SECRETS MANAGER

FLEXDEPLOY AND SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company - Flexagon

Website – http://www.flexagon.com

Name of Product - FlexDeploy

Version – 9.0.0.0

Date – 1/1/2025

Commented [EM1]: Update the date

FLEXDEPLOY OVERVIEW

FlexDeploy is a purpose-built DevOps platform for Enterprise Software Technologies that accelerates software delivery and enhances quality, while minimizing risks and complexities in enterprise environments.

FlexDeploy optimizes Oracle Technologies, such as Fusion Applications, Cloud Integration, E-Business Suite, and Database, Salesforce, and SAP.

FlexDeploy also strengthens audit and compliance processes through an auditable CI/CD pipeline, ensuring adherence to industry standards and regulations.

KEY BENEFITS

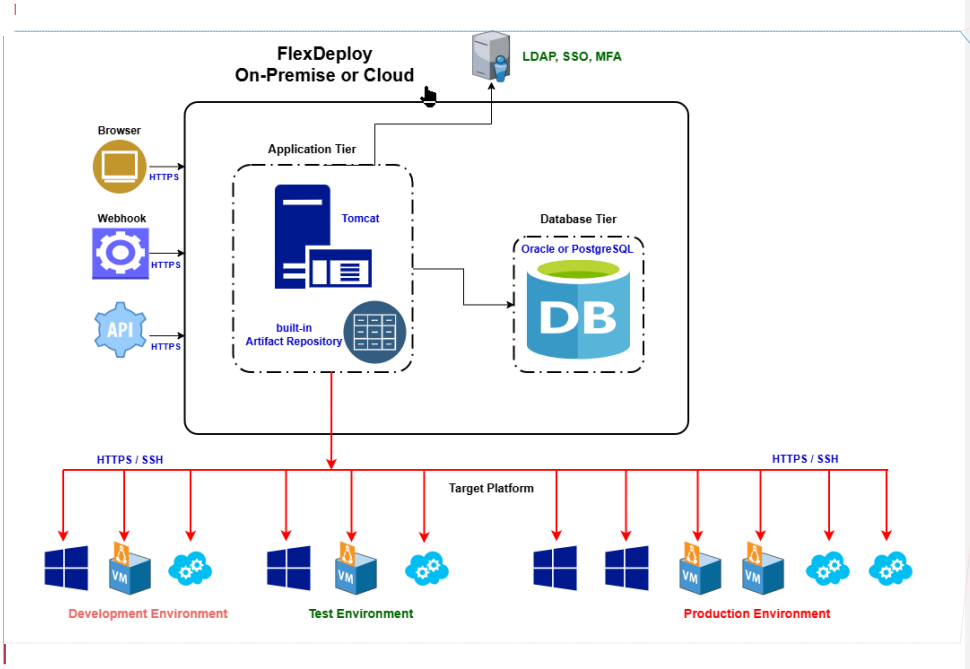
Key Features of FlexDeploy are

- **Comprehensive CI/CD Capabilities**: FlexDeploy provides end-to-end continuous integration and delivery pipelines, ensuring consistent and automated deployment across all environments.
- **Environment Management**: Simplifies configuration and management of environments, including development, testing, and production, to ensure seamless release processes.
- **Plugin Extensibility**: Supports an extensive library of plugins for various tools and platforms, enabling easy integration with existing DevOps ecosystems.
- **Support for Multiple Technologies**: FlexDeploy works across diverse technologies such as Java, Oracle, Salesforce, and more, making it a versatile solution for enterprise environments.
- **Automated Workflows**: Reduces manual intervention by automating build, deployment, and operational workflows, leading to faster and error-free application delivery.
- **Built-in Artifact Management**: Provides an Artifact Repository feature that allows organizations to manage and store artifacts, such as binaries, and packages, in a centralized and secure location. This repository serves as a reliable source for storing, versioning, and distributing artifacts throughout the software delivery process.
- **Release Orchestration**: Coordinates releases with dependencies in complex, multi-tier applications, ensuring smooth and synchronized deployments.
- **Security Features**: Includes secure credential management and integration with tools like CyberArk for safe handling of sensitive information during automation.
- **Audit and Compliance Support**: Provides detailed insights into deployment activities and access logs, supporting governance and regulatory compliance.
- **Customizable and Scalable**: Designed to adapt to both small teams and large enterprises, FlexDeploy scales with your needs while allowing configuration to meet specific requirements.

