



CYBERARK SECRETS MANAGER

(Agent Based Credential Provider CP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Flexera

Website: www.flexera.com

Name of Product: FlexNet Manager Suite | Flexera One Inventory Beacon

Version: 2020 R1

Date: 20 September 2017 (Revised 04 October 2024)

FLEXNET MANAGER SUITE OVERVIEW

Flexera is the global leader in software licensing, compliance, cybersecurity, and installation solutions.

Flexera helps application producers and enterprises increase application usage and security, enhancing the value they derive from their software. Our software licensing, compliance, cybersecurity, and installation solutions are essential to ensure continuous licensing compliance, to optimize software investments, and to future-proof businesses against the risks and costs of constantly changing technology. A marketplace leader for more than 25 years, Flexera is a trusted and neutral source of knowledge and expertise for more than 80,000 customers who rely on the automation and intelligence designed into our products.

Flexera is the established global leader in software asset management and software license optimization solutions, enabling enterprises to gain visibility and control of IT assets, to reduce ongoing software costs, and to maintain continuous license compliance. These capabilities are delivered as a comprehensive suite of enterprise software asset management and license compliance solutions that optimize the management of software assets throughout the software lifecycle. Version: 2017 R2 SP1

KEY BENEFITS

FlexNet Manager Suite for Enterprises is a comprehensive, proven, next generation solution for hardware asset management, software asset management, license compliance and software license optimization. FlexNet Manager Suite provides entitlement-based license management and software license optimization to help organizations to reduce ongoing software licensing costs and maintain continuous license compliance. It is used by thousands of enterprises to gain control of and optimize software spend while reducing the time and effort required to manage the software estate.

FLEXNET MANAGER PLATFORM

The foundation of FlexNet Manager Suite, FlexNet Manager Platform provides extensive hardware and software asset management (HAM and SAM) capabilities for managing desktop, laptop, and server hardware, as well as software from almost 17,000 vendors (and increasing every month). FlexNet Manager Platform also provides automated, entitlement-based Software License Optimization for desktop software from vendors including Adobe, Microsoft, and Symantec. The Platform also serves as the foundation for integrated, add-on server license optimization products included in FlexNet Manager Suite for Enterprises.

Key functionality in FlexNet Manager Platform includes: **IT**

Asset Discovery & Inventory

- Provides cross-platform desktop to datacenter (Windows, Linux, UNIX, and MAC OS), physical and virtual machine discovery, inventory, and application usage data collection
- Leverages existing IT investments through integration with a multitude of third-party standard inventory sources

Software Inventory Normalization

- Applies consistent naming conventions for software publishers and titles to ensure accurate counts

- Enables organizations to ‘know what they have’ in their IT environment and consolidate vendors and applications

Purchased Versus Installed/Consumed License Reconciliation

- Reconciles software purchases against software installed or used on computers and virtual machines within the enterprise
- Enables organizations to maintain license compliance to reduce audit cost and risk

Management Dashboard and Reporting

- Includes customizable Analytics dashboards for custom reporting to executives
- Provides an intuitive management dashboard, enabling an administrator to understand the current license position, receive alerts on issues, and review key events such as data imports
- Provides a compliance overview report that summarizes an organization’s exposure, such as its financial liability and the number of licenses at risk for each publisher
- Includes drilldowns that provide deeper information for any vendor products and the licenses attached to those products.

