APPLICATION ACCESS MANAGER

AMDOCS ATOMIQ PAM GATEWAY AND CYBERARK CENTRAL CREDENTIAL PROVIDER (CCP) AAM INTEGRATION

DOCUMENT PURPOSE: THIS DOCUMENT PROVIDES DETAILS OF AMDOCS ATOMIQ PAM GATEWAY INTEGRATION WITH CYBERARK AAM (CCP).

Name of Company - Amdocs Software Solutions LLP

Website - www.amdocs.com

Name of Product - Amdocs atomIQ PAM Gateway

Version - v1.0

Date - 28-09-2020

PARTNER SOLUTION OVERVIEW

Amdocs atomIQ PAM gateway v1.0 is a REST API based solution to integrate the client applications, which requires to access remote servers, databases, applications, with CyberArk PAM AAM Central Credential provider.

The Client application, hosted on a Linux machine, docker or kubernetes, calls the REST API of the gateway with the parameters to query the vault. The gateway connects with CyberArk AAM Central Credential Provider and retrieved the password and returns to the client application.

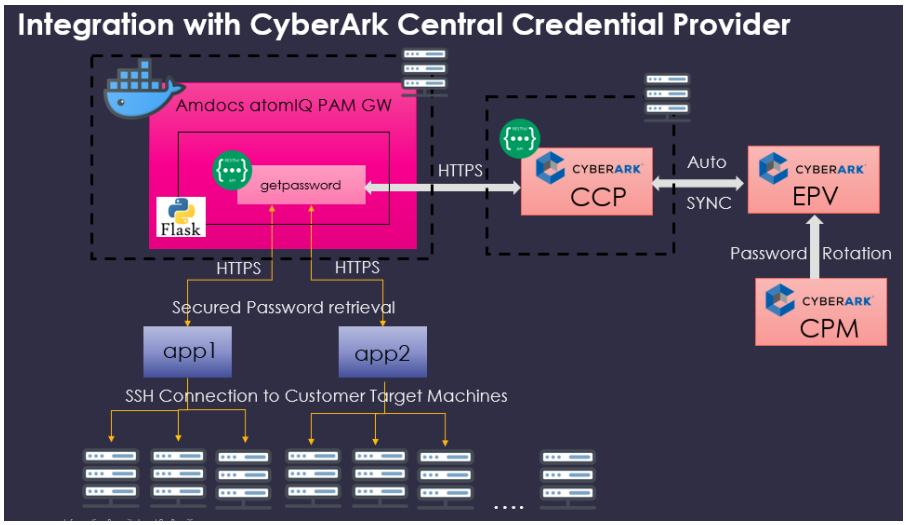
In case of Central Credential Provider, the gateway could be hosted on a different machine.

KEY BENEFITS

The key benefits of Amdocs atomIQ PAM gateway is that it is a REST API based solution, that makes it compatible with any type of client application (Java, Python, etc). The gateway is a single point of contact for many components within the client application, which requires to talk to CyberArk Central Credential provider to retrieve the password of remote servers.

The Gateway is lightweight Python Flask application and can be easily enhanced to be highly scalable and available.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



Amdocs atomIQ PAM GW could be installed either on same machine or on separate machine with CCP. The gateway is certified with python3.7 on REHL as well as Windows 10. The client application (shown as app1 and app2 in diagram above), which requires to connect to remote host (Protected by CyberArk PAM), calls REST API of the gateway with parameters like username & password or just the Account name/Object name. The gateway gets the parameters, validates and send REST API GET request to CCP to query for the password. The response from CCP is then structured into a json and sent back to the client application.

