

****

CyberArk Integration

Version: v1.0

Last Updated: 19-Jun-2019

**Copyright**

Copyright © 2019 [Tecknodreams Software Consulting Pvt. Ltd.](http://www.tecknodreams.com) All Rights Reserved.

**Restricted Rights Legend**

This documentation is subject to and made available only pursuant to the terms of the Tecknodreams License Agreement and may be used or copied only in accordance with the terms of that agreement. It is against the law to copy the documentation except as specifically allowed in the agreement. This document may not, in whole or in part, be copied photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without prior consent, in writing, from Tecknodreams.

Information in this document is subject to change without notice and does not represent a commitment on the part of Tecknodreams.

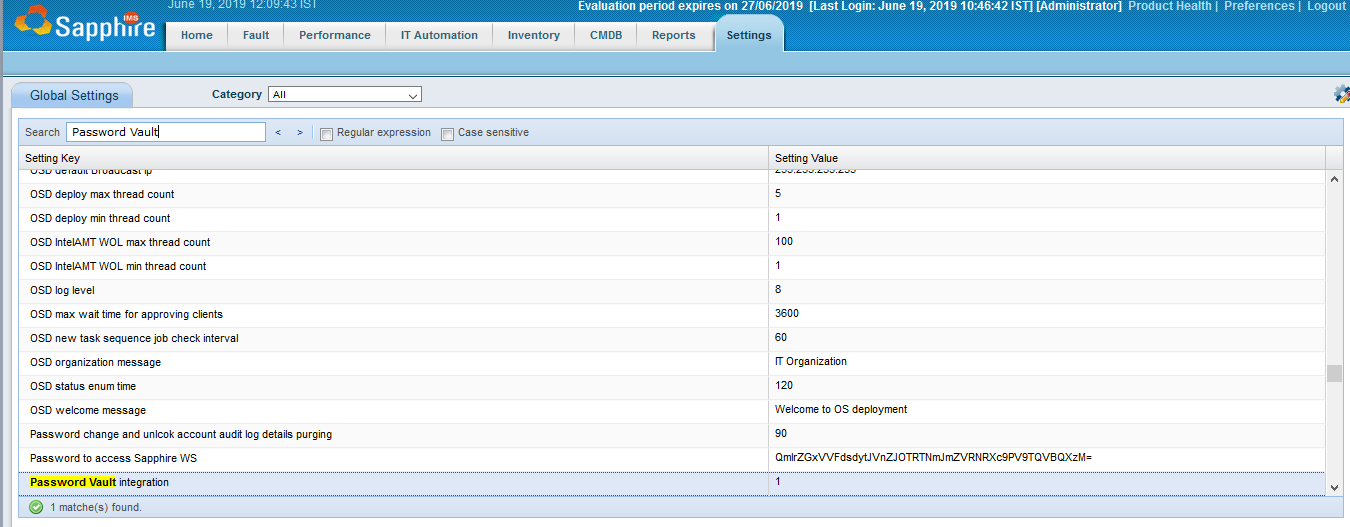
This document will explain how to integrate Password Vault to SapphireIMS

To integrate Password Vault to SapphireIMS the following steps are required

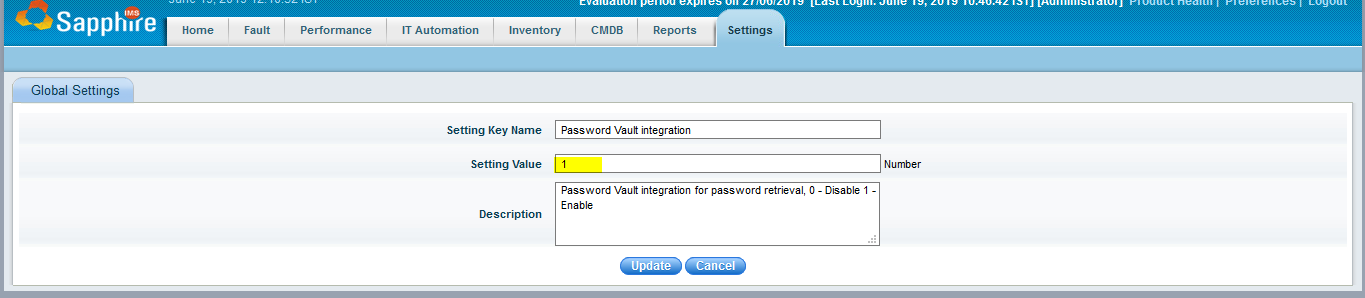
1. Enable the Password Vault from SapphireIMS application.
2. Install the ‘Password Vault Manager’ plugin on a server which has network. connectivity to the CyberArk AIM Server.
3. Configure Password Vault Configuration in SapphireIMS.
4. Configure corresponding profiles in SapphireIMS

