



APPLICATION IDENTITY MANAGER

AIM INTEGRATION - TECHNICAL DOCUMENTATION

Phantom

<http://phantom.us>

Phantom Security Automation and Orchestration Platform

Version 2.1

February 28, 2017

PARTNER SOLUTION OVERVIEW

Phantom is a security automation and orchestration platform that integrates with your existing security technologies in order to provide a layer of “connective tissue” between them. Phantom operates at machine speed through the execution of digital “Playbooks” to achieve in seconds what may normally take minutes or hours to accomplish with the dozens of point products that you use every day. Phantom doesn’t replace existing security products, but instead makes your investment in them smarter, faster and stronger. Phantom accomplishes this through a logical architecture that abstracts product capabilities, through the Phantom App model, into simple Actions that can be automated from within Playbooks. This allows Phantom to act as an “operating system” for your security products.

KEY BENEFITS

Security teams operate Smarter, Faster & Stronger using Phantom’s Security Automation & Orchestration platform. Phantom works like a security OS to orchestrate key stages of security operations from prevention to triage and resolution, delivering dramatic increases in security operations productivity and effectiveness. Codifying your “rules of engagement,” approval authorities, and escalations let your skilled first responders bring to bear all of their experience to make better decisions and act quickly and confidently. Phantom helps security operations reduce time to detect and respond through automation. Faster triage, investigation, and recovery, combined with granular control of assets, ensures security at machine speed while maintaining continuity and control. Phantom helps you create a security team and environment that is worth far more than the sum of its parts. Consolidation and control make formerly static security systems agile and dynamic as you use Phantom to control your environment. Phantom works like “connective tissue” delivering the flexibility to connect in-house and third-party systems into one consolidated, integrated and extensible platform. Learnings from improved operations mean that your defenses are proactive and not reactive as you investigate, degrade, contain, recover and prevent security incidents.

While Phantom currently is capable of storing and encrypting passwords in a local database, some administrators would prefer not to have credentials stored in multiple places or any place that might come under attack. Additionally there are management challenges to keeping passwords in sync across an enterprise, especially where policies dictate that passwords be changed frequently or when there is any kind of breach. The resolution to both challenges is to keep passwords stored in a credential management application such as CyberArk AIM. Enabling CyberArk to provide secure storage and access to passwords reduces the attack surface, reduces the number of places where credentials can be found, and solves the challenge of keeping credentials synchronized.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

