARAP
- 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.

POLICIES ACCOUNTS MONITORING APPLICATIONS REPORTS ADMINISTRATION

Back Edit Delete

Application Details: Cavinr_ARAP

Application Id: Cavinr_ARAP

Description: Application ID for Cavinr's Automated R... [Show more](#)

Business Owner:

Business Owner's Phone:

Business Owner's Email:

Location: \

Access Permitted: None

Expiration Date: None

Disabled: No

Authentication Allowed Machines

Add

- OS user
- Path
- Hash

Extended Info

Page 1 of 1

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

☐ Use credential file authentication

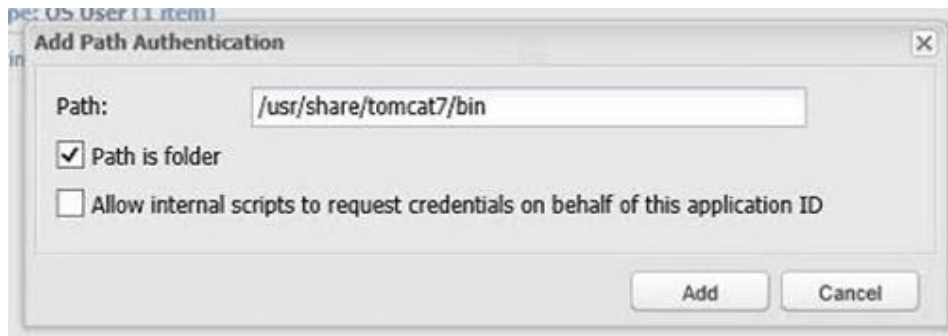
- ☐ Check the **Allowing extended authentication restrictions** box. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.
- ☐ Specify the application's **Authentication** details. This information enables the Credential Provider to check certain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

Add Operating System User Authentication

OS User: Cavinr X

Add Cancel

- ☐ Specify the name of the OS user who will run the application, then click **Add**. The OS user is listed in the Authentication tab.
- ☐ Select **Path**. The Add Path Authentication window appears.



- ☐ In the **Path** box, specify the path where the application will run. To indicate that the specified path is a folder, select **Path is folder**. 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**.
- ☐ Click **Add**. The Path is added as an authentication characteristic with the information that you specified.

POLICIES ACCOUNTS MONITORING APPLICATIONS REPORTS ADMINISTRATION

Back Edit Delete

Application Details: Cavinr_ARAP

Application Id: **Cavinr_ARAP**

Description: **Application ID for Cavinr's Automated R...**
[Show more](#)

Business Owner:

Business Owner's Phone:

Business Owner's Email:

Location: ****

Access Permitted: **None**

Expiration Date: **None**

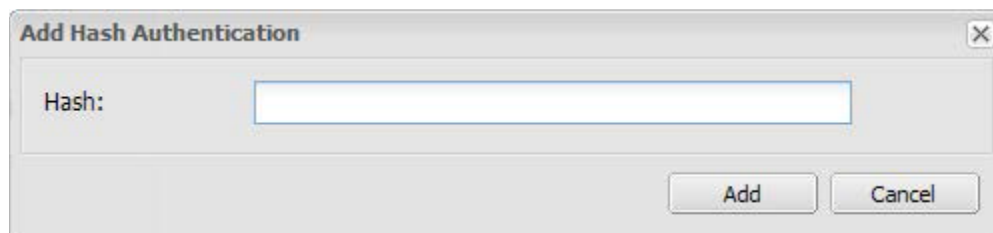
Disabled: **No**

Authentication
Allowed Machines

Add

Value	Extended Info
Type: OS User (1 item)	
Cavinr	
Type: Path (1 item)	
/usr/share/tomcat7/bin	Folder

- ☐ Specify a hash:
 - Run the AIMGetAppInfo utility to calculate the application's unique hash. Copy the hash value that is returned by the utility.
 - In the PVWA, select **Hash**. The Add Hash window appears.