1. Enable the Password Vault from the SapphireIMS application UI:

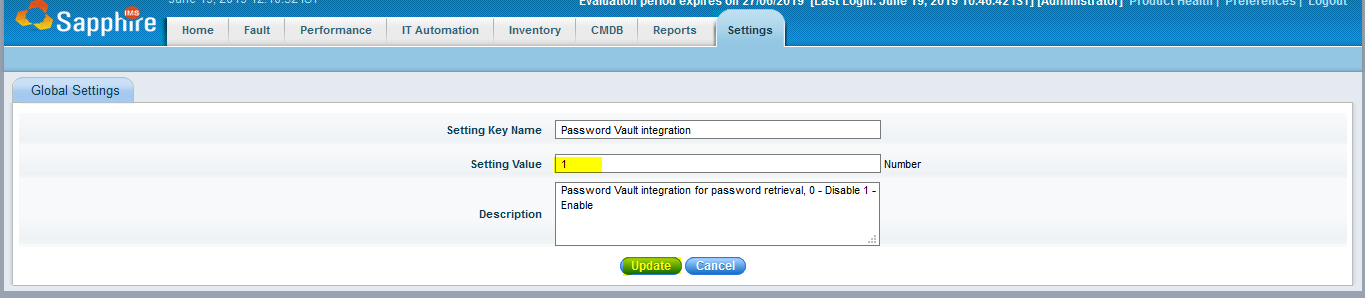
* In SapphireIMS, navigate to **Settings** > **Advanced System Settings** > **Global Settings**.
* Search for ‘**Password Vault Integration**’.



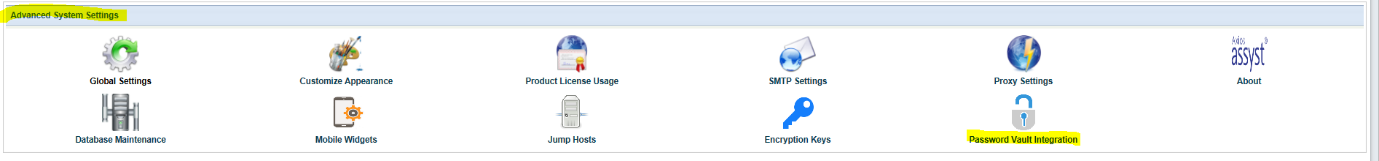
* Enable the setting key to ‘**1**’.



* Select ‘**Update**’.



* A new icon **‘Password Vault Integration’** will be visible on the settings page:



This concludes enabling the Password Vault from the SapphireIMS application UI.

1. Install the ‘**Password Vault Manager**’ plugin:

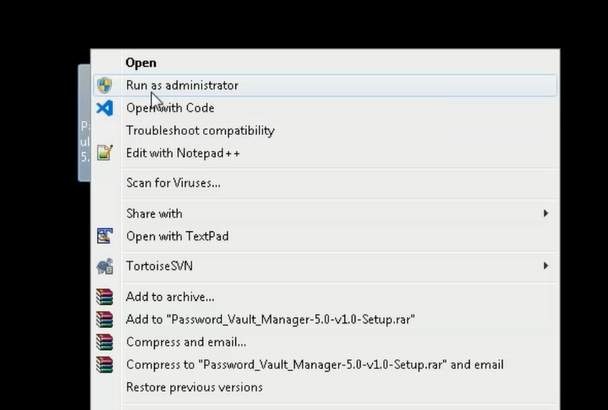
**Pre-requisites**

To install Password Vault plugin the following are the pre-requites

|  |  |  |
| --- | --- | --- |
| Processor | Memory | Free Hard Disk |
| Quad core | 2GB | 50 GB\* |

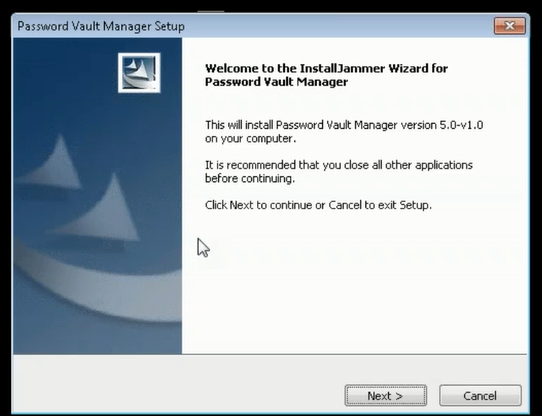
Operating Systems:

* Windows Server 2012/2012 R2
* Windows Server 2008/2008 R2
* Windows Server 2003
* Windows 10, 8, 7
* Right Select on ‘**Password\_Vault\_Manager\_5.0**’ plugin.
* Select ‘**Run as Administrator**’.

