AAM INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: OpsRamp

Website: www.opsramp.com

Name of Product: OpsRamp

Date: April 23, 2019

OPSRAMP SOLUTION OVERVIEW

OpsRamp is an IT operations management platform on the cloud. OpsRamp helps you deliver availability, performance, capacity, asset, configuration, and remote access management as shared services and transform IT operations.

KEY BENEFITS

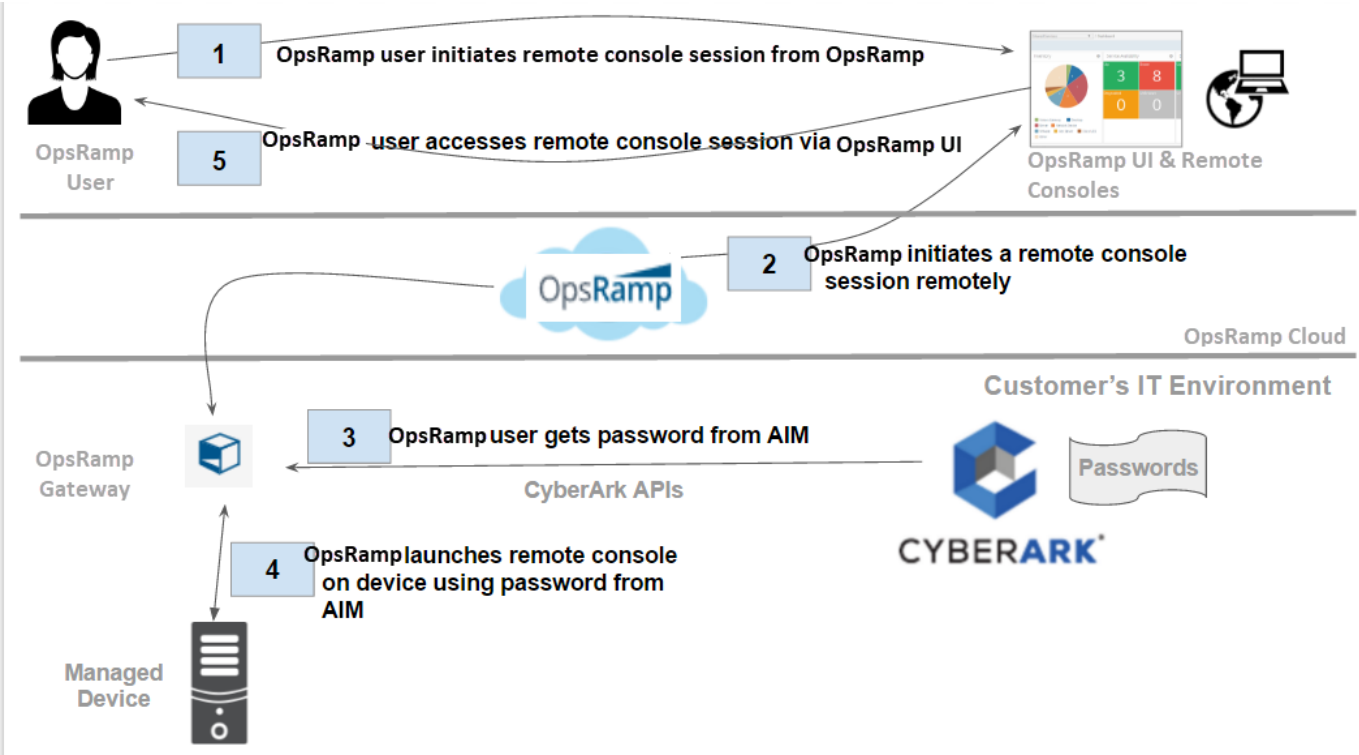
OpsRamp enables customers to:

- Manage more IT assets with the same staff levels.
- Establish a single point of visibility and control across datacenter and cloud.
- Enable your business to roll out new apps and IT services at digital speeds.

