CYBERARK SECRETS MANAGER

(Agent Based Credential Provider CP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Amelia

Website: www.amelia.ai

Name of Product: Amelia Platform (Previously IPsoft IPcenter)

Version: 5

Date: 3 December 2012 (Revised 31 January 2024)

AMELIA PLATFORM OVERVIEW

Amelia Platform is a real-time ITIL V3-aligned, real time portal, providing transparent access to the IT service delivery process.

Amelia Platform is an autonomic IT management platform. Amelia Platform is the only platform that guarantees business and services outcomes to drive productivity to new heights. Amelia Platform Virtual Engineers change the rules of the game by automating the interaction between all the different tools and people in your IT environment. Without being forced to replace your existing investments, you can automate end-to-end processes and pave the way for vast increases in productivity

Version: 4

KEY BENEFITS

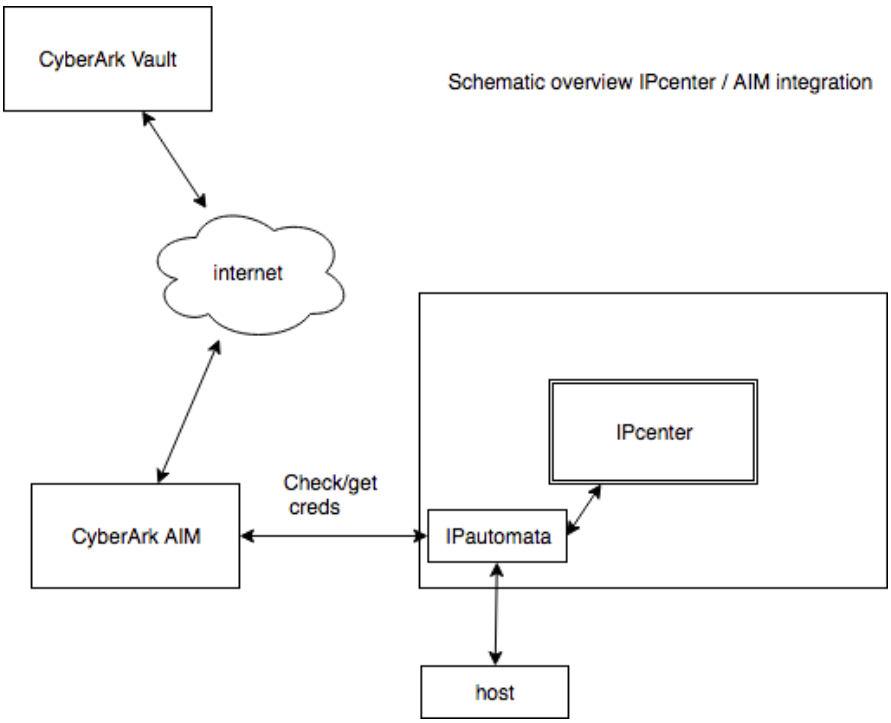
Key benefits of Amelia Platform

- ITIL v3 Aligned Service Portal
- Systematically enforced processes
- End-to-end automation

Key benefits of the Scerets Manager integration

The integration between CyberArk's Secrets Manager and Amelia Platform gives clients the ability to secure, monitor, and rotate credentials for the devices that Amelia Platform uses to monitor and automate the infrastructure in a client environment.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



SECRETS MANAGER INTEGRATION

The Secrets Manager client is installed on the application server. When IPautomata connects to a host, it communicates with the Secrets Manager agent, which has a hash that is bound to the Amelia Platform class(es).

The location is mid-tier. Endpoints vary greatly.

CREDENTIAL RETRIEVAL

Credentials are fetched and used in the connection to the host.

Credentials are fetched from CyberArk whenever the IP automata attempts to connect to the target device. The target device can be any operating system, but Amelia Platform runs on Linux (Scientific Linux) server.

REQUIREMENTS

Amelia Platform requires Secrets Manager to be installed on Red Hat Enterprise Linux (RHEL), on the same server as Amelia Platform.

SECRETS MANAGER INSTALLATION

Refer to the “Credential Provider and ASCP Implementation Guide” for CyberArk Agent based installation and configuration.

