SECRETS MANAGER INTEGRATION GUIDE

(Credential Provider CP)

DOCUMENT PURPOSE: THIS TEMPLATE IS TO BE COMPLETED BY PARTNER AND IS REQUIRED FOR CYBERARK SECURED CERTIFICATION. THE SECRETS MANAGER INTEGRATION TECHNICAL DOCUMENTATION WILL BE MADE AVAILABLE TO PARTNERS, CUSTOMERS AND PROSPECTS.

Name of Company	SecureAuth
Website	www.secureauth.com
Name of Product	SecureAuth IdP
Version	9.0.1
Date	8/01/2016

PARTNER SOLUTION OVERVIEW

SecureAuth IdP is a Windows (Windows Server 2012 R2) based appliance that provides authentication security, single sign-on and user self-service tools in a unified platform, allowing strong identity security with minimal user disruption.

KEY BENEFITS

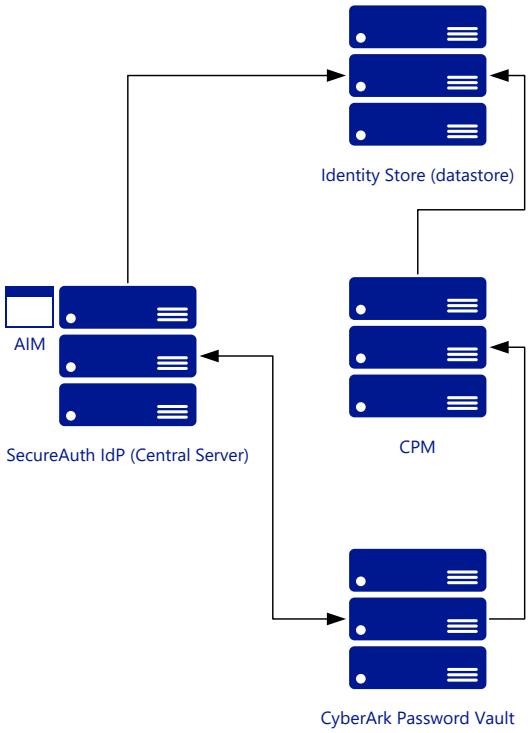
Authentication Security – With pre-authentication risk analysis, adaptive workflows, over 20 methods of multi-factor authentication and continuous authentication. SecureAuth IdP is the most comprehensive identity solution in the market.

Single Sign-On – SecureAuth IdP allows any device, with any identity type to authenticate to any identity store using any VPN to access any application – unparalleled choice and flexibility.

User Self-Service – End users can control their password resets, account unlocks, device self-enrollment and self-provisioning – reducing helpdesk workload.

Integrating with CyberArk SECRETS MANAGER, SecureAuth IdP removes the need for our joint customers to manage passwords of privileged accounts previously required to access customer identity stores (datastores).

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



SECRETS MANAGER will install directly onto the SecureAuth IdP appliance (Central Server) and when CyberArk is enabled, SECRETS MANAGER will replace the need to hardcode any service accounts passwords used in accessing identify stores (datastores) when end users' logins.

Whenever an end user authenticates to an identity store (LDAP, SQL, Oracle) and CyberArk is enabled to retrieve service account passwords, SECRETS MANAGER will be invoked to retrieve the password of the service account. Depending on the size of the customer and the number of users logging in, SECRETS MANAGER can be invoked 0-100+ times per minute.

All supported platforms can use 1-5 properties to retrieve passwords as long as any combination of the 5 properties are unique.