Key benefits of integrating FlexDeploy with CyberArk Secrets Manager

- **Enhanced Security**: FlexDeploy integrates with CyberArk Secrets Manager to securely manage sensitive credentials, ensuring they are never exposed within scripts or workflows. This minimizes the risk of unauthorized access.
- **Streamlined DevOps Processes**: The integration enables seamless integration of secure credential retrieval into CI/CD pipelines. Automated workflows reduce manual intervention, simplifying deployment and operations.
- **Improved Compliance**: Audit capabilities in CyberArk Secrets Manager complement FlexDeploy's traceability features, creating end-to-end visibility into credential usage and system access. This supports regulatory compliance and internal policies.
- **Secure Credential Management**: Eliminates the need for hardcoding credentials by dynamically fetching them from CyberArk Secrets Manager, reducing attack surface and enhancing overall system security.
- **Automation-Friendly**: Combines FlexDeploy's automation features with CyberArk Secrets Manager's centralized credential storage, allowing secure automation across the software delivery lifecycle.
- **Scalable and Configurable**: Supports complex enterprise environments where multiple teams can securely share access to critical resources without compromising security policies.

FLEXDEPLOY ARCHITECTURE DIAGRAM & DESCRIPTION OF CYBERARK INTEGRATION



FlexDeploy workflow is a main execution engine which contains one or more plugin operations to perform overall process of build/deploy. Such plugin operations will be executed on target servers. Workflow designer is responsible for putting operations together to achieve specific goals.

FlexDeploy connects to target servers (aka Endpoint) using SSH protocol. FlexDeploy application is responsible for retrieval of various credentials necessary to connect to target servers as well as credentials necessary to execute specific operations, for example database password. Such credentials are retrieved by FlexDeploy application and passed on to plugin operation over SSH or HTTPS. This means that FlexDeploy to CyberArk Secrets Manager in only invoked from FlexDeploy application server tier. At this point, FlexDeploy is a single server application, hence all integration access will occur from one server.

Build/deploy actions can be initiated manually or automatically based on some trigger/schedule. FlexDeploy will initiate workflow execution to perform specific build/deploy. At this point, just before workflow execution starts, credentials will be retrieved and passed to execution engine. FlexDeploy will not cache credentials, i.e. they are only used for one execution, next workflow execution will retrieve credentials once again. Note that credentials are also retrieved when SSH connection is initiated to target server.

Commented [EM2]: Is this supposed to be here? Im guessing it needs to be removed

Commented [CP3R2]: removed

Commented [EM4]:

Commented [EM5]: I think this image and the message were supposed to be removed? '

Remove extra white space

SECRETS MANAGER INSTALLATION

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

FlexDeploy provides two options for integration with CyberArk Secrets Manager. Integration can be achieved by Agent or AIMWebservice.