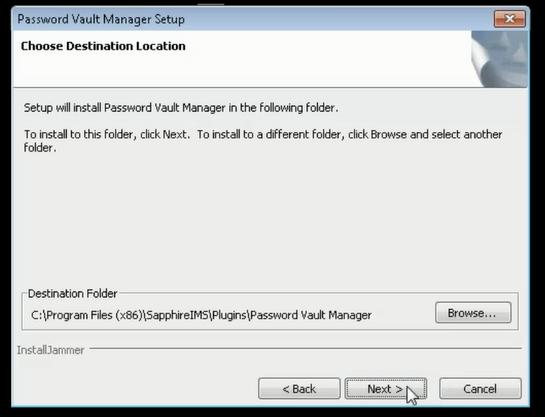




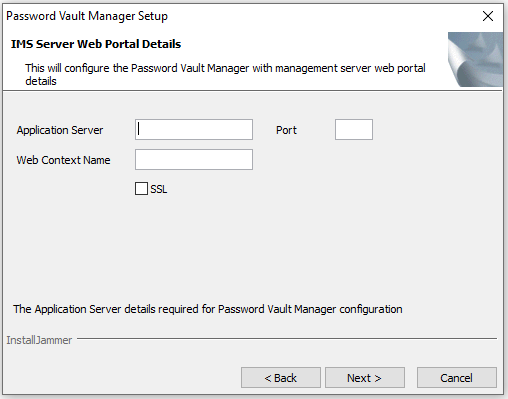
* Select **‘Yes’.**



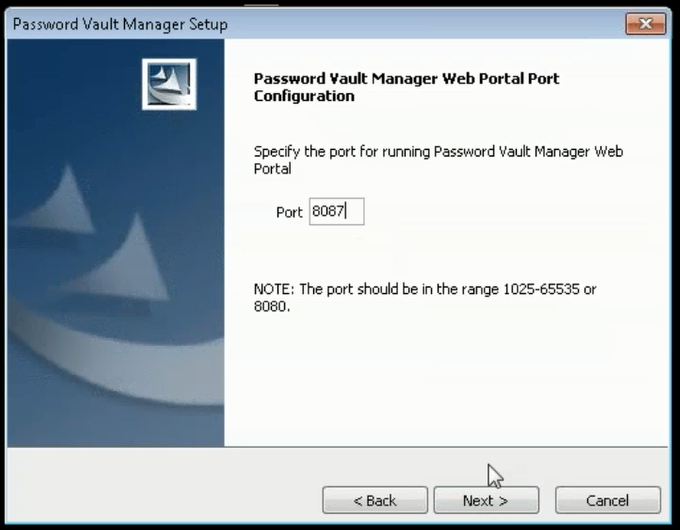
* Select **‘Next’.**



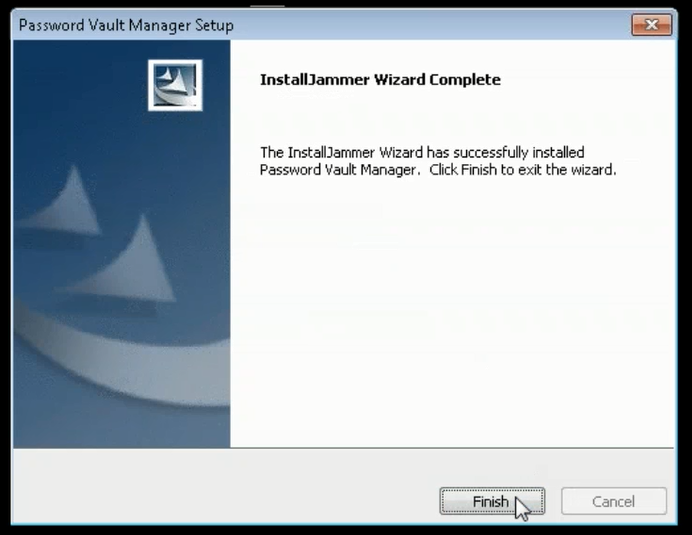
* Select ‘**Next**’.
* Configure SapphireIMS Server Web Portal details as required and Select **‘Next’.**



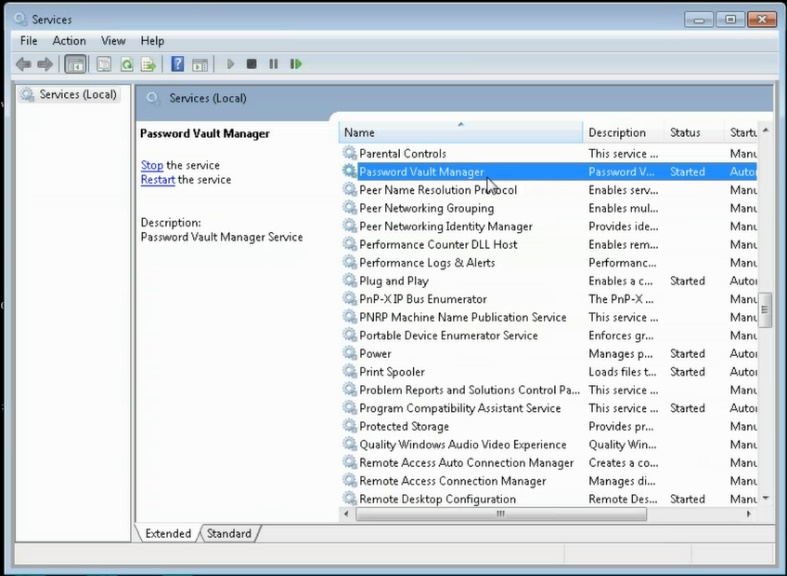
* Configure Web Portal Port Configuration details as required.
* Select ‘**Next**’.



