



Secrets MANAGER

(Agentless Central Credential Provider CCP)

Secrets manager INTEGRATION - TECHNICAL DOCUMENTATION TEMPLATE

Name of Company: Pontis Research Inc

Website: www.pontisresearch.com

Name of Product: iamaware CyberArk Collector

Version: 1.4

Date: February 10, 2021

PARTNER SOLUTION OVERVIEW

iamaware™ v2.0 offers a groundbreaking single pane view of disparate IAM solutions in an enterprise.

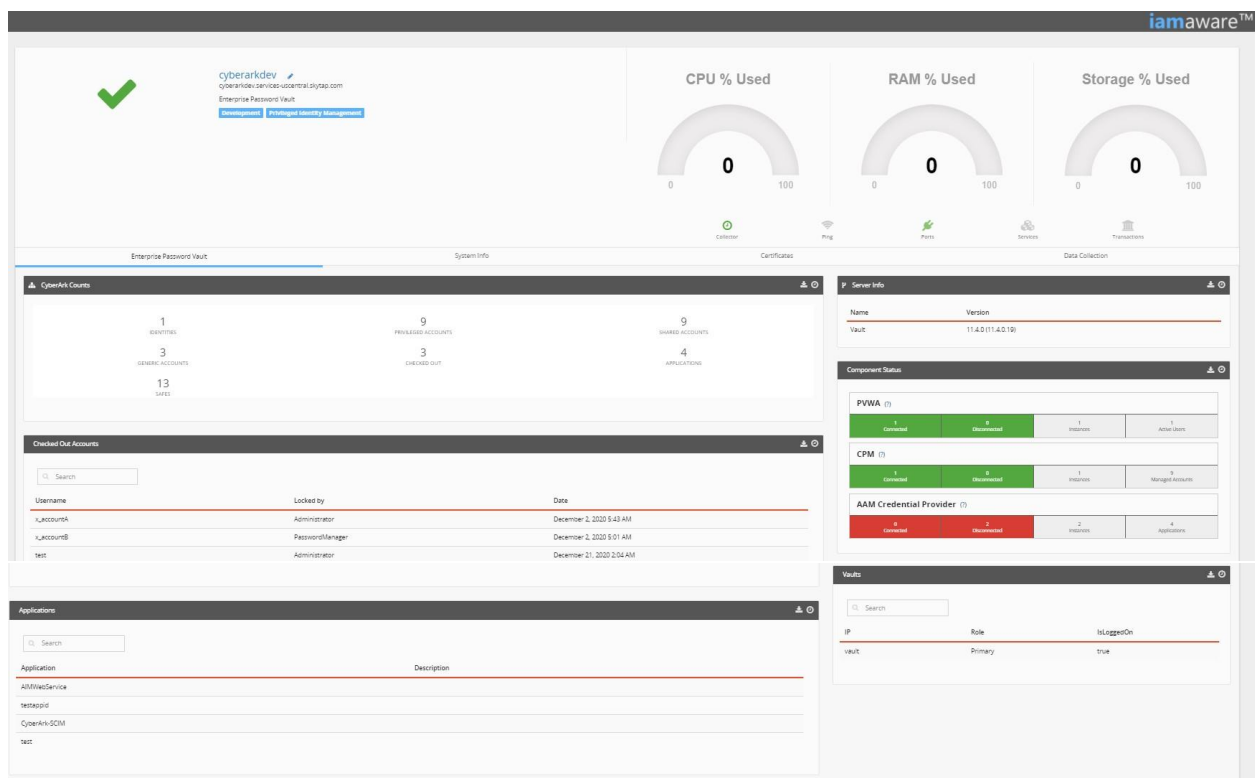
Organizations can assess the productivity and value of their IAM investment, monitor and identify potential issues before they bring systems down, forecast IAM resource needs based on actual usage and trends, thereby reducing operational costs while improving productivity.

Once **iamaware** is installed in the enterprise, it provides management, administrators and operations staff a holistic view of the overall IAM landscape.