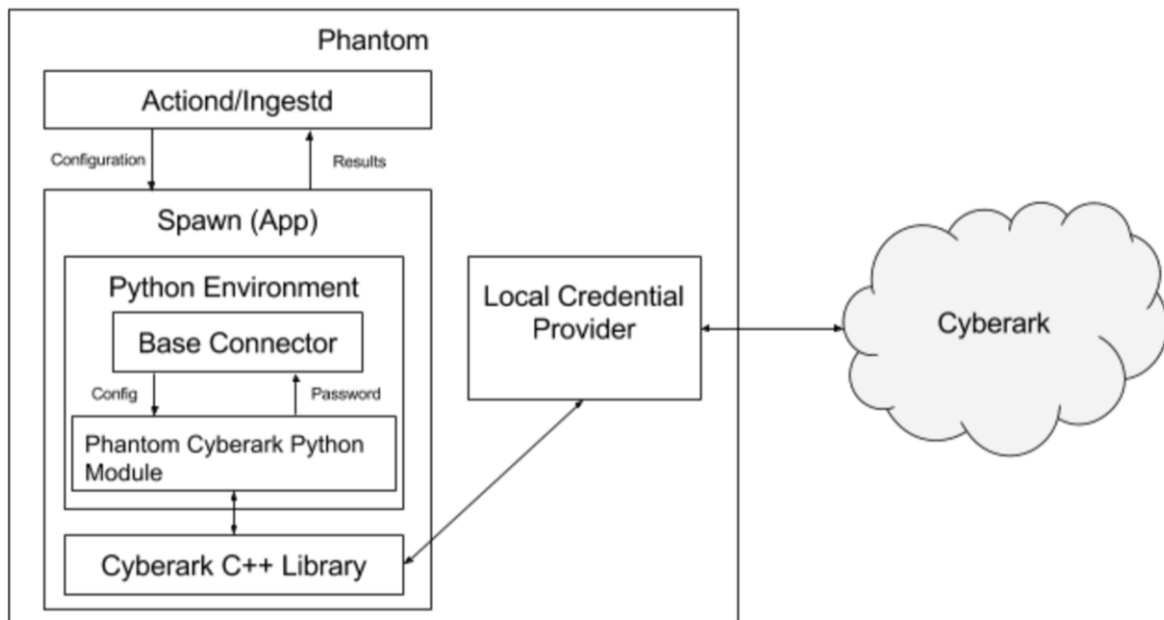


Figure 1: Interactions between Phantom App components and CyberArk

I. Description of where AIM Integration lies:

Phantom supports an App model to define how actions are executed against point security products and tools. Each time an action within an App is invoked, credentials are required to authenticate to the device. At this point, the App will retrieve the **Safe**, **Path**, and **Object Name** and pass that to the local credential provider installed on the Phantom platform. The local credential provider is installed and configured outside of the Phantom application, but on the same operating system. The local credential provider is then responsible for managing the delivery of the credentials from the CyberArk service.

II. The role of credential retrieval in the Phantom platform:

Actions that are invoked on the platform are ultimately executed on a point security product. Examples include (but not limited to) the following:

- Invoking a 'Block IP' action on a Firewall
- Invoking a 'File Reputation' action on a Reputation Service
- Invoking a 'Quarantine Device' action on an Endpoint solution

When an action is invoked, it is using the remote API of that product or service to carry out the execution of the action. Most services will require an authentication mechanism as part of the API call.

Examples include API tokens, API keys, Username/Password combinations. At action execution time, these credentials are used to carry out the API call. While Phantom supports the ability to store the credentials locally on the system, many users elect to use a credential management system such as CyberArk, where the credentials can be securely retrieved from CyberArk at action execution time.

AIM INSTALLATION

Refer to “Credential Provider and ASCP Implementation Guide” for CyberArk Credential Provider installation.

AIM CONFIGURATION

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

To define the Application, here are the instructions to define it manually via CyberArk’s PVWA (Password Vault Web Access) Interface:

1. Logged in as user allowed to managed 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

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

☐ Use credential file authentication

Add **Cancel**

2. Specify the following information:
 - In the Name edit box, specify Phantom.
 - 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.

3. Click **Add**; the application is added and is displayed in the Application Details page.

Application Id: **Phantom**

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
-------	---------------

Page 1 of 1

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

☐ Use credential file authentication

- **Allowing extended authentication restrictions.** This enables you to specify an unlimited number of machines and Windows domain OS users for a single application. Please check this box.
4. 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.

Add allowed machine

Address:

Enter IP/host name/DNS

Add Cancel

- 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 AIM 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 (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 Account Security Implementation Guide**.

2. 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.
 - 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.

Add Safe Member

Search:

Search In:

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

- ii. 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
Phantom		

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

- iii. If your 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.
- iv. 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 Account Security Implementation Guide**.