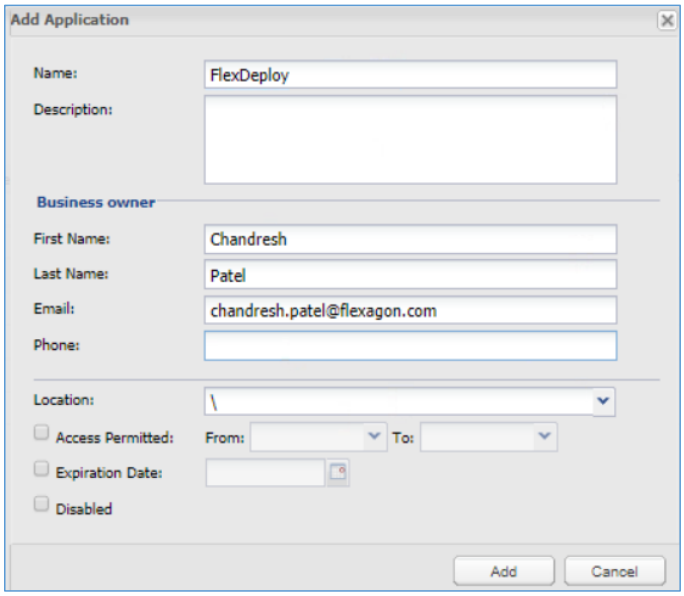
1. For integration using Agent, follow CyberArk Agent installation and configuration only on FlexDeploy server. You only need to provide location of clipasswordsdk executable in FlexDeploy configurations.
2. For integration using Webservice, there is no installation necessary on FlexDeploy server. But you need client certificate for authentication. If CyberArk Secrets Manager is setup using self-signed certificates, then you also need to provide server root certification. You can place both of these certificates on FlexDeploy server.

SECRETS MANAGER CONFIGURATION

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

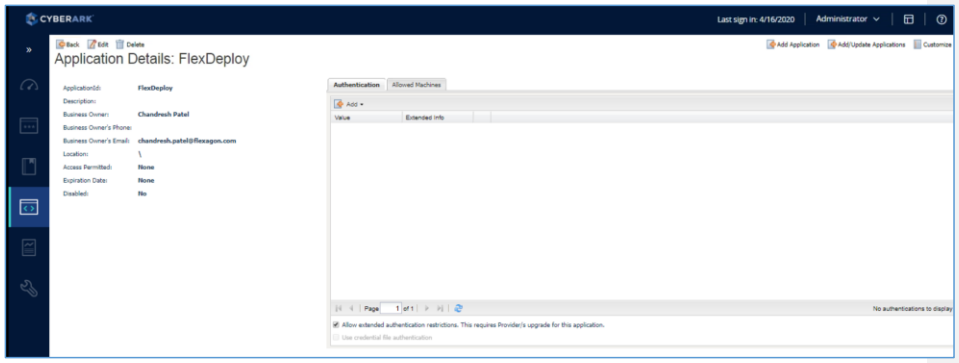
To define the Application, here are the instructions to define it manually via CyberArk’s PVWA (Password Vault Web Access) Interface:

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 the unique name (ID) of the application. The recommended Application ID for this integration is: APP ID = _FlexDeploy_
    - 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.

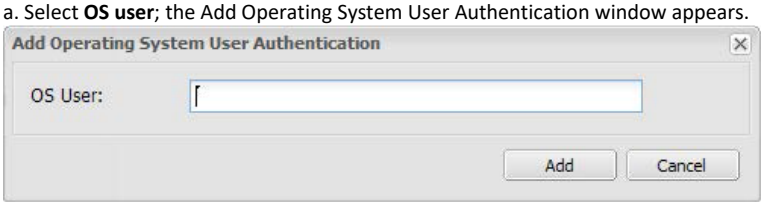


- **Allowing extended authentication restrictions**. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application. Please check this box.

4. Specify the application's **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password. FlexDeploy recommends use of Certificate Serial Number authentication.

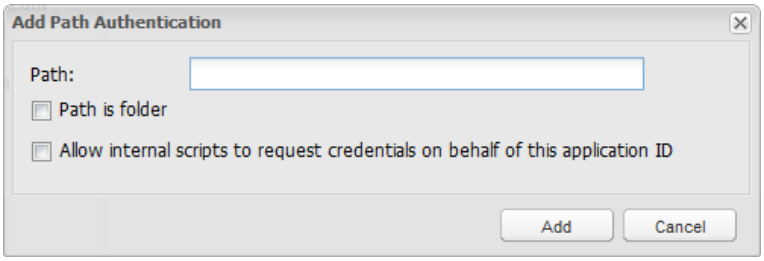
   - In the Authentication tab, click **Add**; a drop-down list of authentication characteristics is displayed.
   - Select the authentication characteristic to specify.