- Username
- Safe Name
- Folder
- Object
- Address

SECRETS MANAGER INSTALLATION

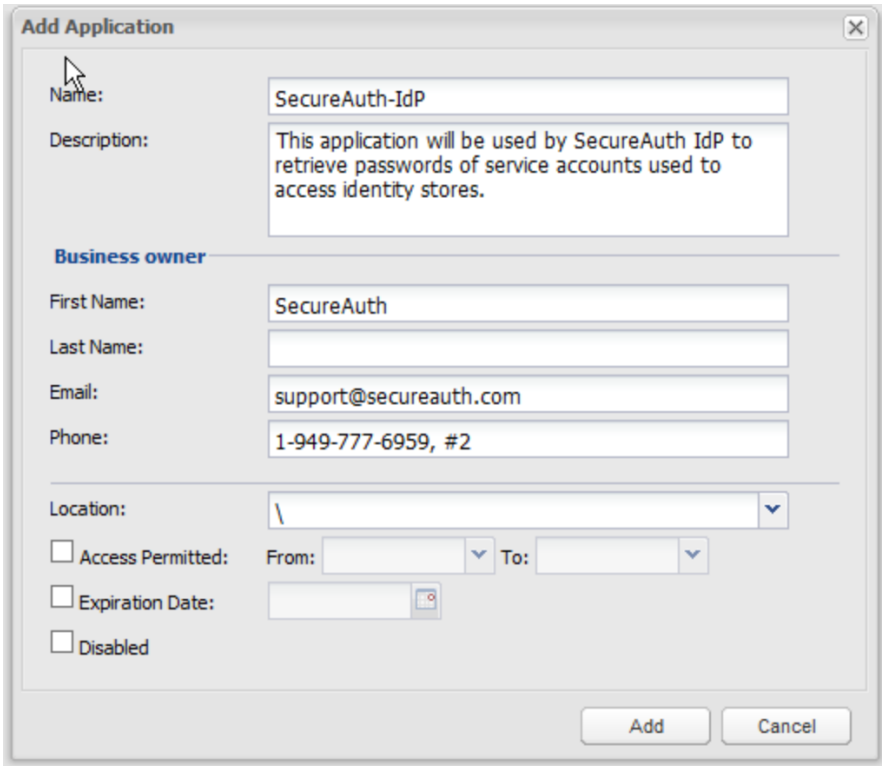
Refer to “Credential Provider and ASCP Implementation Guide” for CyberArk Credential Provider installation.

SECRETS MANAGER 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:

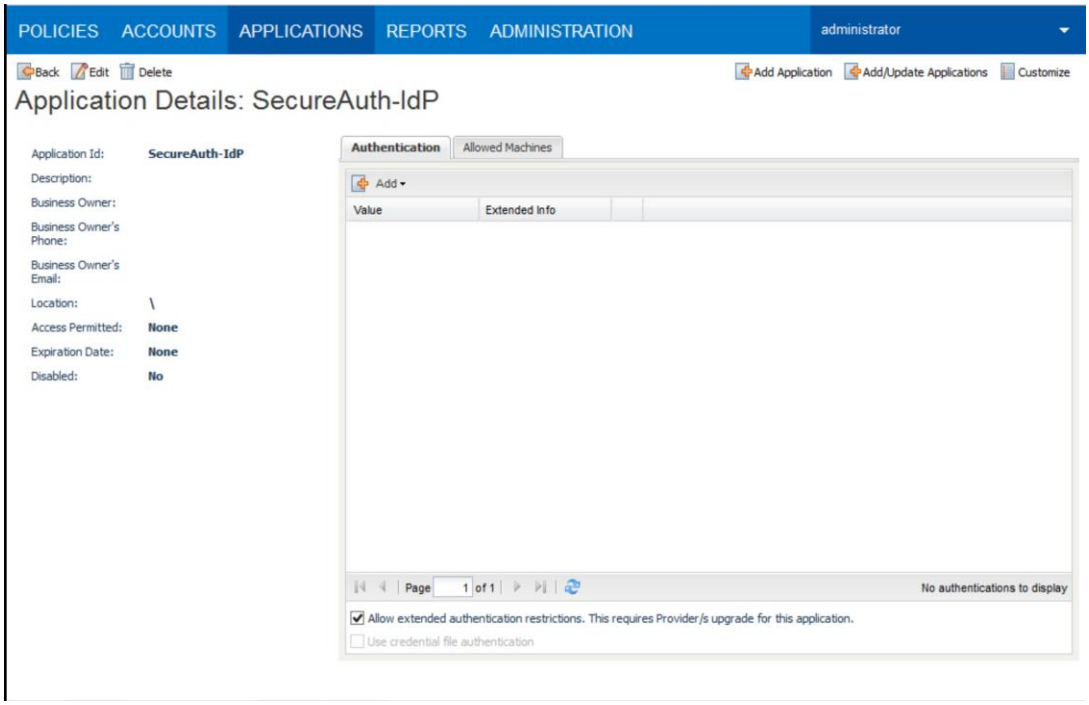
1. Logged in as user allowed to managed applications (it requires Manage Users authorization), in the Applications tab, click **Add Application**; the Add Application page appears.