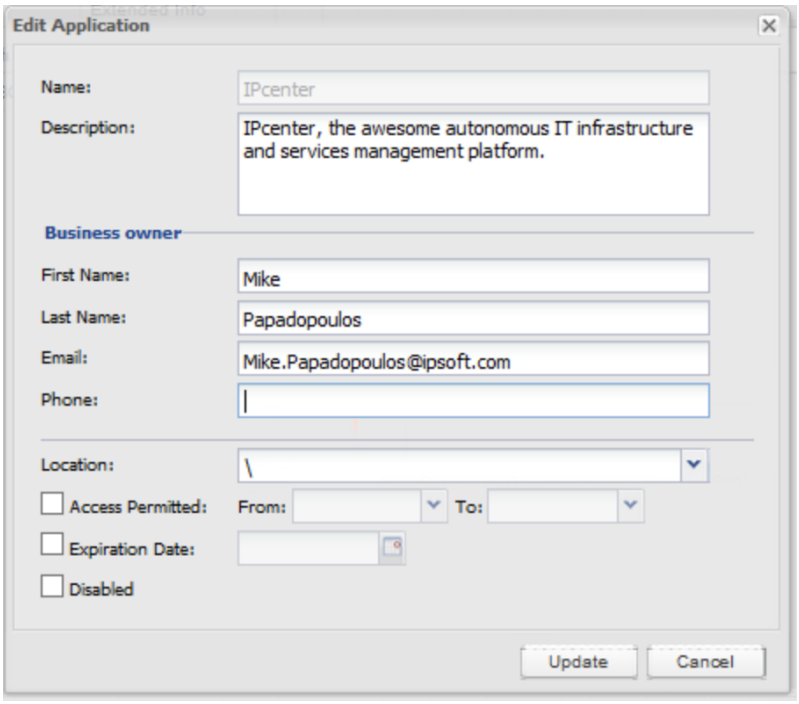
SECRETS MANAGER CONFIGURATION

The following sections provide details on Amelia Platform with CyberArk Secrets Manager.

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

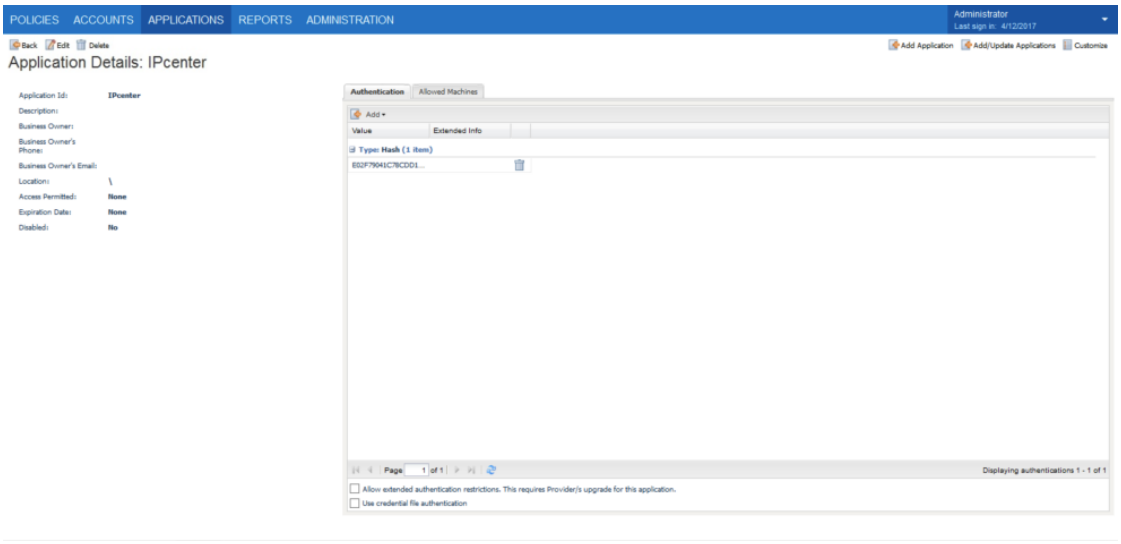
To define the application, define it manually through the CyberArk Password Vault Web Access (PVWA) interface:

- ☐ 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.



- ☐ Specify the following information:
  - In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: Amelia Platform
  - 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.