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.

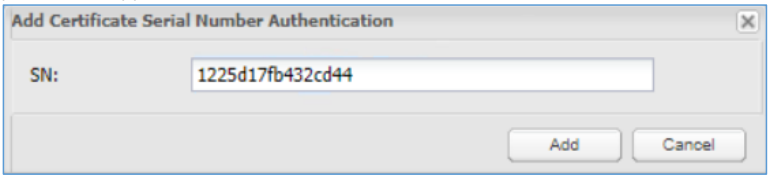


b. Specify the path where the application will run.
c. To indicate that the specified path is a folder, select **Path is folder**.
d. To allow internal scripts to retrieve the application password for this application, select **Allow internal scripts to request credentials on behalf of this application 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.

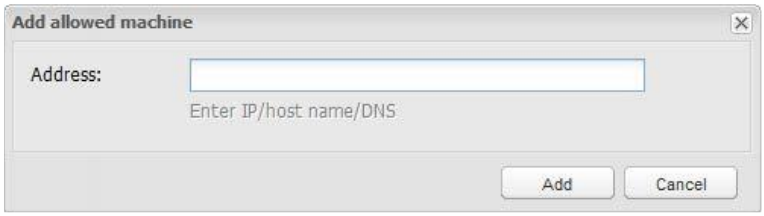
   d. In the Hash edit box, paste the application's unique hash value, or specify multiple hash values with a semi-colon. You can add additional information in a comment after each hash value specified for an application by specifying '#' after the hash value, followed by the comment.
   For example, OE883B7OD5B6E3EE37D37198049C9507C8383DB6 **#app2**
   Note: The comment must not include a colon or a semicolon.
   e. Click **Add**; the Hash is added as an authentication characteristic with the information that you specified.

8. Specify the Certificate Serial number:
   a. When using the Agentless Secrets Manager (Central Credential Provider) there's an option to protect the Application ID with a client certificate serial number:



9. 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 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 (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).

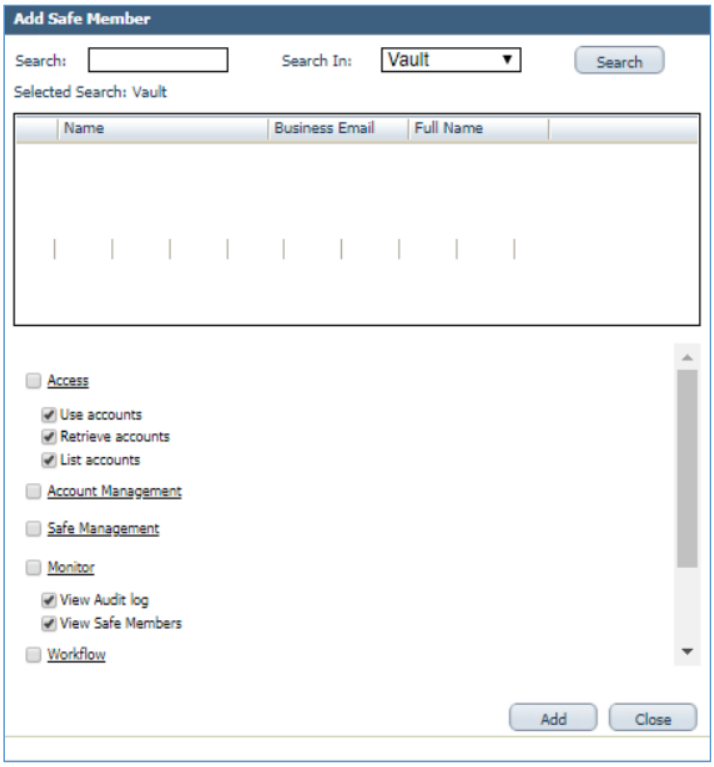
- In the Password Safe, provision the privileged accounts that will be required by the application. You can do this in either of the following ways:
  - **Manually** – Add accounts manually one at a time, and specify all the account details.
  - **Automatically** – Add multiple accounts automatically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