FLEXNET MANAGER SUITE SERVER LICENSE OPTIMIZATION SOLUTIONS

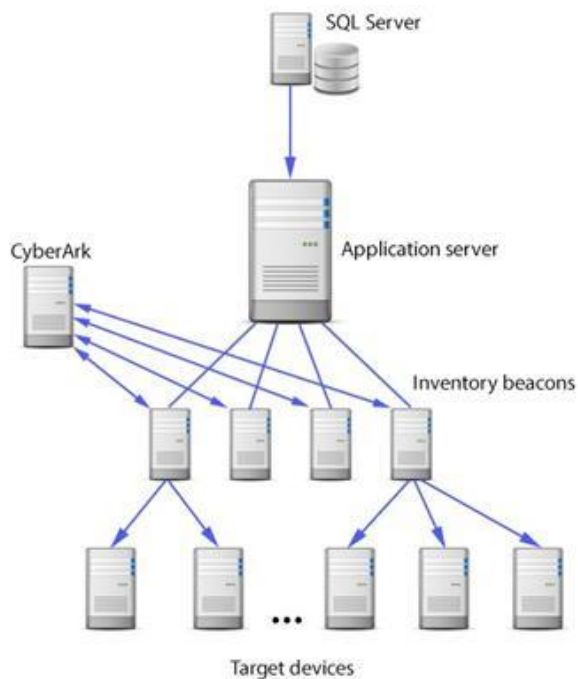
FlexNet Manager Suite includes next generation software asset management and license optimization solutions that analyze inventory, application usage, purchase order data, license entitlements, and contract terms to optimize license consumption for server software. By automating the process of optimizing software license management for key vendors, FlexNet Manager Suite enables organizations to save on license purchases, audits, renewals, and annual true-ups, while reducing time and effort.

These optimization solutions enable organizations to implement multiple software license management and contract optimization strategies that save time, help ensure continuous license compliance and reduce costs by:

- Applying product use rights to optimize license consumption based on license agreements. Among others, use rights include upgrade, downgrade, right of second use, multiple use, roaming use, virtual use, and license mobility. Product use rights for key vendors such as Adobe, IBM, Microsoft, Oracle, SAP, Symantec, and VMware are encapsulated in a Product Use Rights Library.
- Utilizing license prioritization to drive intelligent allocation and minimize license consumption.
- Tracking detailed usage of SAP software to automatically determine the optimal Named User License type for each user.
- Optimizing the license count and application mix for engineering applications that use a concurrent license model.
- Analyzing cloud usage trends for better budgeting and forecasting, improving efficiency, optimization of instance types, and reducing expenditures on cloud services.

FlexNet Manager Suite integrates with CyberArk Secrets Manager to enable our joint enterprise customers to gather appropriate in-depth data securely from datacenter resources with managed privileged and protected access.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



SECRETS MANAGER INTEGRATION

Integration between FlexNet Manager Suite and CyberArk is implemented at the level of the inventory beacons. You may implement multiple inventory beacons, either as a flat layer as shown above, or in a reporting hierarchy, based on your environmental requirements. The diagram above is a typical structure supporting 30000 to 50000 target inventory devices.

These inventory beacons are the front line for remote execution tasks required by FlexNet Manager Suite. These tasks may include:

- Automatic installation of the FlexNet inventory agent on the target device, when required
- Discovery, including discovery of the device itself on the network, and probing the device to see what other services are available on this device
- Remote inventory gathering from devices where the FlexNet inventory agent is not (and perhaps cannot be) installed locally

For all these kinds of tasks, the inventory beacon may need credentials to gain access to target devices.

Each inventory beacon has a local Password Manager that you may use to record the credentials needed by this individual inventory beacon to access the devices it is targeting. Each Password Manager is completely independent and stores only those additional credentials that this inventory beacon requires for remote execution tasks. Further, no inventory beacon communicates accounts or passwords to the central application server.

When the credentials are stored in a CyberArk Vault, the Password Manager on the inventory beacon only stores a reference to (specifically, a query for) each required credential that it can request from CyberArk. Retrieving credentials from CyberArk means that, on each such inventory beacon deployed in your environment, the CyberArk Credential Provider must be locally installed. The Password Manager requests each credential from the Credential Provider, which as always handles the integration with the CyberArk Vault.

CREDENTIAL RETRIEVAL

Credential retrieval is triggered by jobs that have been scheduled for the inventory beacon. The local Password Manager includes a set of filters you may use to ensure that only the most appropriate credential for the target device is retrieved, and once the login with the credential is achieved, the credential is dropped. Account names and passwords are never cached. Subsequent requirements for this same credential trigger a fresh retrieval from the CyberArk Vault.

SECRETS MANAGER INSTALLATION

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

When installation is complete, please use Windows Explorer to validate that CPasswordSDK.dll is present in %windir%\System32 on a 32-bit device, or %windir%\SysWOW64 on a 64-bit device.