* Select ‘**Finish**’.



* Once it is installed it will create a Service called **‘Password Vault Manager’.**



* This concludes Installing the ‘**Password Vault Manager**’ plugin.

The next step is only required if the customer is using the local credential provider SapphireIMS Password Vault Manager console. If the customer is using the local credential provider, the JAR File will need to be uploaded.

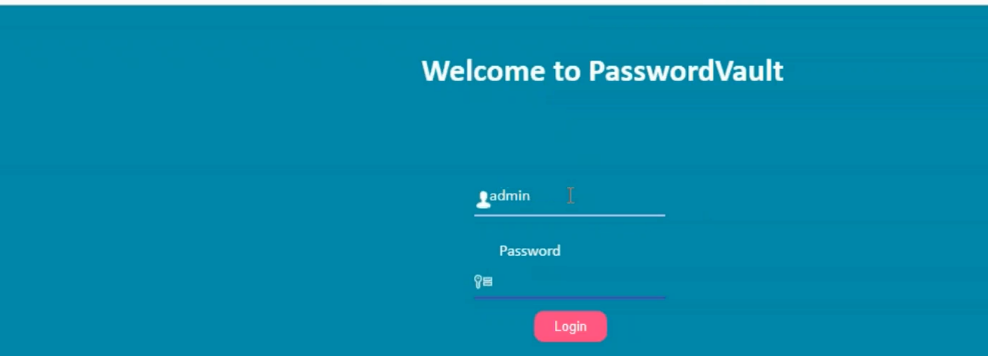
The JAR File comes from AIM local credential provider installation.

The JAR File connects to CyberArk vault to retrieve information (this is for security).

* Open an internet browser.
  + Enter the IP address or hostname of the server where the Password Vault Manager plugin has been installed following by ‘**/PasswordVault/**’. For Example:

172.16.8.180.8087/PasswordVault/

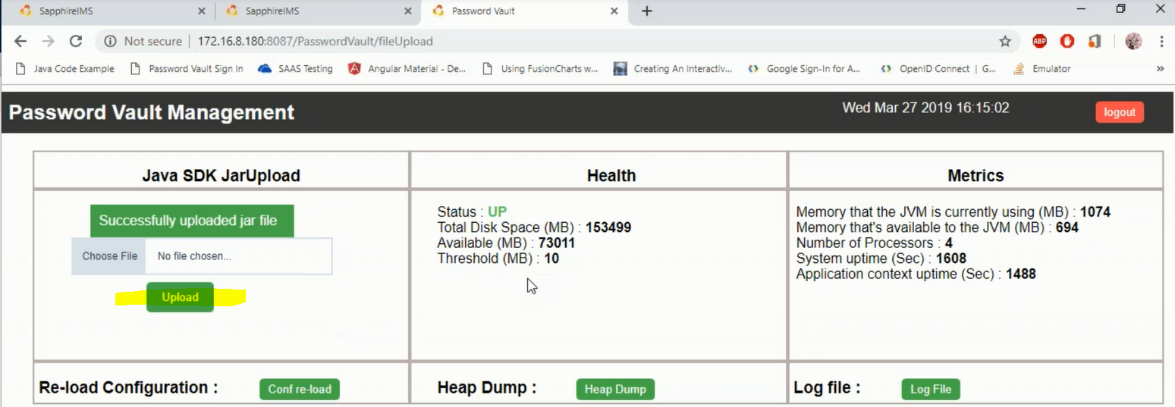
* Enter the username and password:
  + Default credentials are ‘**admin**’/’**admin**’.
  + We strongly recommend that these are changed after plugin install.



* **Once authenticated t**his will bring you to the console where was can upload the JAR file :



* From the ‘**Java SDK JarUpload**’ section select ‘**Choose File**’.
* Located the ‘**JavaPasswordsSDK.JAR**’ file from the AAM local provider folder.
* Select **‘Open**’**.**
* Then select‘**Upload**’**.**