2. Specify the following information:
    - In the Name edit box, specify **SecureAuth-IdP**
    - 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.

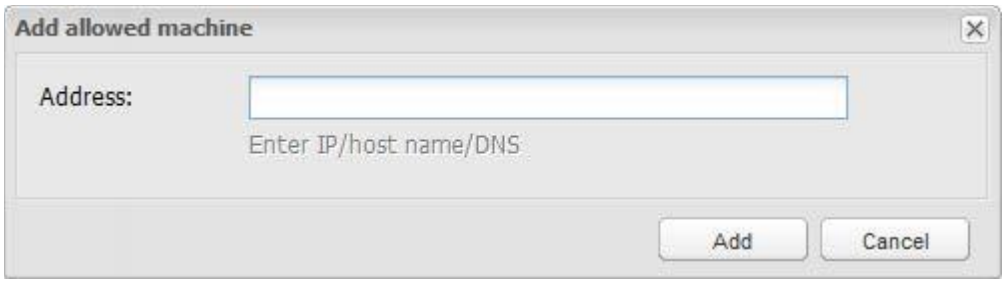
3. Click **Add**; the application is added and is displayed in the Application Details page.



- **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 SecureAuth-IdP **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password. SecureAuth recommends using the IP address of the SecureAuth IdP appliance where the SECRETS MANAGER Credentials Provider was installed to add another layer of security.

5. 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 SecureAuth IdP appliance where SECRETS MANAGER was installed, then click **Add**; the IP address is listed in the Allowed machines tab.

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).

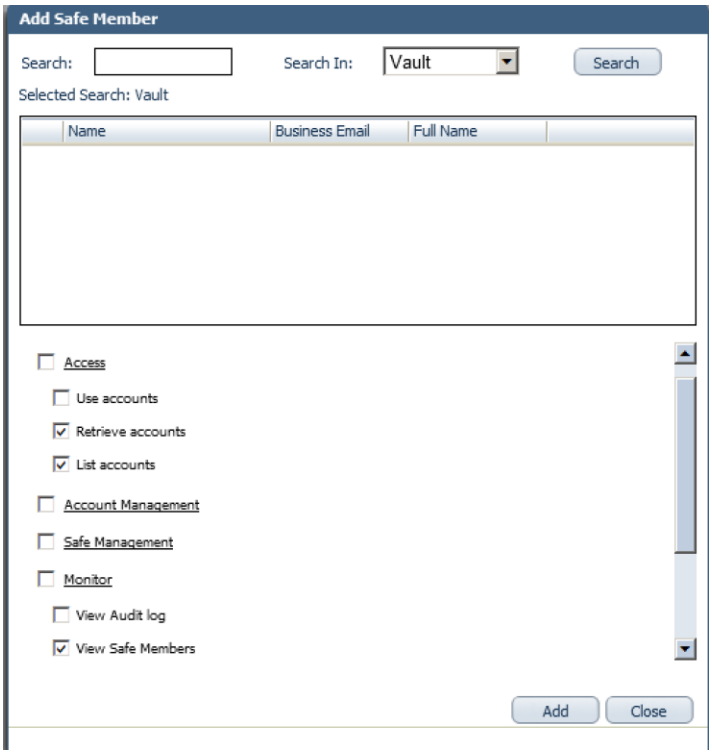
1. In the Password Safe, provision the privileged accounts that will be required by the applications. You can either do this in either of the following ways:
   - **Manually** – Add accounts manually one at a time, and specify all the account details.
   - **Automatically** – Add multiple accounts automatically 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 Account Security Implementation Guide.**