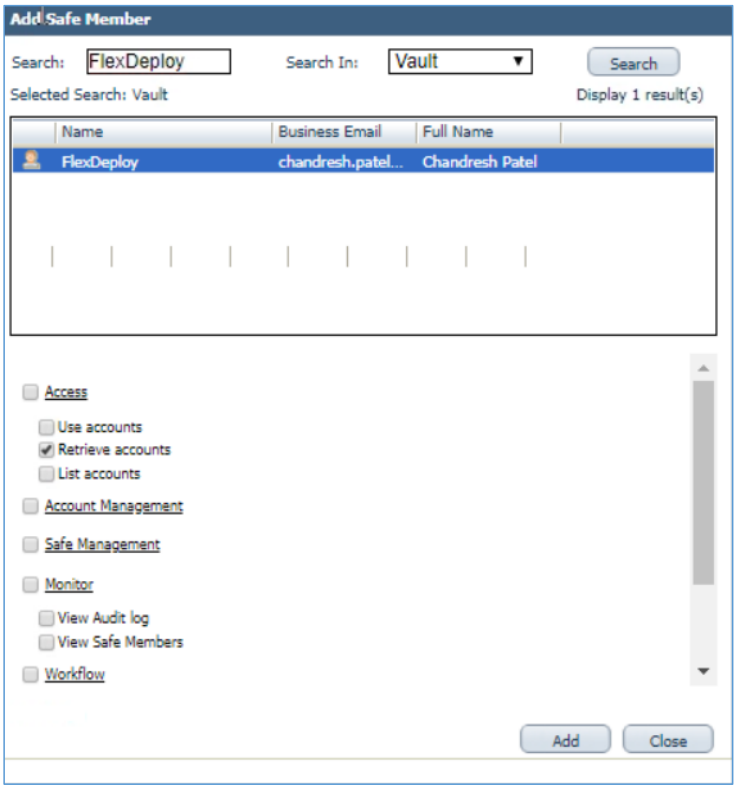
- Add the Credential Provider and application users as members of the Password Safes where the application passwords are stored. This can either be done manually in the Safes tab, or by specifying the Safe names in the CSV file for adding multiple applications.
  i. Add the Provider user as a Safe Member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

FLEXDEPLOY INSTALLATION & INTEGRATION CONFIGURATION

Refer to FlexDeploy Documentation for Partner Product installation.

FlexDeploy provides two out of box options for integration with CyberArk Secrets Manager:

- Command line option with Agent and
- HTTP call to AIM webservice

Here are high level integration steps for either type of CyberArk Secrets Manager integration:

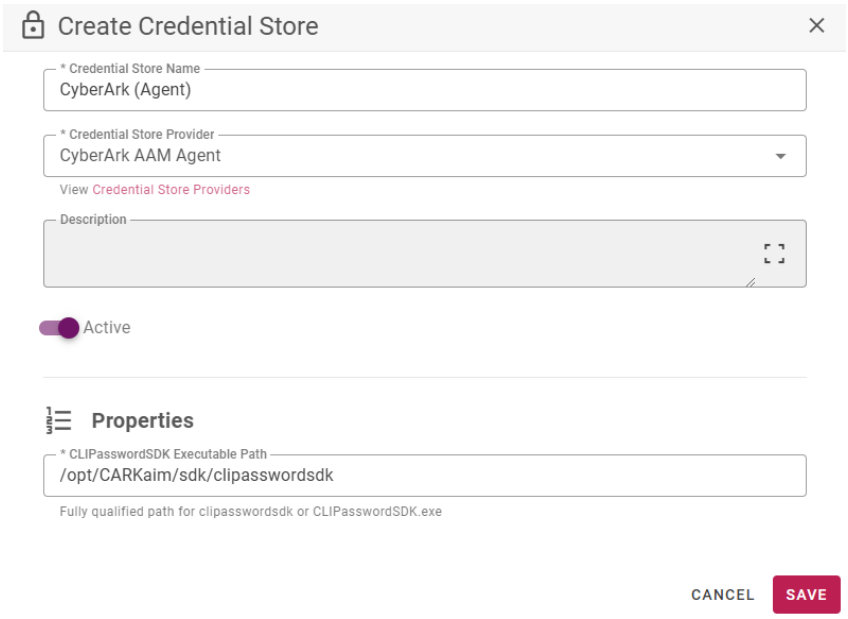
- Configure credential store in FlexDeploy with details necessary to interact with CyberArk
- Configure individual credential for each secret value necessary
- Use credential in build/deploy configurations