OpsRamp's integration with AAM enables customers to log into managed devices remotely via OpsRamp's remote console capability, using passwords securely stored within the CyberArk Vault.

DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

The figure below describes how a user would use the AAM integration between OpsRamp and CyberArk.



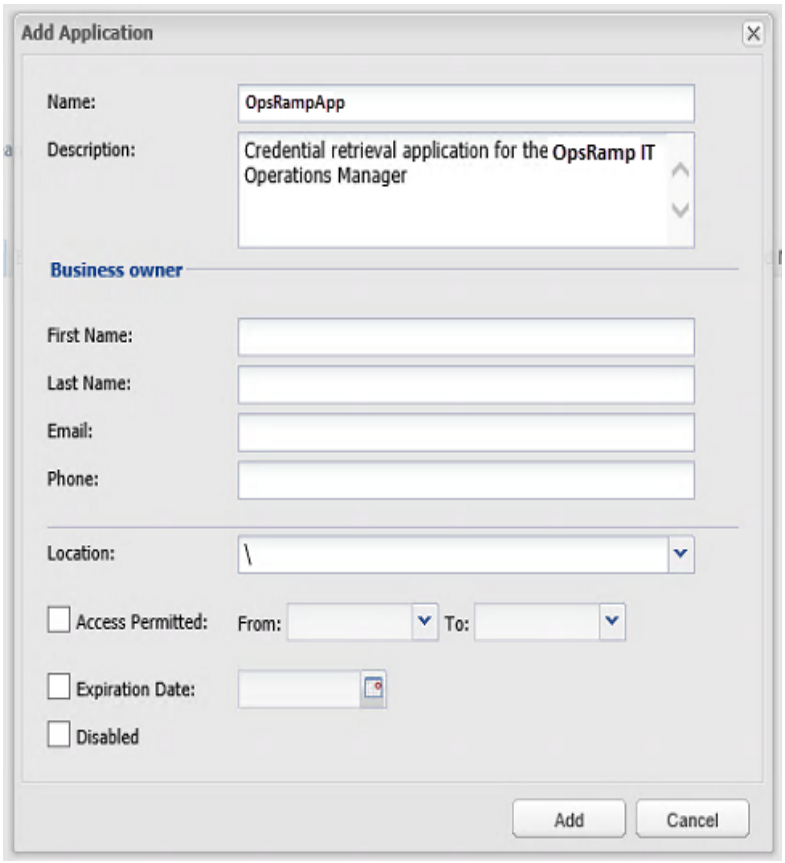
As shown in the figure above, OpsRamp's Gateway component integrates with AAM to fetch passwords, on demand, and use the password to launch a remote console session to the managed device.