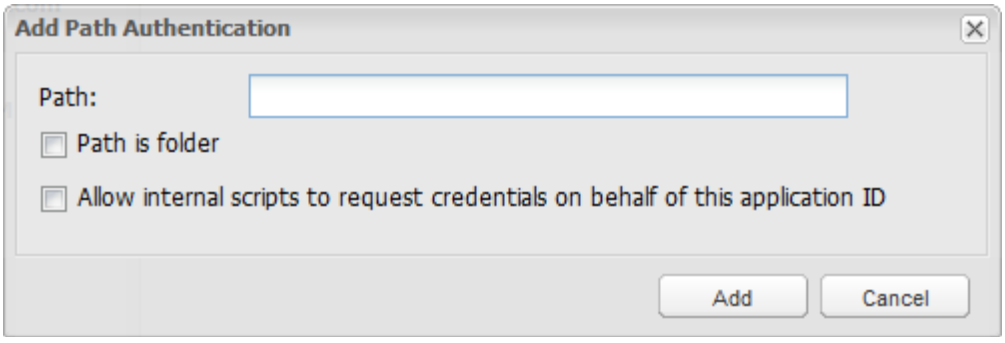
☐ In the Authentication tab, click **Add**. A drop-down list of authentication characteristics is displayed.

☐ 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.

☐ 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.

☐ Specify a hash:

- Run the AIMGetAppInfo utility to calculate the application's unique hash:

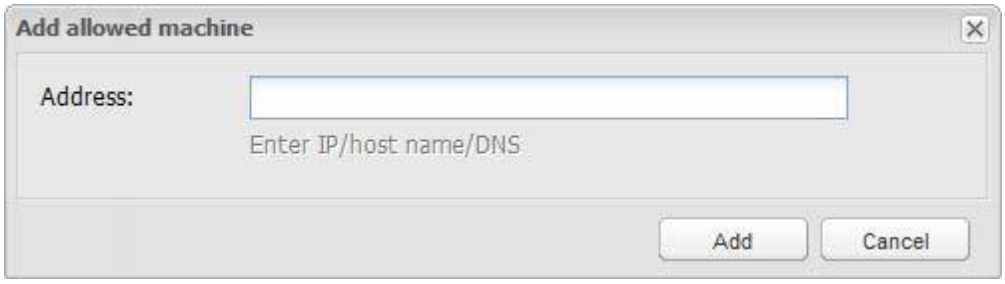
```
java -jar /opt/CARKaim/bin/javaaimgetappinfo.jar GetHash \-
AppExecutablesPattern="/apps/IP/amelia/classes" \-
OnlyExecutablesWithAIMAnnotation=yes -LogFileDirectory="/tmp"
```

- 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.**

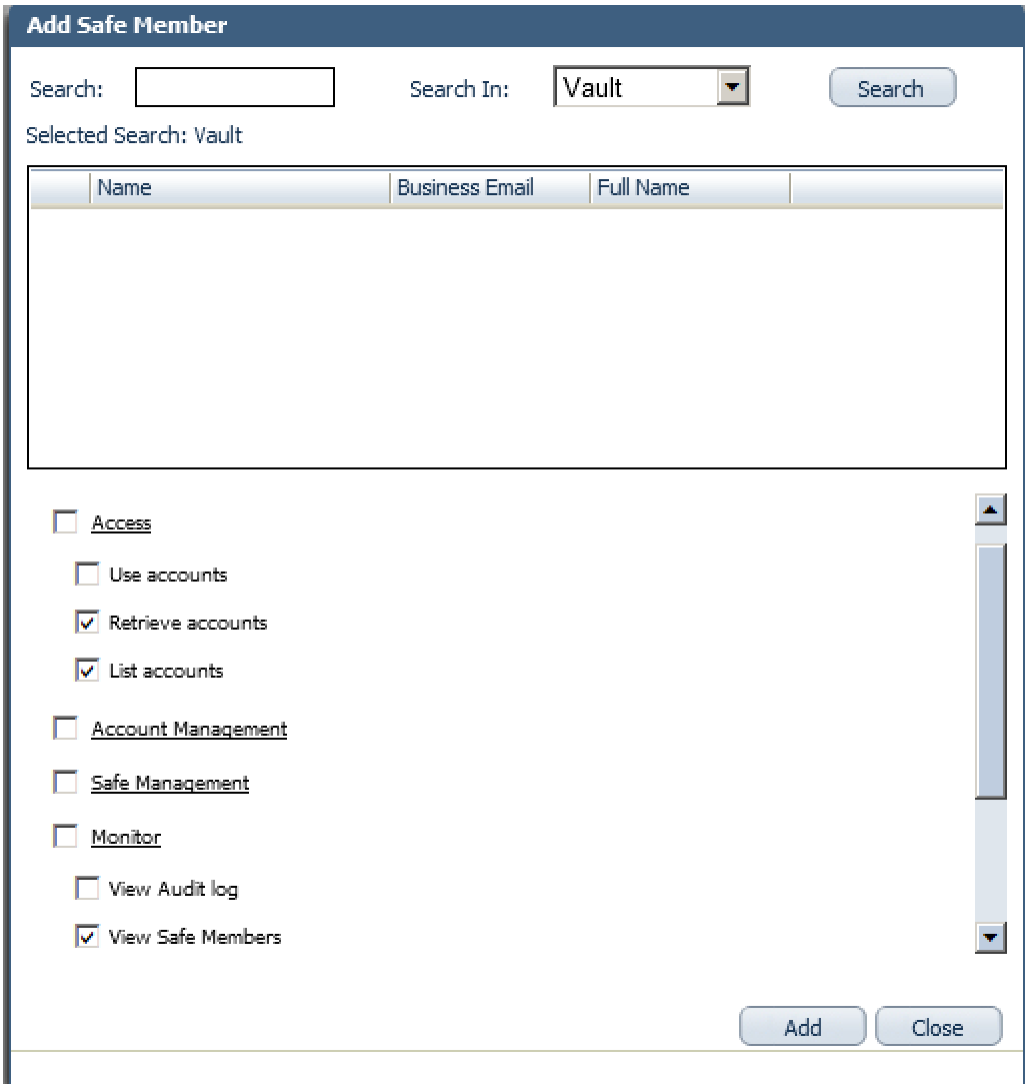
Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application.