Commented [EM6]: Please expand and include screenshots

Commented [CP7R6]: Screen shots are in next section

CONFIGURE AGENT INTEGRATION

For integration using agent, first you need to install and configure CyberArk agent on the FlexDeploy server, which will setup clipasswordsdk executable in /opt/CARKaim/sdk. Now create credential store configuration using CyberArk Secrets Manager Agent provider and provide location of clipasswordsdk.

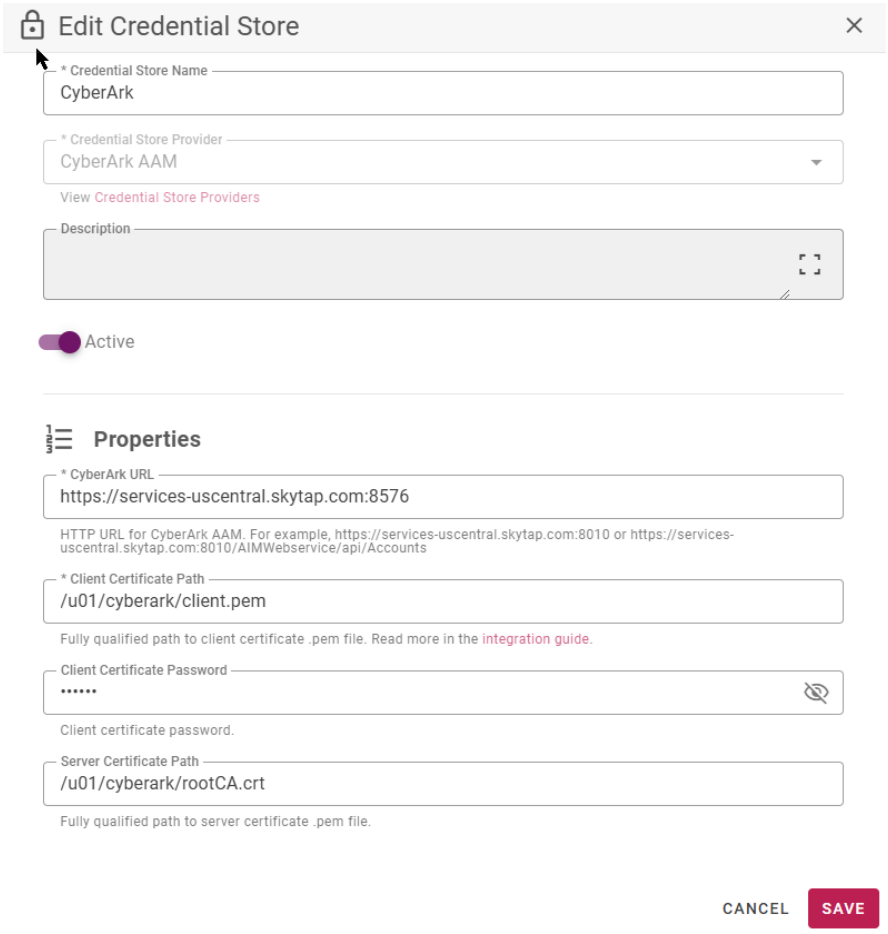


FlexDeploy will invoke command line to get secret. For example,

/opt/CARKaim/sdk/clipasswordsdk GetPassword -p AppDescs.AppID=FlexDeploy -p Query="safe=Database%20Accounts;folder=root;object=apps" -o Password

CONFIGURE WEBSERVICE INTEGRATION

For integration using webservice, you need various details like CyberArk URL and Client Certificate. Client certificate is used for authentication. If you are using self-signed certificates, you need to provide server certificate as well. Now create credential store configuration using CyberArk Secrets Manager provider and provide various details.