AAM CONFIGURATION

DEFINING THE OPSRAMP ID (APPID) AND AUTHENTICATION DETAILS

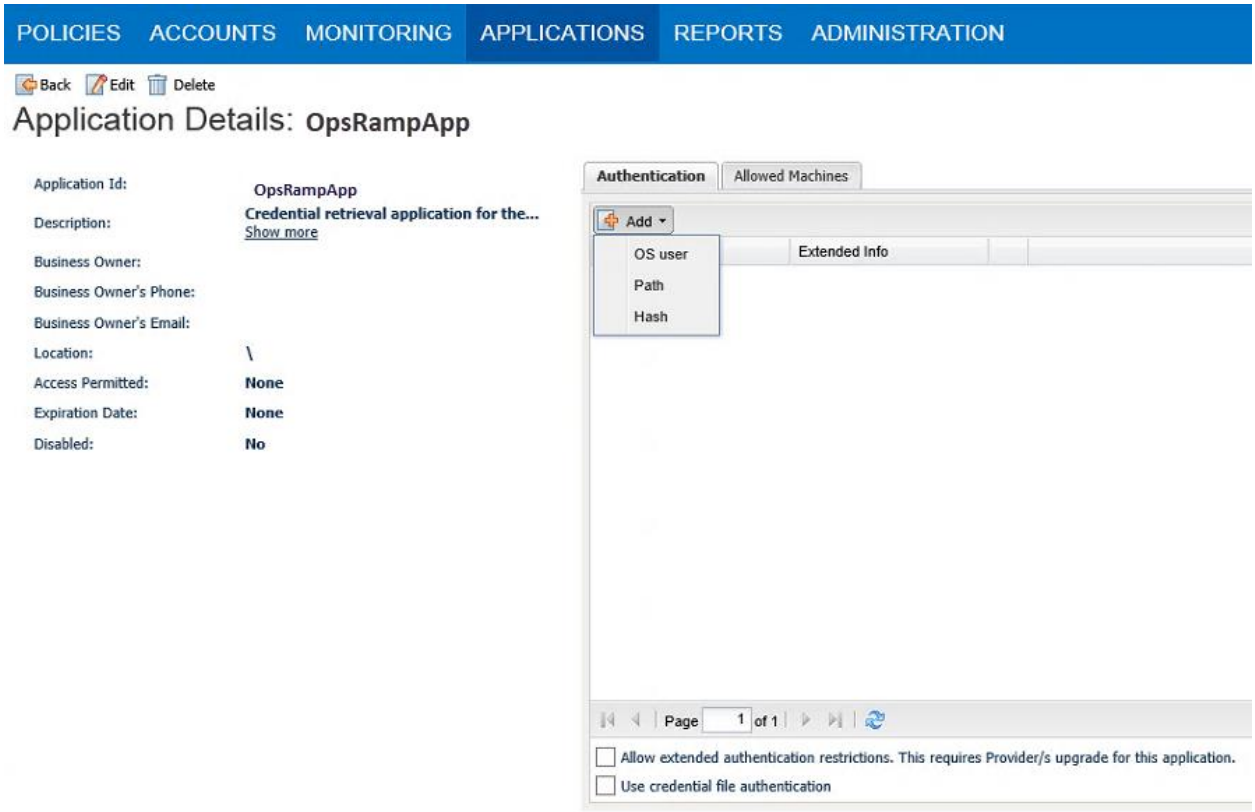
To define the Application, here are the instructions to define it manually via CyberArk's PVWA (Password Vault Web Access) Interface:

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.



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

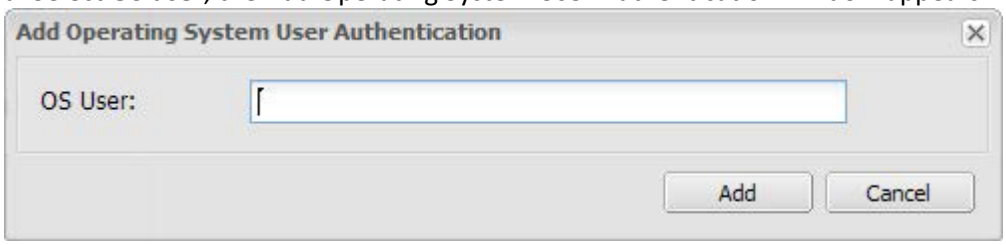
3. Click **Add**; the application is added and is displayed in the Application Details page.



- **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.

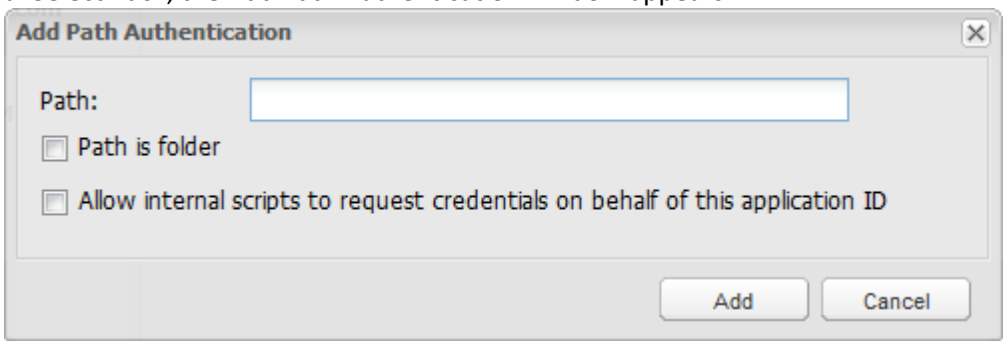
4. Specify the application's **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password.
   - In the Authentication tab, click **Add**; a drop-down list of authentication characteristics is displayed.
   - Select the authentication characteristic to specify.