AAM INSTALLATION

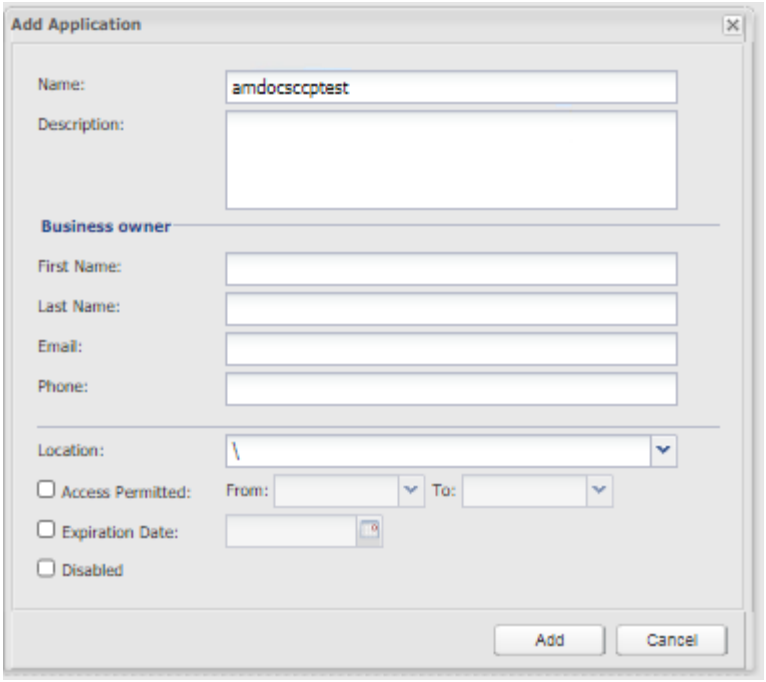
Refer to the “Central Credential Provider Implementation guide” for Agentless installation and configuration.

AAM CONFIGURATION

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

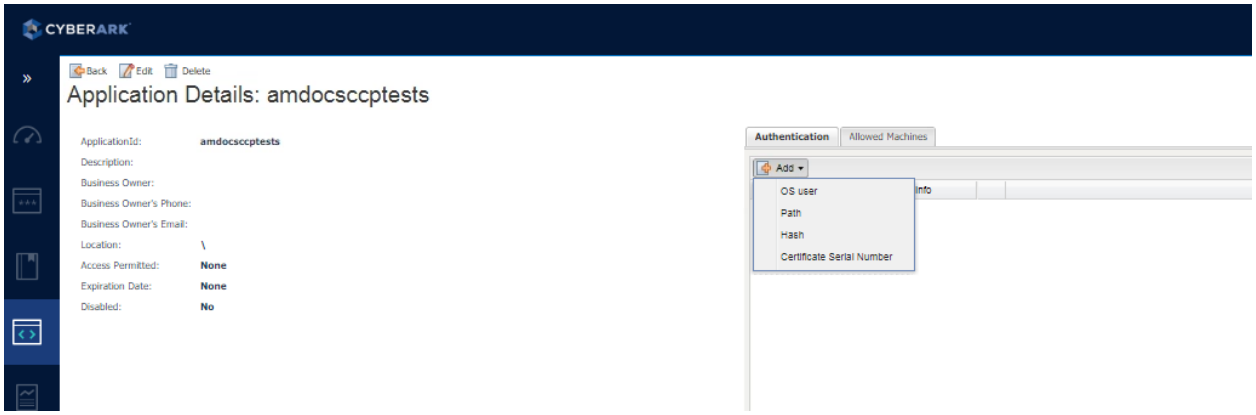
To define the Application, here are the instructions to define it manually via CyberArk’s PVWA (Password Vault Web Access) Interface:

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.



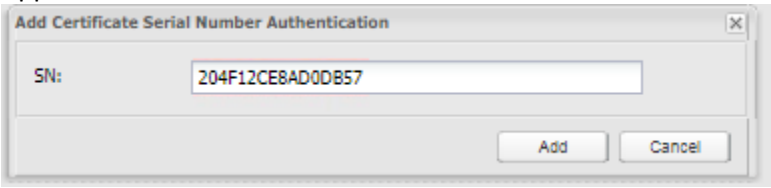
2. Specify the following information:
    - In the Name edit box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: APP ID = amdocsccptest
    - In the Description, specify a short description of the application that will help you identify it.
    - 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 Certificate Serial number:
   a. When using the Agentless AAM (Central Credential Provider) there's an option to protect the Application ID with a client certificate serial number:



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).