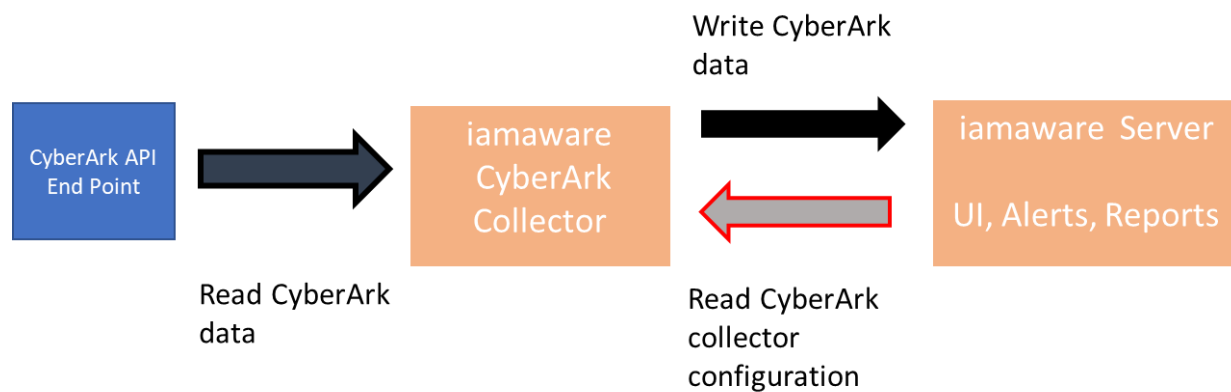
KEY BENEFITS

Benefits of **iamaware**:

- Monitors productivity, security and health of IAM solutions
 - Monitors IAM tools on-premise and in the Cloud
 - Continuously tracks the health of IAM across different products and vendors
 - Alerts on anomalous behavior, allowing for proactive correction before users are impacted
 - Optional reporting of user metrics from HR, ITSM and other data sources
- Flexible set of IAM focused dashboards
 - Views of expiring and expired certificates, failed login attempts, privileged account activity and trends, server statistics, productivity measurements, etc.
 - Dashboards that can be customized and set up by role or technology
 - Single view of all IAM servers, across Production, Test and Development environments
 - Support for disparate products from leading IAM vendors



PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



Secrets Manager INTEGRATION

iamaware uses credentials to collect data from servers/appliances/cloud environments. These credentials can be stored in the iamaware database or in CyberArk.

If the credentials are stored in CyberArk, the iamaware collector periodically (configurable) retrieves the credentials from CyberArk Secrets Manager using the object, app id and safe information stored in the iamaware database. In a typical installation there is one iamaware collector. The iamaware collector is an end point.

CREDENTIAL RETRIEVAL

Credential retrieval is triggered when the iamaware collector starts collecting for a server or periodically thereafter (the frequency is configurable, default is every 10 minutes).

No specific properties other than user ID and password are required for windows/unix/other credentials as the credential context is stored in iamaware.

REQUIREMENTS

Remote Access Requirements:

The Pontis team requires remote access to the iamaware™/ iamsmart™ server in order to deploy and configure the tool. This includes creating user accounts for PRI resources and granting VPN access.

iamaware/iamsmart Server Requirements

Server	OS	CPU	RAM	Storage	Prerequisites
--------	----	-----	-----	---------	---------------

iamaware/iam smart Application Server	Windows/Linux	8	16GB	50GB filesystem for iamaware/iam smart user (Linux only)	.net 4.0 (windows only)
Database Server (SQL Server or DB2)	Windows/Linux	8	16GB	150GB for database	SQL Management Studio (windows only)

Security Credential Requirements

1. Application Server and Database

a. Windows Server

Credential	New or Existing	Comments	Example ID
iamaware/iam smart AD domain account	New	To allow WMI access to Windows servers to gather CPU, RAM and other metrics. This ID requires administrative access on the IAM servers it is monitoring as well as the iamaware/iam smart server.	iamaware
iamaware/iam smart database instance IDs	New	Used by the iamaware/iam smart database. This is not an	iaminst1
		AD account but a local SQL account. Requires dbo rights.	

b. Linux Server

Credential	New or Existing	Comments	Example ID
iamaware/iamsmart account	New	Application will run as this user	IAMAWARE
iamaware database instance IDs	New	Used by the iamaware/iamsmart database. This is not an AD account but a local SQL account. Requires db owner rights.	iaminst1

Secrets Manager INSTALLATION

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

Secrets Manager CONFIGURATION

The following sections provide details on the iamaware 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.

Application Details: PontisResearch-IAMAware

ApplicationId: PontisResearch-IAMAware
Description:
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: Certificate Serial Number (1 item)		
204F12CEBA...		

☐ Specify the following information:

- In the Name edit box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: APP ID = PontisResearch-IAMAware
- In the Description, 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 lowest section, 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.