5. Specify the OS user:
   a. Select **OS user**; the Add Operating System User Authentication window appears.



   b. Specify the name of the OS user who will run the application, then click **Add**; the OS user is listed in the Authentication tab.

6. Specify the application path:
   a. Select **Path**; the Add Path Authentication window appears.

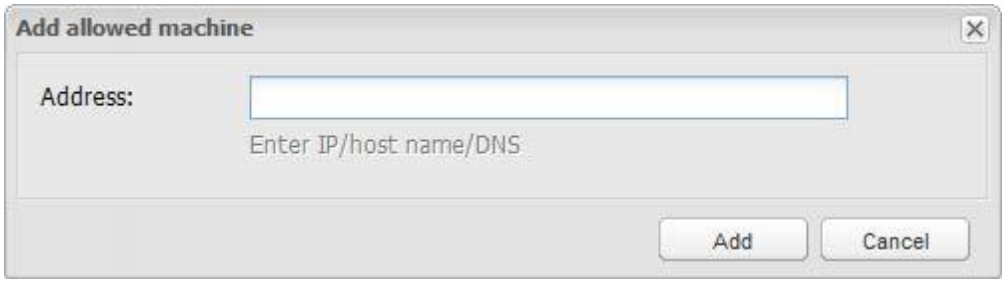


   b. Specify the path where the application will run.
   c. To indicate that the specified path is a folder, select **Path is folder**.
   d. To allow internal scripts to retrieve the application password for this application, select **Allow internal scripts to request credentials on behalf of this application ID**.
   e. Click **Add**; the Path is added as an authentication characteristic with the information that you specified.

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

   d. In the Hash edit box, paste the application's unique hash value, or secify 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.
   e. Click **Add**; the Hash is added as an authentication characteristic with the information that you specified.

8. 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.



    - Specify the IP/hostname/DNS of the OpsRamp Gateway, then click **Add**; the IP address is listed in the Allowed machines tab.
      Make sure the servers allowed include all the OpsRamp Gateways.