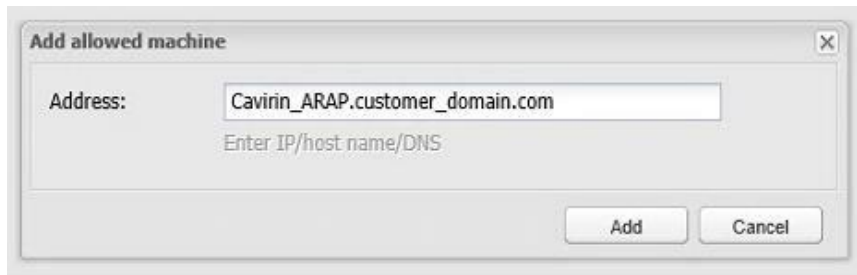
- In the Hash edit box, paste the application's unique hash value, or specify multiple hash values with a semi-colon. You can add additional information in a comment after each hash

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.

- Click **Add**. The Hash is added as an authentication characteristic with the information that you specified.
- ☐ 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.
- 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.

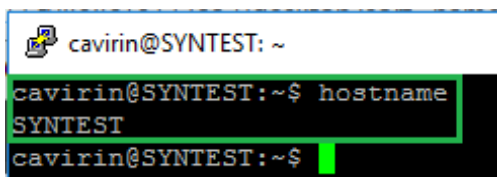
Add the Credential Provider and application users as members of the Password Safes where the application passwords are stored. This can either be done manually in the Safes tab, or by specifying the Safe names in the CSV file for adding multiple applications.

☐ 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.

Get the hostname. open terminal, type hostname.

A terminal window with a black background and green text. The prompt is 'cavirin@SYNTEST: ~'. The command 'hostname' has been entered, and the output 'SYNTEST' is displayed on the next line. The prompt 'cavirin@SYNTEST: ~\$' is visible at the bottom.

```
cavirin@SYNTEST: ~  
cavirin@SYNTEST:~$ hostname  
SYNTEST  
cavirin@SYNTEST:~$
```

Click **Add Member**. This window appears. Search with prov_hostname (Ex: prov_SYNTEST). Select the user. Give permissions as shown below, then click **Add**.

Add Safe Member

Search: Search In:

Selected Search: Vault Display 1 result(s)

Name	Business Email	Full Name
 Prov_SYNTEST		

☐ 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
Cavirin_ARAP		

☐ Access
☐ Use accounts
☒ Retrieve accounts
☐ List accounts
☐ Account Management
☐ Safe Management
☐ Monitor
☐ View Audit log

Cavirin_ARAP has been added.

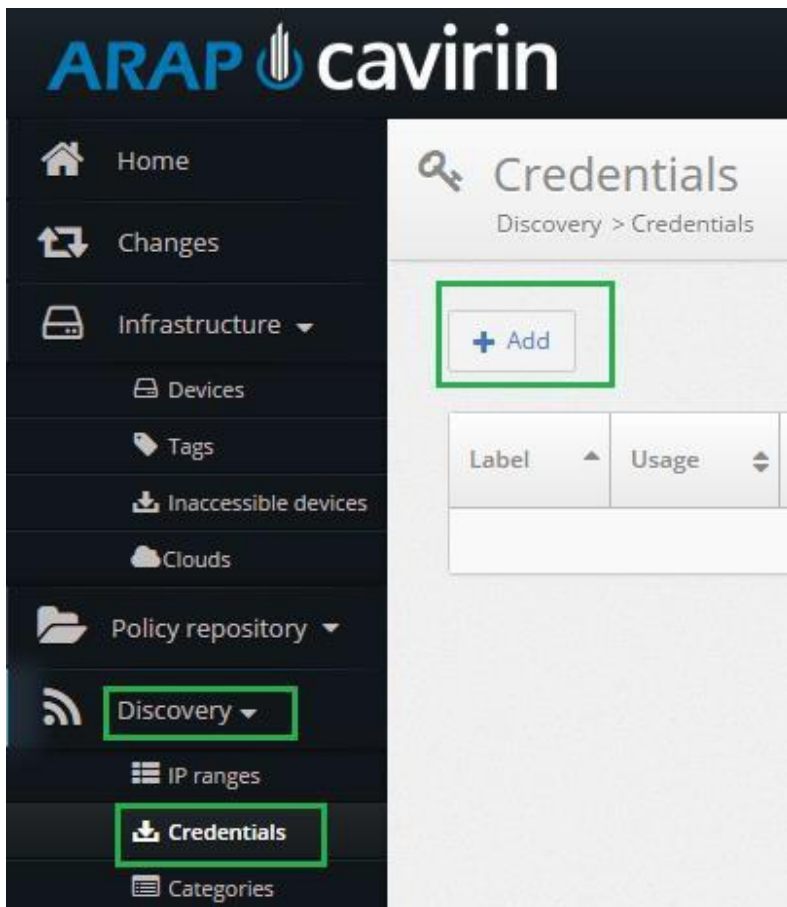
- ☐ If the Safe is configured for object level access, make sure that both the Provider user and the application have access to the password(s) to retrieve.