Tip: If this is not already the case, following installation of the CyberArk Credential Provider on this inventory beacon, you can find a copy of CPasswordSDK.dll (this 32-bit version, and not the equivalent 64-bit version) in the Credential-Provider-installation- path\ApplicationPasswordSdk folder. Copy this to the appropriate location for the architecture of your inventory beacon server.

Both the Credential Provider service and the BeaconEngine service must be running on the inventory beacon for integration to be successful.

SECRETS MANAGER CONFIGURATION

The following sections provide details on FlexNet Manager Suite configuration with CyberArk Secrets Manager.

Once both the CyberArk Credential Provider and FlexNet Beacon are installed and operational on the inventory beacon server, your CyberArk administrator can register the application with the level of security required by your corporate operating procedures.

CyberArk supports multiple processes for configuration, including manual interaction and automated processes. This summary assumes the manual process for clarity. The manual process is most conveniently started from the inventory beacon in question. Ensure that you have open both the FlexNet Beacon interface (this requires administrator privileges on the inventory beacon) and a web browser that can access your CyberArk implementation.

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

To define the application, define it manually through the CyberArk Password Vault Web Access (PVWA) interface:

- ☐ Log in as user allowed to manage applications (it requires Manage Users authorization) ☐
In the Applications tab, click **Add Application**. The Add Application page appears.

>> Replace this screenshot with data filled in (i.e. with the pre-defined APPID the customer should use, specified in the “Name” field)

The screenshot shows the 'Add Application' dialog box. It has a title bar with a close button. The form includes the following fields and sections:

- Name:** A text input field.
- Description:** A text area with scrollbars.
- Business owner:** A section header followed by four text input fields: First Name, Last Name, Email, and Phone.
- Location:** A dropdown menu.
- Time Restrictions:** A checkbox followed by 'From:' and 'To:' dropdown menus.
- Expiration Date:** A checkbox followed by a date input field.
- Disabled:** A checkbox.
- Buttons:** 'Add' and 'Cancel' buttons at the bottom right.

☐ Specify the following information:

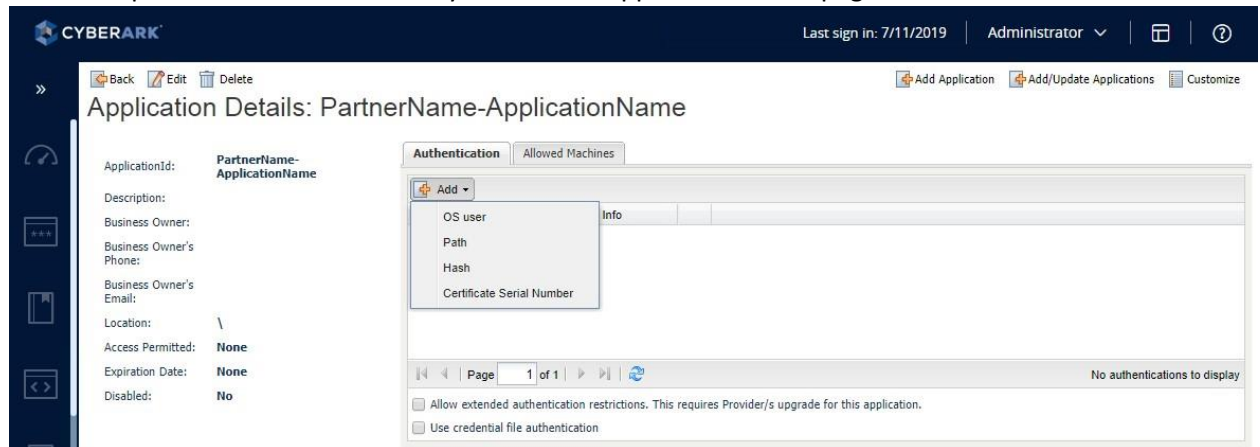
- In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: APP ID = _____
- In the **Description** box, specify a short description of the application that will help you identify it.
- In the **Business owner** section, specify contact information about the application’s business owner.
- In the **Location** box, 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. For **Location**, it is typical to select the \Applications folder, but this is not mandatory.