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:

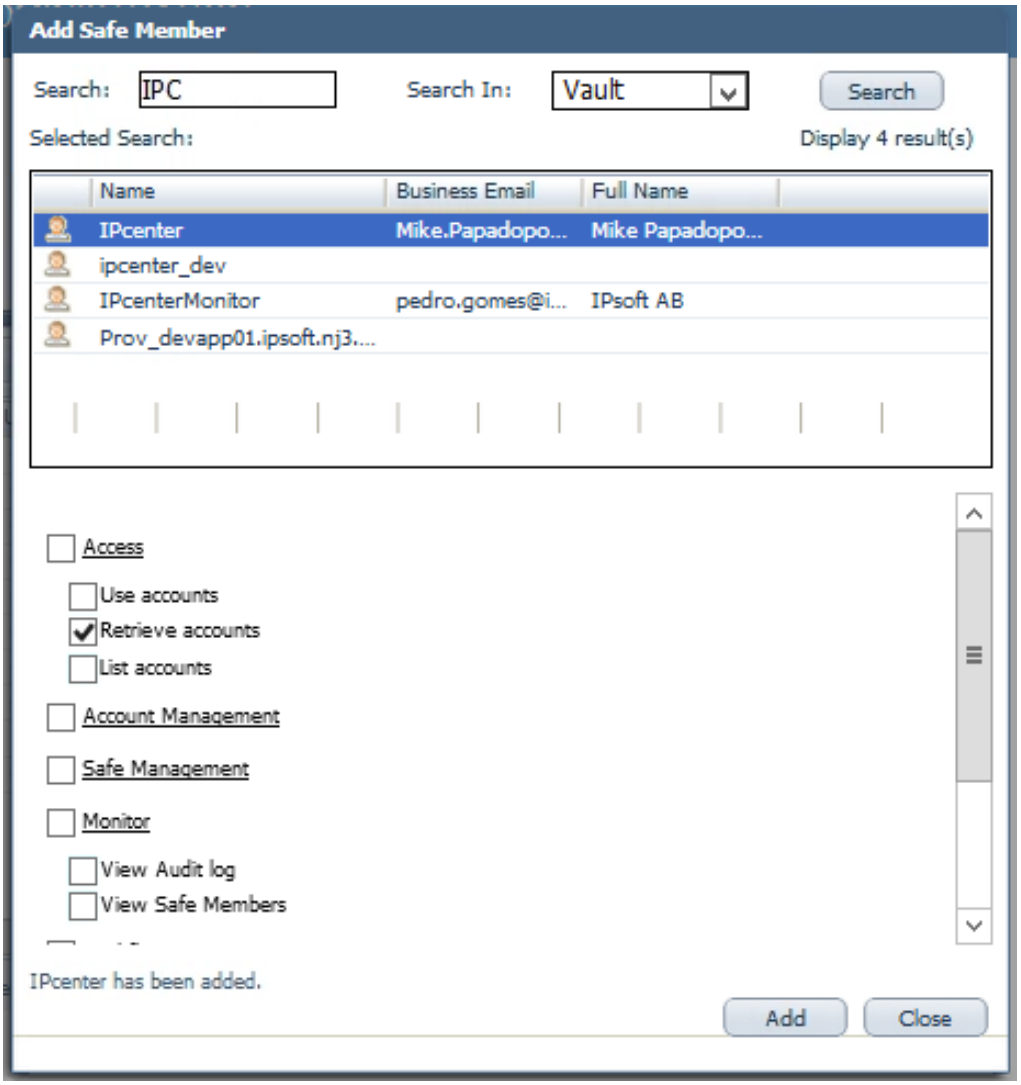
- List accounts
- Retrieve accounts
- View Safe Members

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.