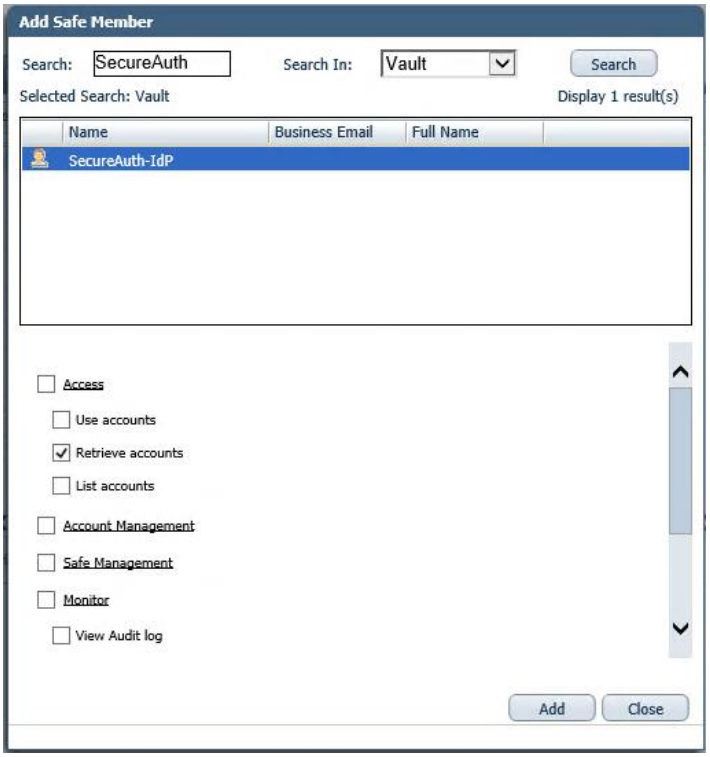
2. Add the Credential Provider and application users as members of the Password Safes where the application passwords are stored. This can either be done manually in the Safes tab, or by specifying the Safe names in the CSV file for adding multiple applications.
   i. Add the Provider user as a Safe 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.



ii. Add the application(**SecureAuth-IdP**) 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.

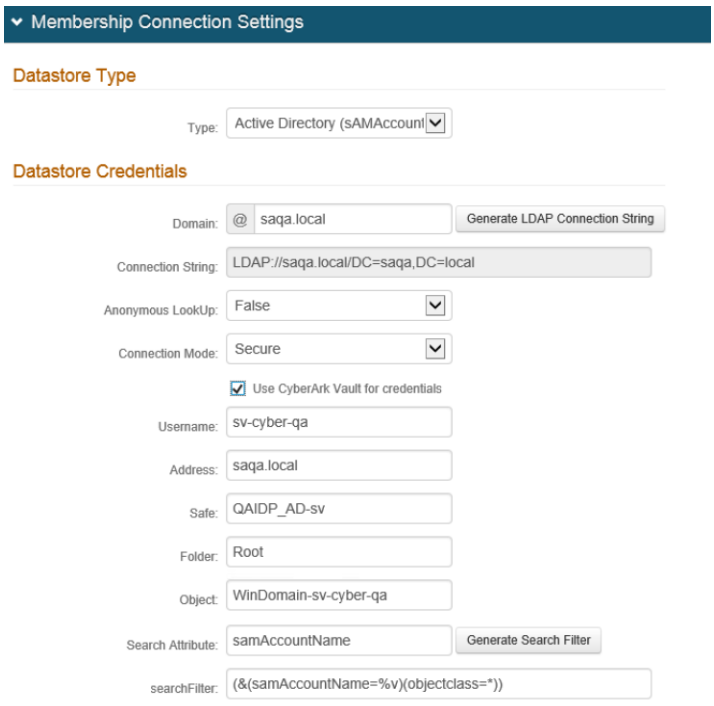
For more information about configuring Safe Members, refer to the **Privileged Account Security Implementation Guide.**