PROVISIONING ACCOUNTS AND SETTING PERMISSIONS FOR APPLICATION ACCESS

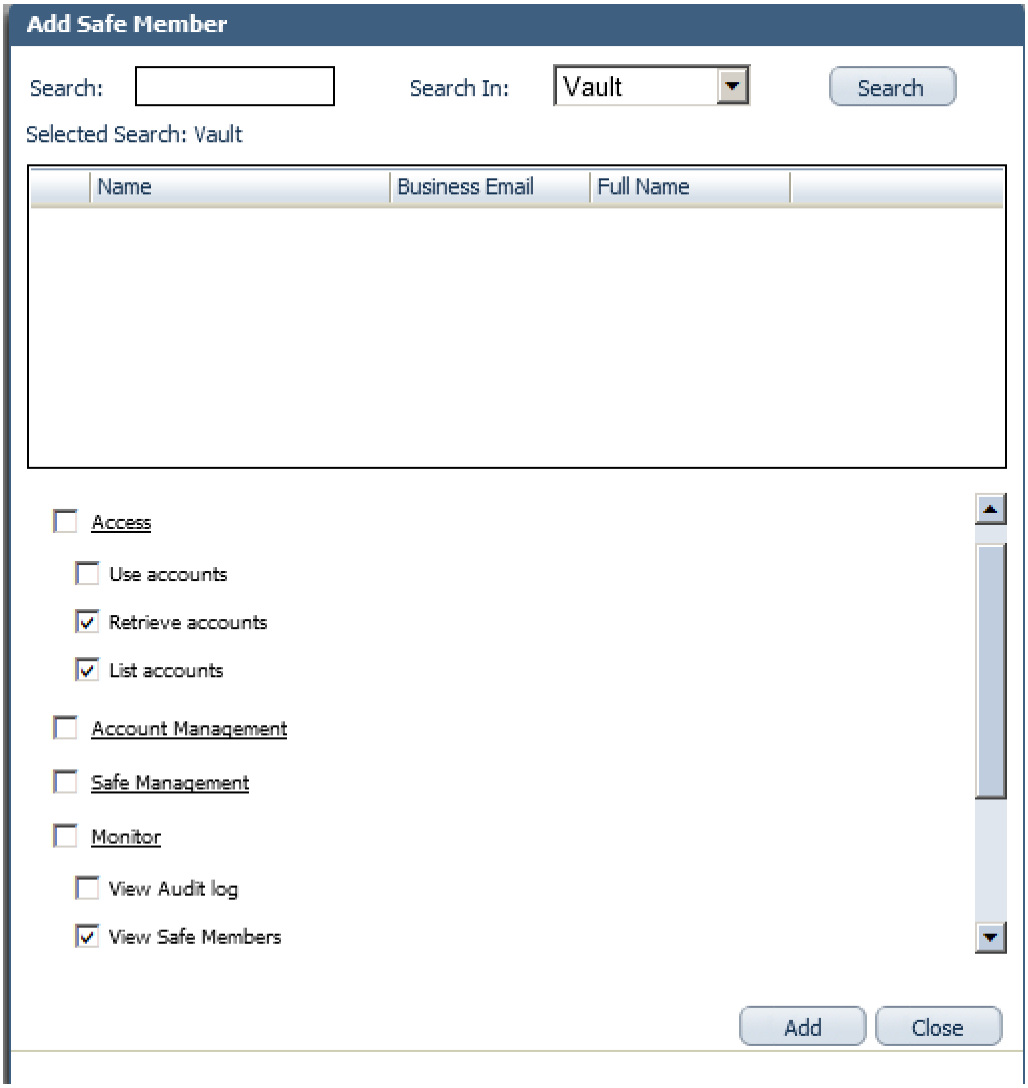
For the application to perform its functionality or tasks, the application must have access to particular existing accounts, or new accounts to be provisioned in CyberArk Vault (Step 1). Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application (Step 2).

1. In the Password Safe, provision the privileged accounts that will be required by the applications. You can either 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.