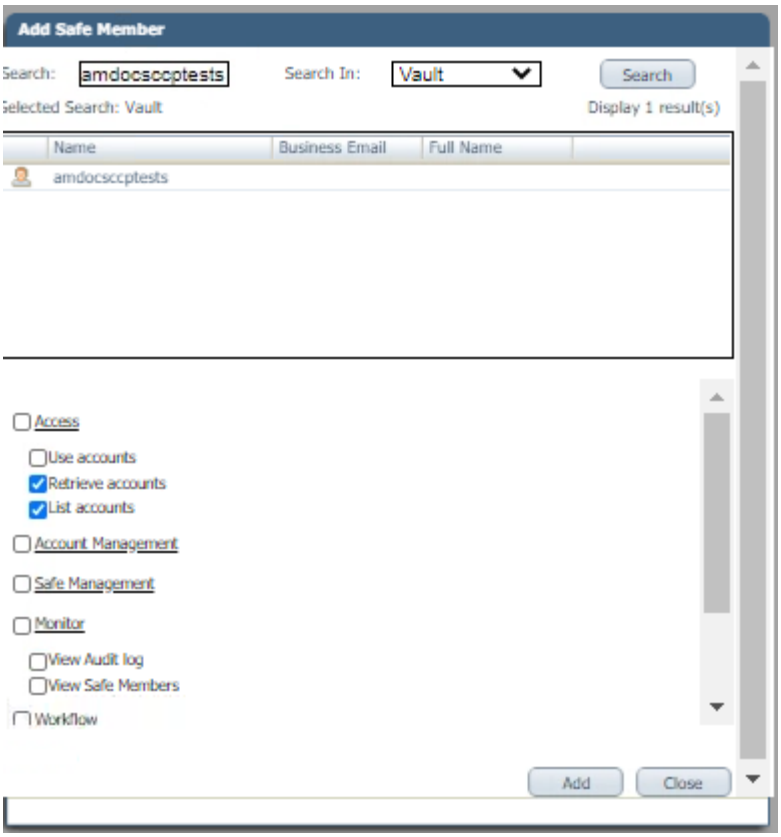
1. In the Password Safe, provision the privileged accounts that will be required by the application. You can do this in either of the following ways:
   - **Manually** – Add accounts manually one at a time, and specify all the account details.
   - **Automatically** – Add multiple accounts automatically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

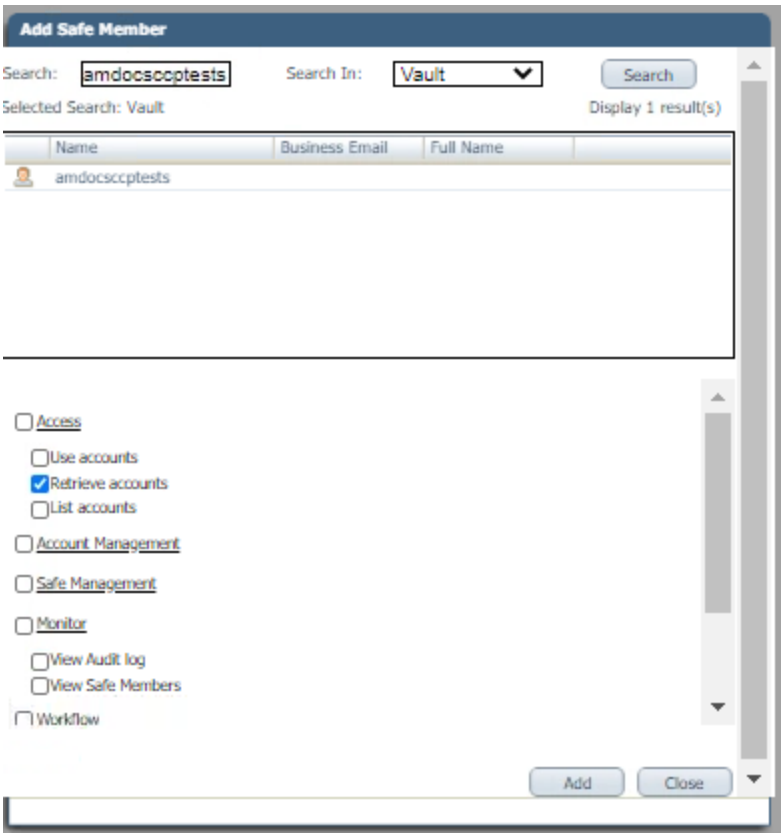
2. Add the Credential Provider and application users as members of the Password Safes where the application passwords are stored. This can either be done manually in the Safes tab, or by specifying the Safe names in the CSV file for adding multiple applications.
   i. Add the Provider user as a Safe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