☐ Add the application (the APPID) as a Safe Member with the following authorizations:

- Retrieve accounts



☐ 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.**

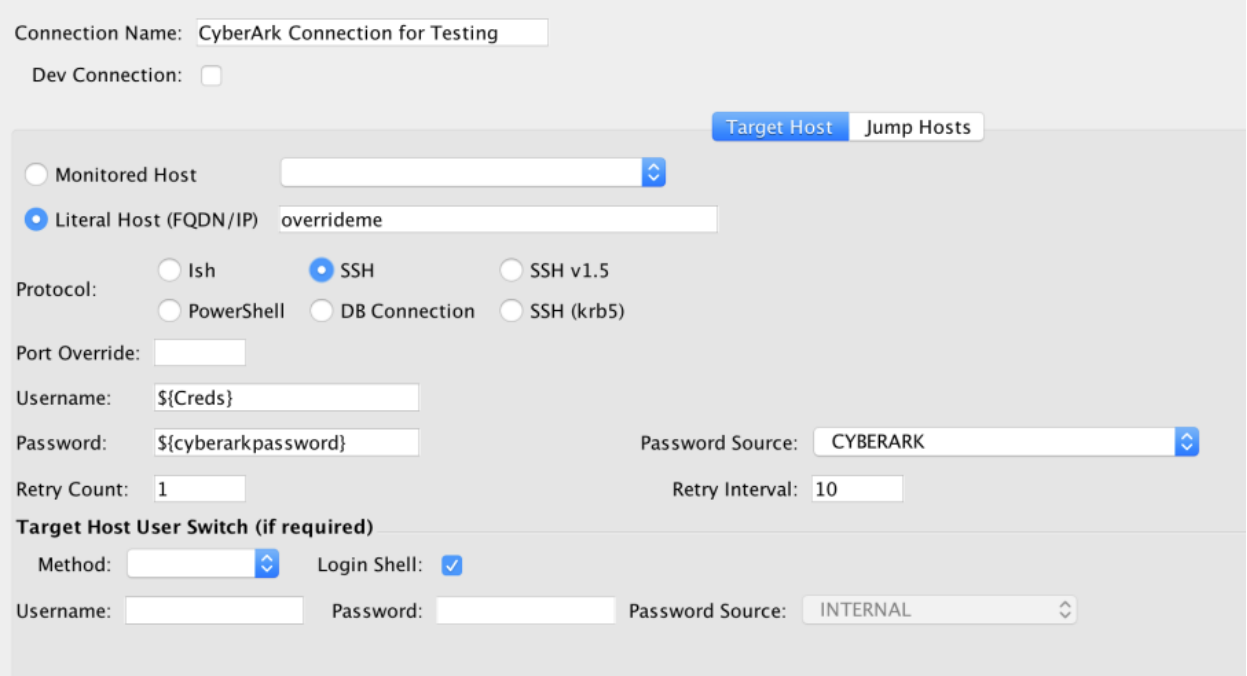
AMELIA PLATFORM INSTALLATION & INTEGRATION CONFIGURATION

Amelia Platform is installed and configured by our own staff.

Refer to 'CyberArk integration' for Amelia Platform installation.

1. Amelia Platform installation varies by type of installation. In general, it is done by running various scripts on the server component that is being installed, with various parameters.
2. The only extra configuration that is needed (besides Secrets Manager setup and configuration) is a connection with Password Source set to CYBERARK. This configuration should be performed by an engineer.
3. The Username and Password fields are populated with variables that will be used to query the configured CyberArk Vault.

The screenshot below shows the configuration in IPautomata designer:



PARTNER CONTACT INFO

Business Contact	Name	Mike Ghicas
	Email	mike.ghicas@amelia.com
Technical Contact	Name	Oleg Poleshuk
	Email	oleg.poleshuk@amelia.com
Support Contact	Name	Mike Ghicas
	Email	mike.ghicas@amelia.com