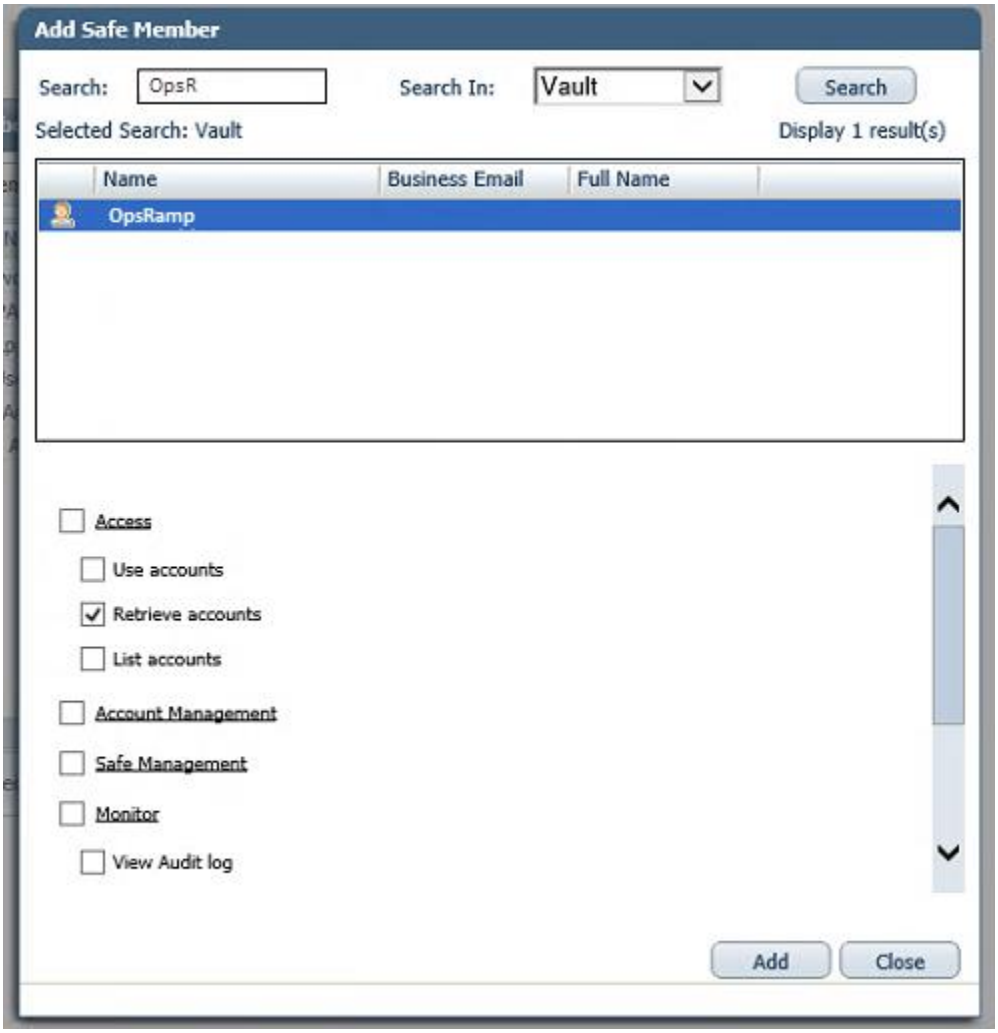
    For more information about adding and managing privileged accounts, refer to **the Privileged Access Security Implementation Guide.**

2. Add the 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:
Vault
Search
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
Add
Close

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

- Retrieve accounts



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 Access Security Implementation Guide.**

Configuration Steps for OpsRamp

1. Log into **OpsRamp**.
2. Click on the **Setup**.
3. Click on the **Integrations** and select **Client** and then click on the **Available Integrations**.
4. Click on the **Other** and then select the **CyberArk**. See figure below.