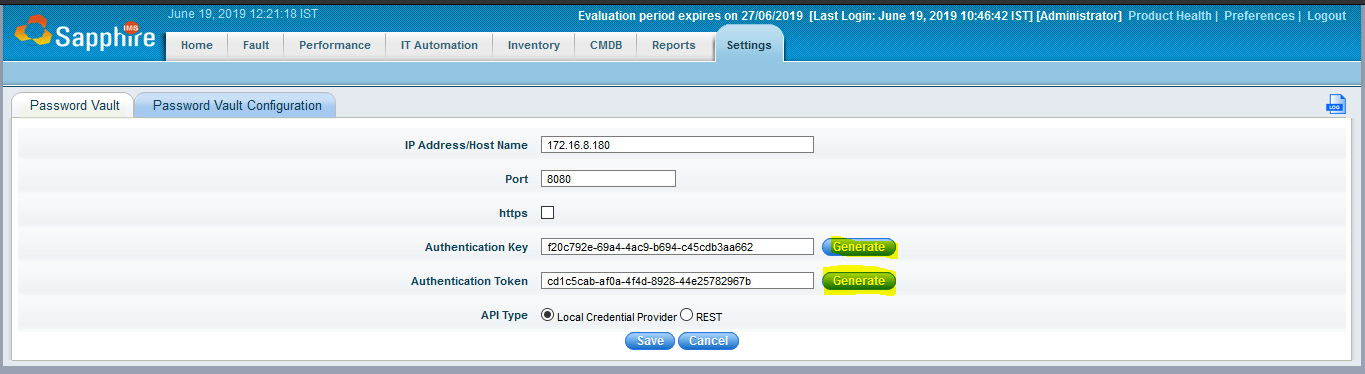


* You will see a message to confirm the upload was successful.

**Note**: this step is only required if the customer is using the local credential provider.

1. Configure Password Vault Configuration:

* In SapphireIMS, navigate to **Settings** > **Advanced System Settings** > **Password Vault Integration**.
* Select on ‘**Password Vault Configuration**’.
* Configure as required:
  + Enter the hostname of IP address of the Server where the plugin is installed.
  + Enter the port number.
  + If https was enabled during install of plugin then you need to check ‘**https**’**.**
  + The Authentication Key or Authentication Token can be entered manually, or you can select the ‘**Generate**’ button.



* Select **‘Save’.**

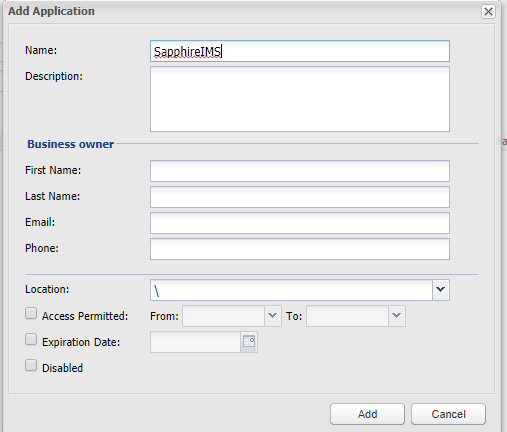
# AIM Configuration

## **Defining the application id (Appid) and authentication details**

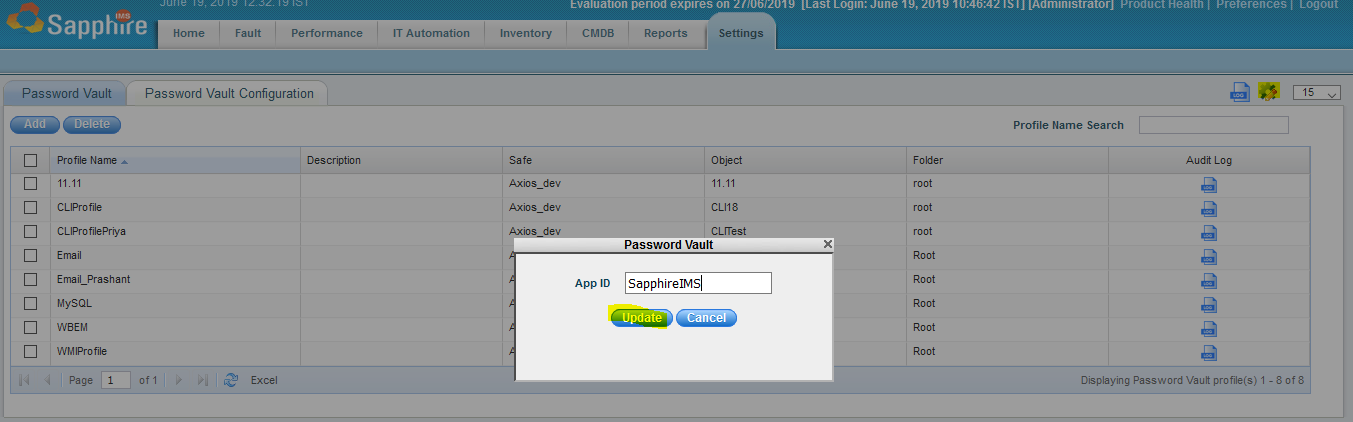
To define the Application, here are the instructions to define it manually via CyberArk’s PVWA (Password Vault Web Access) Interface:

1. Logged in as user allowed to managed applications (it requires Manage Users authorization), in the Applications tab, Select **Add Application**; the Add Application page appears.

* In CyberArk, create an Application ID.



* In SapphireIMS, navigate to **Settings** > **Advance System Settings** > **Password Vault Integration**.
* On the right-hand side, select settings and populate the App ID to reflect that which was configured in CyberArk.