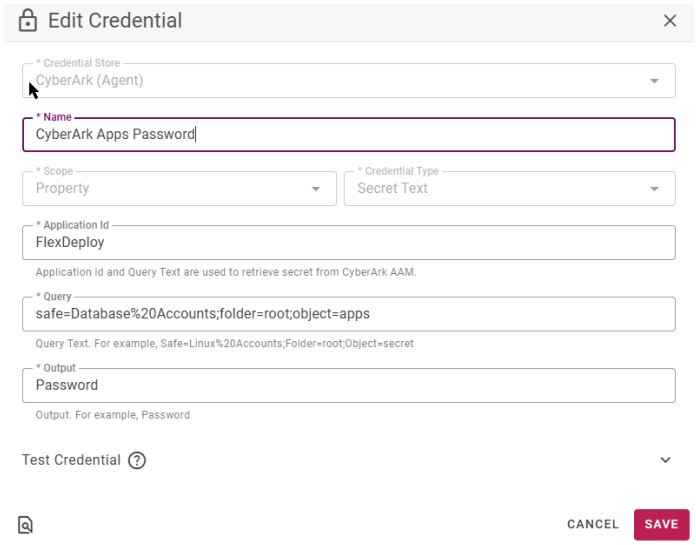


FlexDeploy will invoke webservice to get secret. For example,

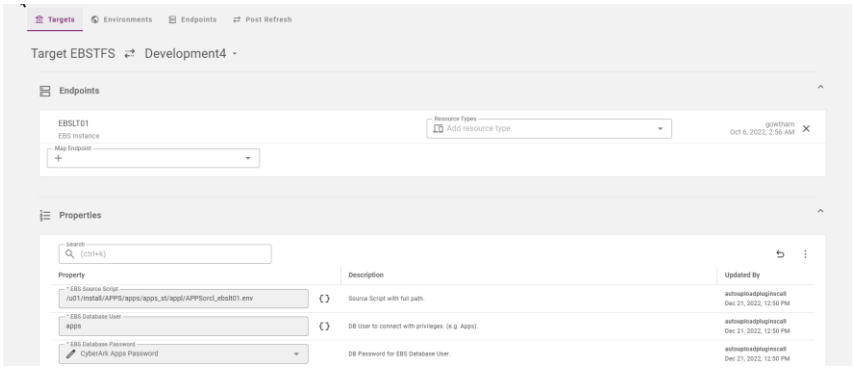
https://services-uscentral.skytap.com:17052/AIMWebservice/api/Accounts?AppID=AppId1&Query=safe=Database%20Accounts;folder=root;object=apps

CONFIGURE CREDENTIAL

For each secret value that you want to use from CyberArk Secrets Manager, configure credential with unique name. In either type of integration, you will need to provide Application Id and Query. Query contains details like safe, folder and object.



Now use credential as necessary in FlexDeploy configurations.



FlexDeploy will retrieve secret from CyberArk as necessary and will not cache or print it. This will allow you to update credentials as per your organization policies and not have to worry about updating FlexDeploy configurations.

FLEXDEPLOY CONTACT INFO

Business Contact	Name	Dan Goerdt
	Email	Dan.goerdt@flexagon.com
	Tel	920 819 6788
Technical Contact	Name	Chandresh Patel
	Email	Chandresh.patel@flexagon.com
	Tel	920 819 4951
Support Contact	Name	Flexagon Support
	Email	support@flexagon.com
	Tel	