For more information about configuring Safe Members, refer to the **Privileged Access Security Implementation Guide**.

CAVIRIN INSTALLATION & INTEGRATION CONFIGURATION

Refer to Cavirin for Cavirin installation.

1. Login to ARAP Application.
2. Go to Discovery → Credentials → Click **Add**.



3. In the type drop down, choose CyberArk. Give Safe, Credential name. Give Label of your choice, then Save.

Add a credential

Review the device credentials that will be used for scanning. [Please read: important credential requirements.](#)

Type:

Usage:

Application:

Safe:

Credentials Name:

Label:

4. Add device in Discovery page and perform scan.

ARAPcavirin

- Home
- Changes
- Infrastructure
 - Devices
 - Tags
 - Inaccessible devices
 - Clouds
- Policy repository
 - Discovery
 - IP ranges**
 - Credentials
 - Categories
 - Scan jobs
- Reports

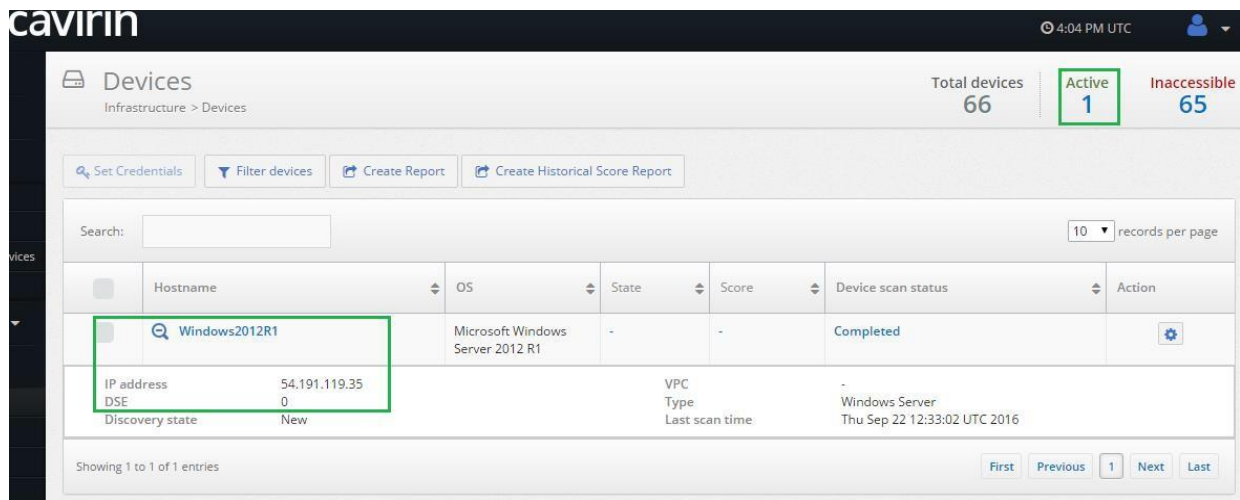
Discovery

Discovery > IP ranges

	Label	Start	End	Actions
☐	win2012R1	54.191.119.35	54.191.119.35	

- Set credentials
- Scan now**
- Schedule
- Edit range
- View scan logs
- Abort scan
- Delete

5. During the scan, ARAP gets the credentials from the Vault and uses those credentials to connect to the device. When credentials are successfully validated, the device will be listed under the Active section.



>>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)

PARTNER CONTACT INFO

Business Contact	Name	Nick Sappa
	Email	nsappa@cavirin.com
	Tel	
Technical Contact	Name	Ravi Rajamiyer
	Email	ravi@cavirin.com
	Tel	(408) 887-8859
Support Contact	Name	
	Email	
	Tel	