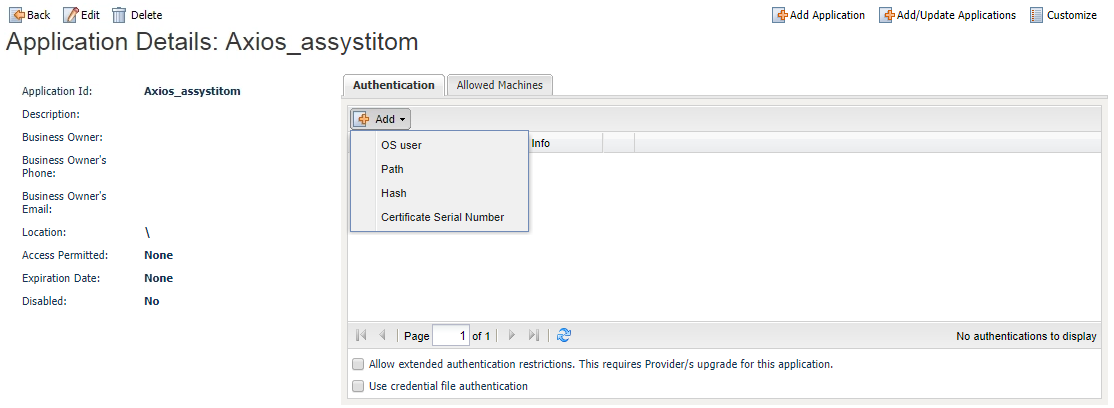


* Select ‘**Update**’

1. Specify the following information:

* In the ‘**Name**’ edit box, specify the unique name (ID) of the application. Recommended APP ID = **SapphireIMS**
* 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.

1. Select ‘**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.

1. 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, Select **Add**; the Add allowed machine window is displayed.



* Specify the IP/hostname/DNS of the machine where the application will run and will request passwords, then Select ‘**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 AAM 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:

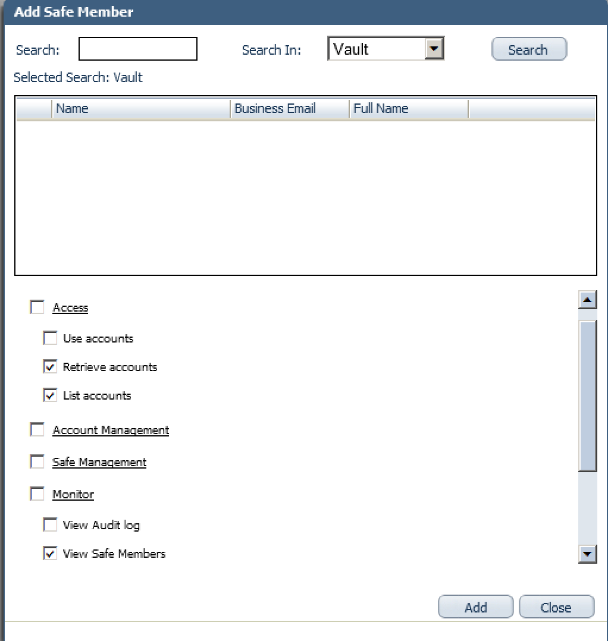
* **Manually** – Add accounts manually one at a time and specify all the account details.
* **Automatically** – Add multiple accounts automatically using the Password Upload feature.
* For this step, you require the **Add accounts** authorization in the Password Safe.

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

1. 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.
2. Add the Provider user as a Safe Member with the following authorizations:

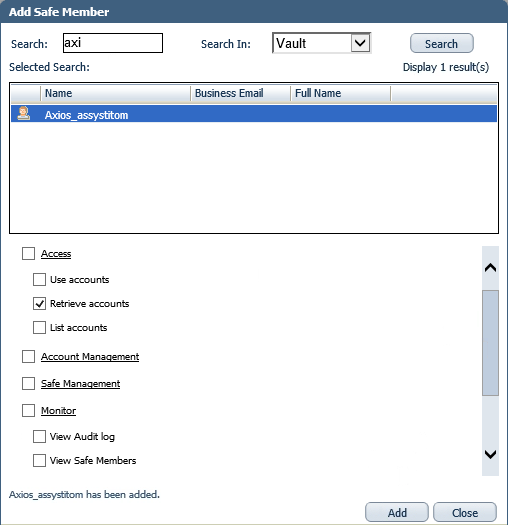
* List accounts.
* Retrieve accounts.
* View Safe Members.