AUTHENTICATION DETAILS

- ☐ Specify the application's **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password. Partner should suggest the authentication details to secure the access by the partner's application (In this case its certificates)
- ☐ Specify the Certificate Serial number:

Authentication		Allowed Machines
Add		
Value	Extended Info	
Type: Certificate Serial Number (3 items)		
3600000028935285868FD98AF0000000000028		
360000002B61C33E9FA8AB2FD100000000002B		
204f12ce8ad0db57		

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 (Step 1). 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 (Step 2).

1. 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.

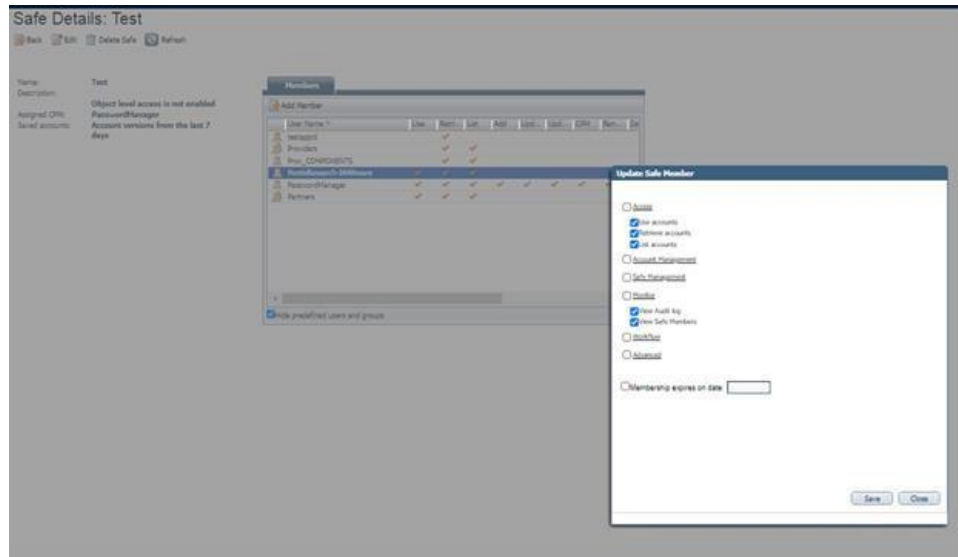
For more information about adding and managing privileged accounts, refer to **the Privileged Access Security Implementation Guide**.

2. 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.

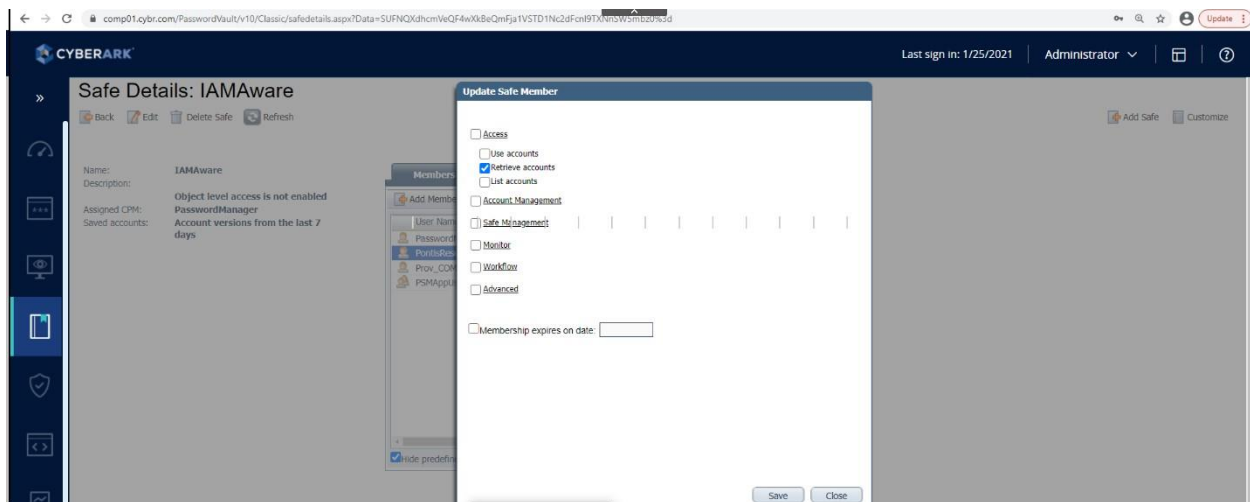
- i. Add the Provider user as a Safe Member with the following authorizations:

- 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.



- ii. Add the application(the APPID) as a Safe Member with the following authorizations:



- iii. 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**.