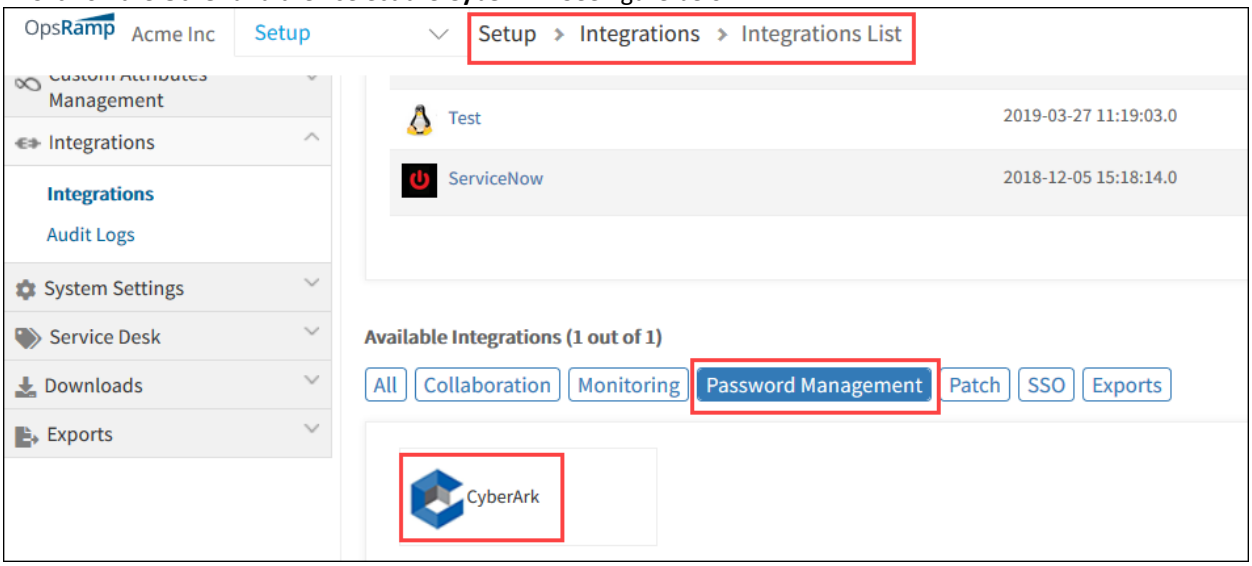


Figure 1: Available Integration- CyberArk

5. Click on the **Install** to install the CyberArk. See figure below.

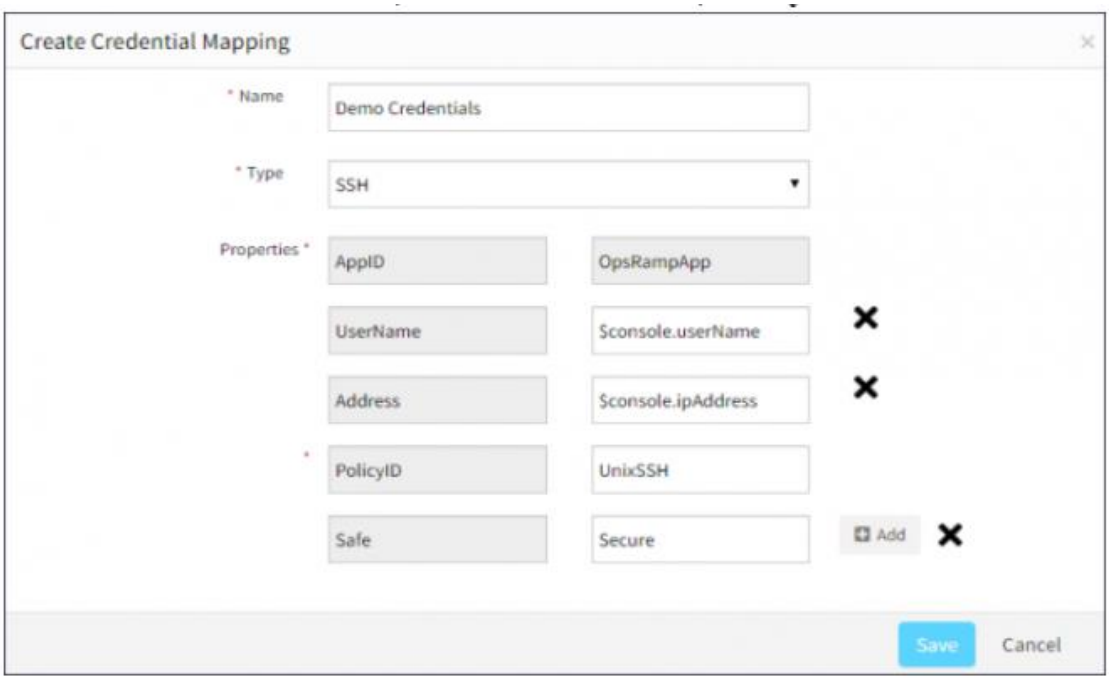
CyberArk Integration 2

Figure 2: Install CyberArk

Note: CyberArk Integration will be shown as **My Integrations** once installed.