**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.



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

* Retrieve accounts



1. 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**

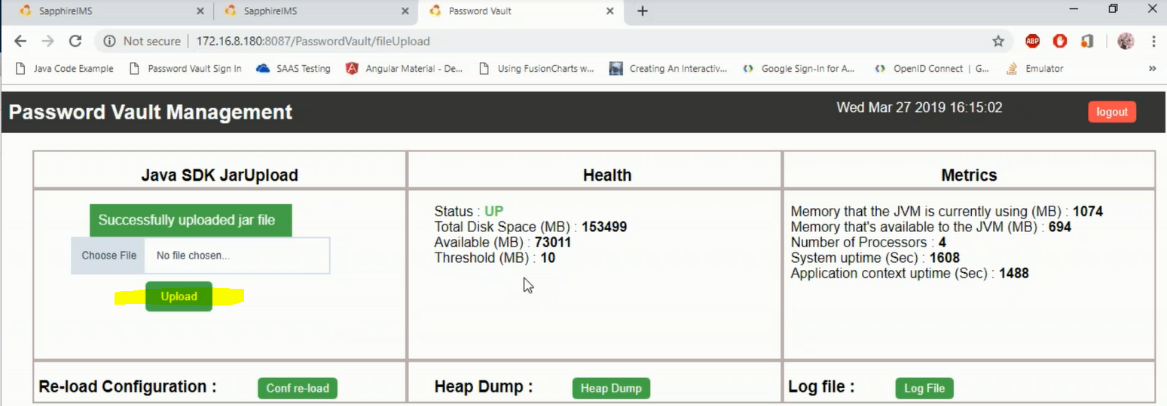
* In Privileged Account Security solutions (v8.0 and higher), when working with dual control, the Provider user can always access without confirmation, thus, it is not necessary to set this permission.

1. 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.**

* Back in the PasswordVault, perform a ‘Cong re-load’ so that the Authentication Key and Authentication Token can be re-synced. For Example:

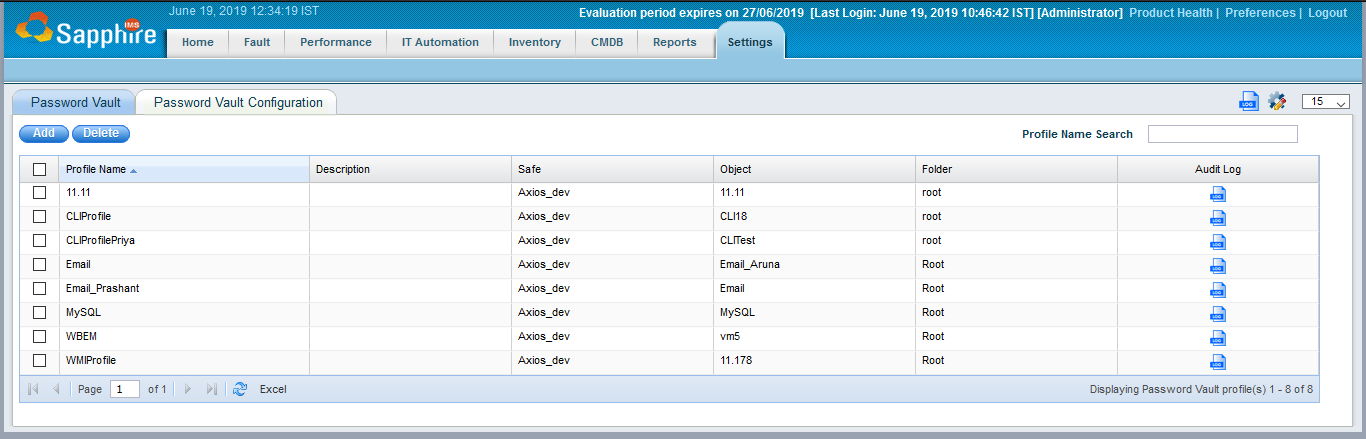
172.16.8.180.8087/PasswordVault/



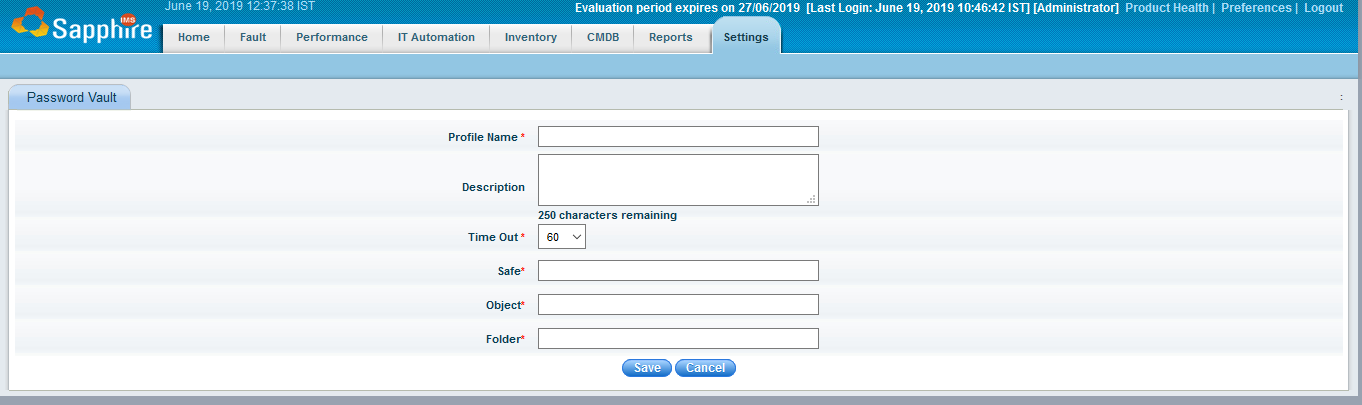
1. Configure corresponding profiles in the SapphireIMS.