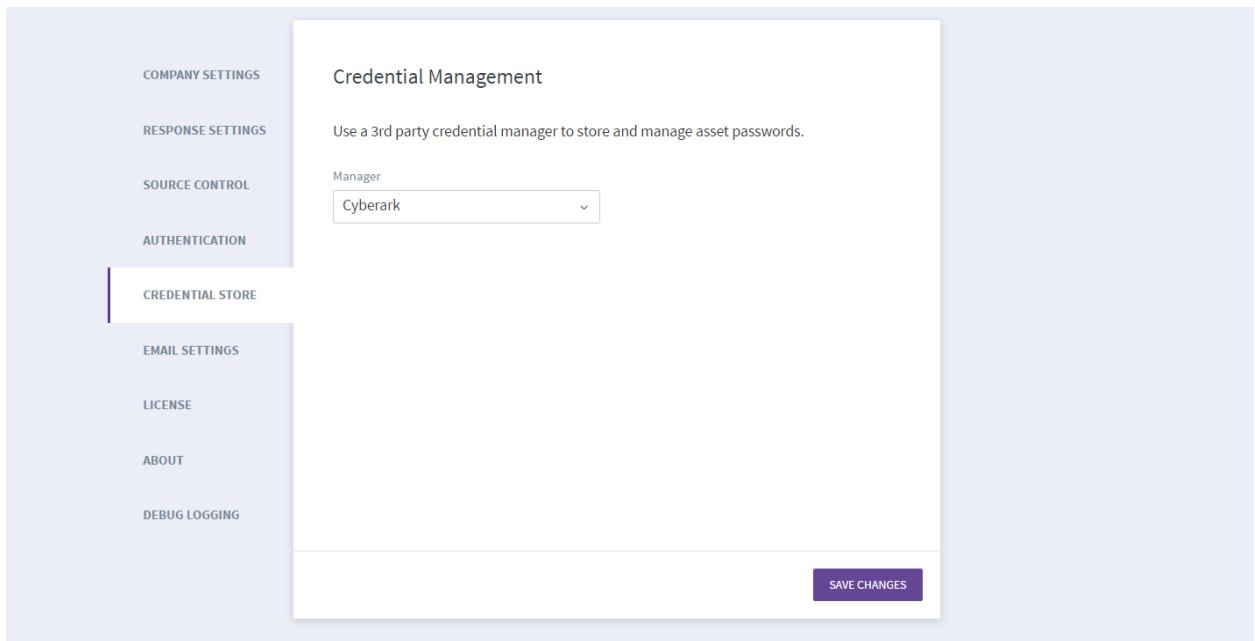
PARTNER PRODUCT INSTALLATION & INTEGRATION CONFIGURATION

Refer to the Phantom [Quickstart Guide](#) for Phantom platform installation.

There are two primary steps required to enable the Phantom platform to utilize CyberArk:

1. Configure a credential manager in the Phantom settings page:

- From the main menu, navigate to Administration -> Credential Store
- Select CyberArk from the Credential Manager drop down list
- The UI will prompt the administrator to enter the information needed to communicate with the CyberArk credential manager



2. Ensure Assets are configured to use the credential manager for authentication

- From the main menu, navigate to Apps
- Locate the App you are interested in configuring
- Select 'Configure New Asset'
- In 'Asset Settings', select which fields are externally managed.
- For each field the information needed in order to retrieve the field's value is expected. For CyberArk that information is the **safe**, **path** and **object name**.
- Use the 'Test Connectivity' action to ensure the configuration is working successfully

Asset Info
Asset Settings
Approval Settings

Device URL including the port, e.g.
https://myjira.enterprise.com:8080

http://10.16.0.180:8000

☐ Verify server certificate

Username

admin

Password

Optional

Credential Management

This section is for Cyberark integration. Typically an asset will have one password field which should be managed by Cyberark. Select which fields are managed via Cyberark and provide the name of the Safe, path in the Safe and name of the Object which contains the password.

Field	Safe	Path	Object	
password	Test	Root	test-g	-
+ FIELD				

EDIT
TEST CONNECTIVITY

Common use cases:

1. Securing credentials for Assets used in Phantom automation
 - a. When configuring the asset, the user will specify the Safe, Path, and Object for each field needed to authenticate to the asset
 - b. Credentials will be accessed only when a user or playbook invokes an action which in turn causes an App to be executed. Only the App, which is a short-lived process, will obtain credentials via CyberArk. Credentials will be resident in the process only for the lifetime of the action run.

PARTNER CONTACT INFO

Business Contact	Name	Robert Truesdell
	Email	robert@phantom.us
	Tel	412.913.8242
Technical Contact	Name	Sourabh Satish
	Email	sourabh@phantom.us
	Tel	
Support Contact	Name	Ryan Russell
	Email	ryan@phantom.us
	Tel	