6. Enter the details for the **Credential Mapping Configuration**

1. Name: Relevant Name
2. Type: Credential type
3. Properties: **AppID** and **PolicyID** are mandatory. You can add more properties to fetch password from



CyberArk. See figure 3.

Figure 3: Add Credentials

4. Click on the **Save**.

7. Click on the **Account Management** and then click on the **Clients** then select the client.

8. Click on the **Credentials** and then select the credential set.

9. Click on the **Edit** to map the credential sets selecting this Cyber ark mappings. See figure below.

CyberArk Integration 3

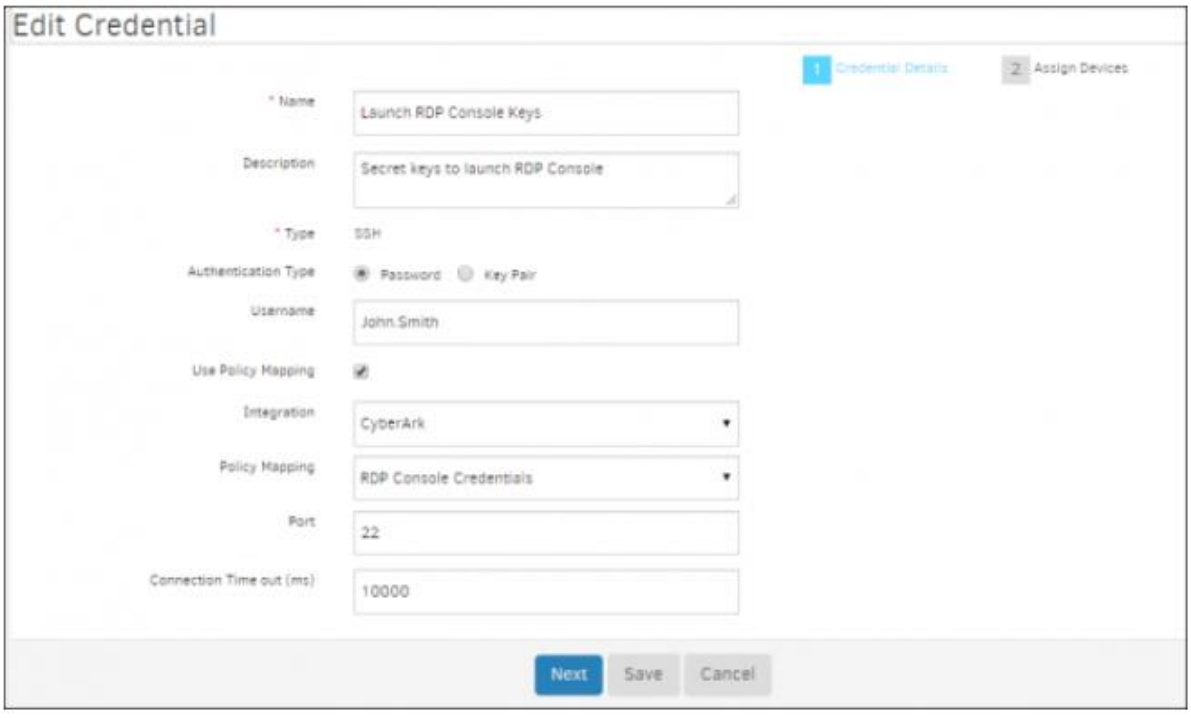


Figure 4: CyberArk Mappings

Now successfully OpsRamp is capable of integrating with CyberArk to fetch the passwords instead save credentials and allows the remote consoles and discovery profiles.

OPSRAMP CONTACT INFO

Business Contact	Name	Mahesh Ramachandran
	Email	mahesh.ramachandran@opsramp.com
	Tel	650-388-6283
Technical Contact	Name	Mahesh Ramachandran
	Email	mahesh.ramachandran@opsramp.com
	Tel	650-388-6283
Support Contact	Name	OpsRamp Support Team
	Email	support@opsramp.com
	Tel	855-847-8272