**Note**: Profiles in the CyberArk vault will need to be referenced as part of this activity.

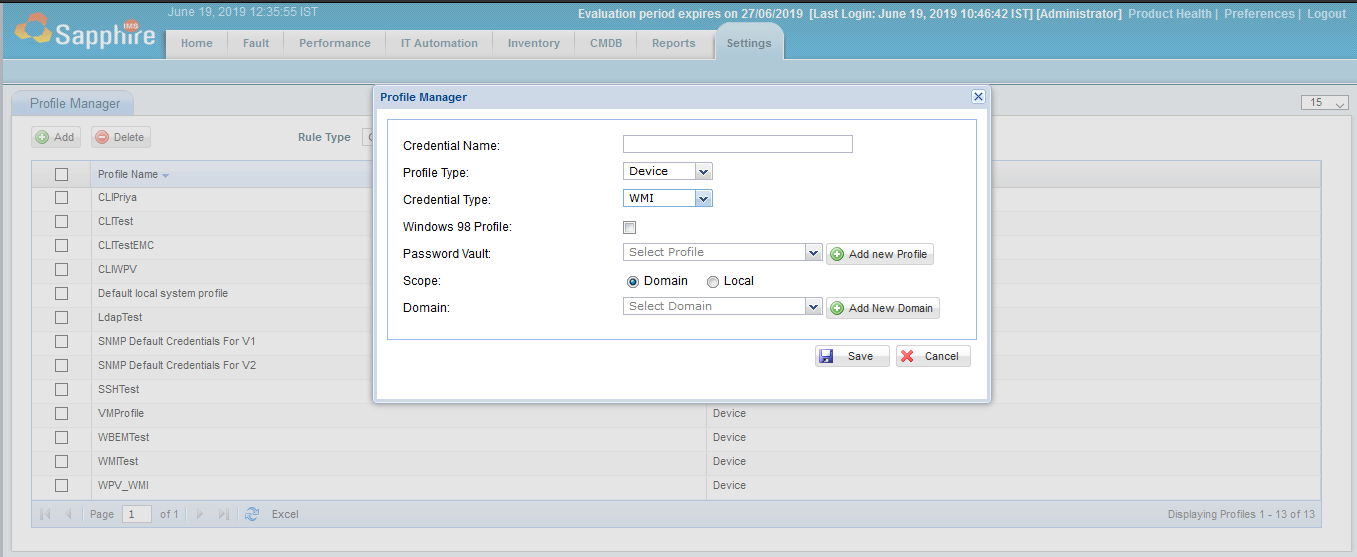
* Navigate to **Settings** > **Advanced System Settings** > **Password Vault Integration** > **Password Vault**.



* Select ‘**Add**’.
* Populate the required details accordingly:
  + Safe, Object and Folder details should reflect those configured in the CyberArk Vault.
  + Folder will be root by default unless the Profile in CyberArk vault has been saved elsewhere.



* Select **‘Save’**
* Now create a standard discovery profile in SapphireIMS. This is the first step required when discovery any devices or applications in SapphireIMS i.e. setting up the credentials which will be used during the network scan process.
* Navigate to **Settings** > **Asset and Inventory Management** > **Profile Manager**.
* Select **‘Add’.**
* Configure as required, selecting the corresponding profile in CyberArk from the Password Vault drop down.



* Populate as required.
* Select **‘Save’.**

# How to test if the credentials are configured correctly on the CyberArk end?

If CyberArk credential is not correctly resolving inside SapphireIMS, the first step is to test if the credential resolves correctly in the CyberArk end.

1. In the CyberArk AIM client folder, they should have a folder created for AppAuditLog which will show you entries for attempts made by discovery.
2. There should be a service CyberArkApplicationPassword running from the CyberArkApplication password provider.
3. On CyberArk AIM server, please navigate to the folder where the CyberArkAIM sdk is present and then run the following command:

Clipasswordsdk.exe getpassword /p appdescs.appid=”YOUR\_APP\_ID” /p query=”safe=YOUR\_SAFE\_NAME;folder=YOUR\_SAFE\_FOLDER;object=YOUR\_CREDENTIAL\_ID” /o password

Once you run this command and the credential resolves, you should see a result from the command and also in the AppAuditLog you should see the entry of this credential request made

# Steps need to taken care for existing profile after enabling PasswordVault feature:

Go to all existing credential profiles and update the Password Vault profiles respectively.

# Steps need to taken care for existing profile after disabling PasswordVault feature:

Go to all existing credential profiles and update username/password respectively.