- Retrieve accounts



iii. If your environment is configured for dual control:

- In Privileged Account Security solutions, 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

Parameter	Default Value	Description
LOG_LEVEL (available in settings.py)	logging.INFO	The level of logging. Valid values are: a. logging.INFO (default) b. logging.ERROR c. logging.DEBUG d. logging.CRITICAL e. logging.WARNING
SLEEP_TIME	20	Time for which the Gateway will wait before next retry when password change is in progress
RETRY_COUNT	5	Number of retries the Gateway will make if password change is in progress
cyb_install_type	CP	Type of AAM to access. Valid values are: a. CCP b. CP
cyb_appid		The secret for authentication between PAM gateway and AAM
port	5000	The port on which the PAM Gateway server is running

API GUIDE

key	defaults	Mandatory YES/NO	Description
object	''	YES either username or Object must be specified	Corresponds to Account Name in Password Vault
safe	''	NO	safe name in the Password Vault
folder	''	NO	Folder of the safe in Password Vault
username	''	YES either username or Object must be specified	username for which Password needs to be retrieved
address	''	NO	The hostname for the remote server to connect

database	''	YES	for Querying Database password
Port	""	NO	Database Port

- Any Application required to connect to remote host, protected by CyberArk PAM, calls REST API of Amdocs atomIQ PAM GW with parameters like username & password or just the Account name/Object name.
- The Amdocs atomIQ PAM GW forwards the request to CyberArk AAM with required Authentication and returns the response back to the calling application.

Common use cases:

1. User needs to connect to remote machine via SSH Username and Password
    a. The user will specify username & Address to the Gateway
    b. Safe name – optional but recommended for increasing performance
    c. The Gateway will GET request to CCP REST API with the username and address parameters.
    d. The response of CCP API will be captured by the gateway and sent back to the user.
2. User needs to connect to remote machine via SSH Username and Password
    a. The user will specify: Account Name to the Gateway
    b. Safe name – optional but recommended for increasing performance
    c. The Gateway will GET request to CCP REST API with the username and address parameters.
    d. The response of CCP API will be captured by the gateway and sent back to the user.
3. User needs to connect to Database
    a. The user will specify username, Address & Database name to the Gateway
    b. Safe name – optional but recommended for increasing performance
    c. The Gateway will GET request to CCP REST API with the username, Address & Database name parameters.
    d. The response of CCP API will be captured by the gateway and sent back to the user.

PARTNER CONTACT INFO

Business Contact	Name	Tali Kolko
	Email	Tali.kolko@amdocs.com
	Tel	
Technical Contact	Name	Navneet B R
	Email	Navneet.br@amdocs.com
	Tel	
Support Contact	Name	Chandrahas Gaikwad
	Email	Chandrahas.Gaikwad@amdocs.com
	Tel	