PARTNER PRODUCT INSTALLATION & CONFIGURATION

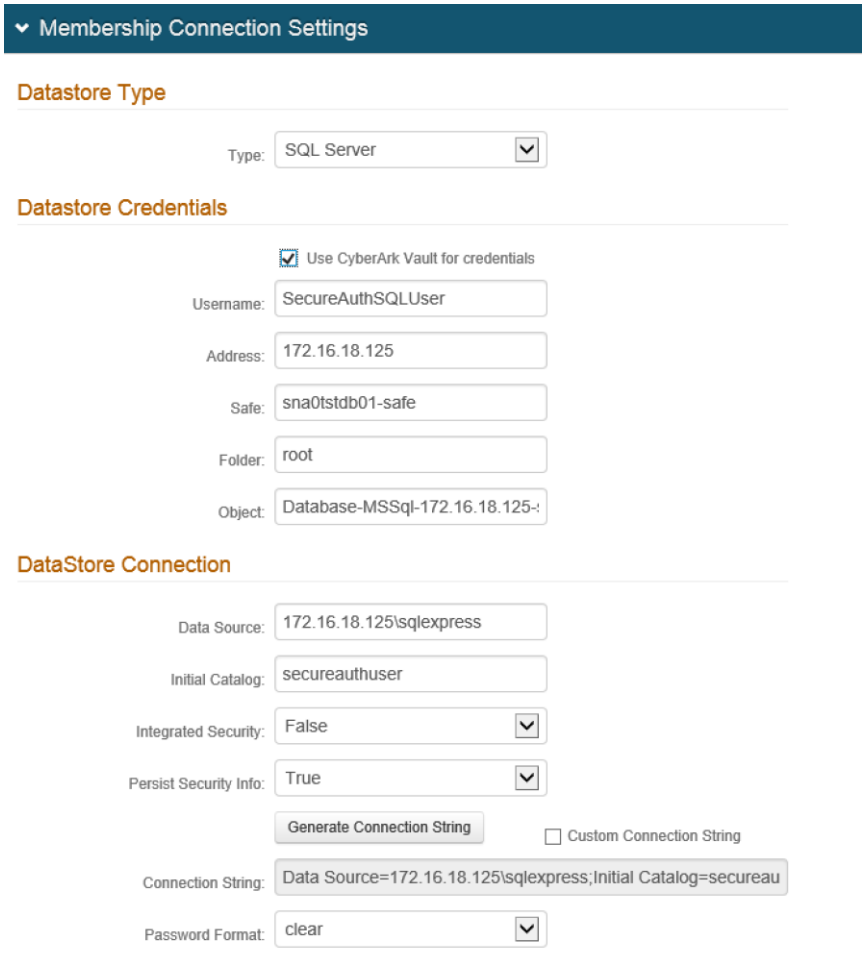
Refer to (https://docs.secureauth.com/display/90docs/Getting+Started+Guide+for+9.0) for SecureAuth IdP installation.

Common use cases:

1. Windows domain credentials or other standard credentials
   a. The user will specify: username, address
   b. Safe name, Folder, Object – optional but recommended for increasing performance



2. Database accounts (SQL/Oracle)
    a. The user will specify: username & address
    b. Safe name, Folder, Object – optional but recommended for increasing performance



PARTNER CONTACT INFO

Business Contact	Name	Mike Desai
	Email	mdesai@secureauth.com
	Tel	
Technical Contact	Name	Ian Barnett
	Email	ibarnett@secureauth.com
	Tel	
Support Contact	Name	https://support.secureauth.com
	Email	support@secureauth.com
	Tel	+1-866- 859-1526