PARTNER PRODUCT INSTALLATION & INTEGRATION CONFIGURATION

Following are the instructions for configuring a new server within **iamaware**:

ADDING A NEW SERVER

To add a new server, select the *New Server* button on the *Servers* dashboard and complete the following steps:



The screenshot shows the 'New Server' form. At the top, there is a dark header bar with a hamburger menu icon and the text 'New Server'. Below this, the form has a section titled 'Clone from existing' which contains a dropdown menu with the placeholder text 'Select Server...'. Below the dropdown menu are two buttons: a green button with a checkmark icon and the text 'Create from Clone', and a blue button with an 'x' icon and the text 'Create from scratch'.

A) If you want to create the new server based on an existing server:

- Select the existing server in the *Clone from existing* dropdown menu
- Enter the fully qualified host domain name in the *Enter the new FQDN* box (host.domain.com)
- Select the *Create from Clone* button

B) If you want to create the new service from scratch, select the *Create from scratch* button.



The screenshot shows the 'New Server' form with the 'Clone from existing' dropdown menu set to 'gitlab'. Below this, the 'Enter the new FQDN' text box contains the text 'idm1.yourcompany.com'. The 'Create from Clone' button is highlighted in green, and the 'Create from scratch' button is blue.

C) On the *Basic Info* tab, enter/update the general information about the server

Basic System Information

FQDN (Fully qualified domain name): idm1.yourcompany.com

ID: idm1

Environment: Production

Network Zone: Internal

Groups: Access Management

Description: test

Groups are used to help you filter and find services, services and appliances.

Administrative Console URLs

These URLs are will be displayed as links when viewing information about this system.

Name	URL
Admin Console	http://hostname.domain.com

+ Add

- i. FQDN: Fully qualified host domain (host.domain.com)
- ii. Environment (Production, QA, Development)
- iii. Network Zone (Internal, External)
- iv. Groups: used to help filter and find services and appliances (Identity Management, Directory, Infrastructure, Privileged Identity Management, Governance)
- v. Description
- vi. Click + Add to configure Administrative Console URLs: displayed as links when viewing information about the system
 - a. Enter Name and URL

D) On the Type tab, enter/update the following information:

Type

Type: Linux

Products Installed: PRI Iamaware™ Remote Collector

This determines how system details will be displayed.

Server Role:

When there are multiple load balanced or clustered servers for a specific product, only a single "Primary" server will be queried for data. Be sure to set other servers as "Secondary" to avoid redundant queries.

- i. Type (Server Type)
- ii. Products Installed (Determines how system details will be displayed.)

- iii. **Server Role** (If there are multiple load balanced or clustered servers for a specific product, only a single "Primary" server will be queried for data. Be sure to set other servers as "Secondary" to avoid redundant queries.)

E) Enter/update the following information on the *Data Collection* tab:

Data Collection Status

Data collection is on by default and should be kept on in order for the system to function correctly. However in some cases you may wish to disable collection temporarily. When collection is disabled no data will be collected for the server and no alert notifications for the server will be sent.

Collect Data? (?)
☒ ON

Data Collection URLs

This data is used by iamaware™ collectors.

Connection Type Unix Server		✖ ✔ Test
Name Unix Server	URL idm1.yourcompany.com	
Login root	Password	

- i. **Data Collection Status** (Data collection is on by default and should be kept on in order for the system to function correctly. However, in some cases you may wish to disable collection temporarily. When collection is disabled no data will be collected for the server and alert notifications for the server will not be sent.)
- ii. For each connection type you want to collect data for, select the *Connection Type* and complete the required information. (Use the + *Add New Connection* to add additional connection types):
- iii. Use the test connection buttons to validate the collector information individually (Test) or all at once (Test All Connections)

✔ Test

✔ Test All Connections

- iv. If using a remote collector, enter the *Remote Collector Hostname*

Remote Collection

This section is only required if you are using a remote collector

Remote Collector Hostname

- v. Click the *Save* button

PARTNER CONTACT INFO

Business Contact	Name	Scott Swegles
	Email	scott.swegles@pontisresearch.com
	Tel	805-777-7424 ext 1010
Technical Contact	Name	Rajesh Sardhara Arvind Narain
	Email	rajesh.sardhara@pontisresearch.com arvind.narain@pontisresearch.com
	Tel	805-777-7424 ext 1005 805-777-7424 ext 1002
Support Contact	Name	Michele Campero Rajesh Sardhara Arvind Narain
	Email	michele.campero@pontisresearch.com rajesh.sardhara@pontisresearch.com arvind.narain@pontisresearch.com
	Tel	805-777-7424 ext 1004 805-777-7424 ext 1005 805-777-7424 ext 1002