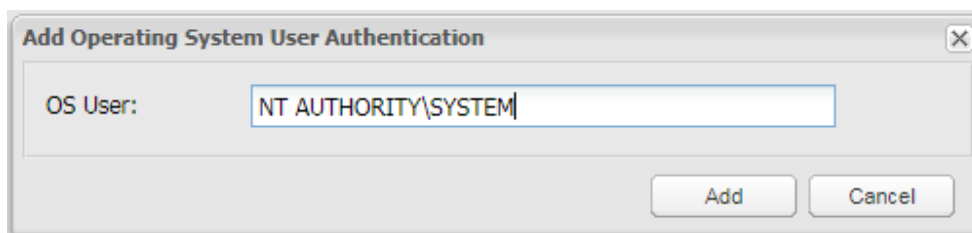
Tip: It is best practice to not add time restrictions or an expiration date for this application's access to the CyberArk Vault. This is because inventory gathering may be scheduled at any time of day, typically after hours when systems are lightly loaded.

- ☐ Click **Add**. The application is added and is displayed in the Application Details page.

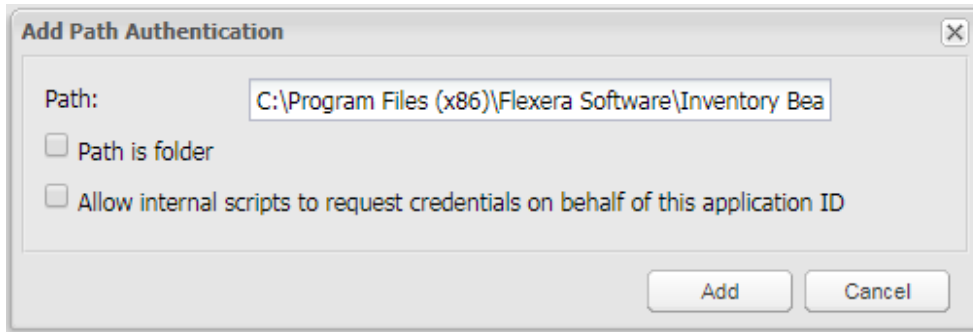
>>Please replace this screenshot with your Partner Application Detail page



- ☐ Check the **Allowing extended authentication restrictions** box. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.
- ☐ 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.
- ☐ Select **OS user**. The Add Operating System User Authentication window appears.



- ☐ From FlexNet Beacon, copy the value of the **Inventory beacon service account**, paste into the **OS User** field in PVWA, and click **Add**. The OS user is listed in the Authentication tab.
- ☐ Select **Path**. The Add Path Authentication window appears.



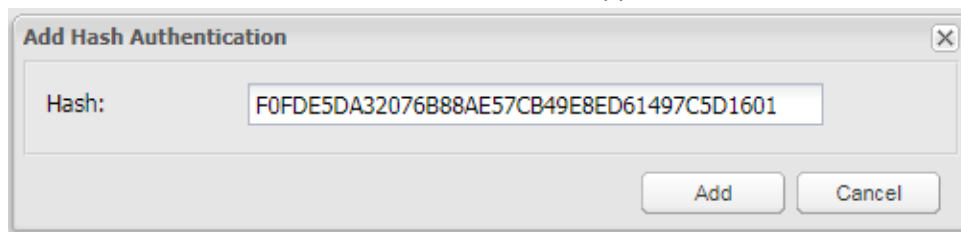
- a. From FlexNet Beacon, right-click the **Beacon executable path** value, copy, and paste into the **Path** field in the **Add Path Authentication** dialog in PVWA (the default value is C:\Program Files (x86)\Flexera Software\Inventory Beacon\DotNet\bin\BeaconEngine.exe, but copy the value in use for your own inventory beacon). Clear the **Path is folder** check box (because these paths include the file name) and click **Add**.

- ☐ To indicate that the specified path is a folder, select **Path is folder**. 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**.

- ☐ Click **Add**. The Path is added as an authentication characteristic with the information that you specified.

- ☐ Specify a hash:

- Run the AIMGetAppInfo utility to calculate the application's unique hash. Copy the hash value that is returned by the utility.
- In the PVWA, select **Hash**. The Add Hash window appears.

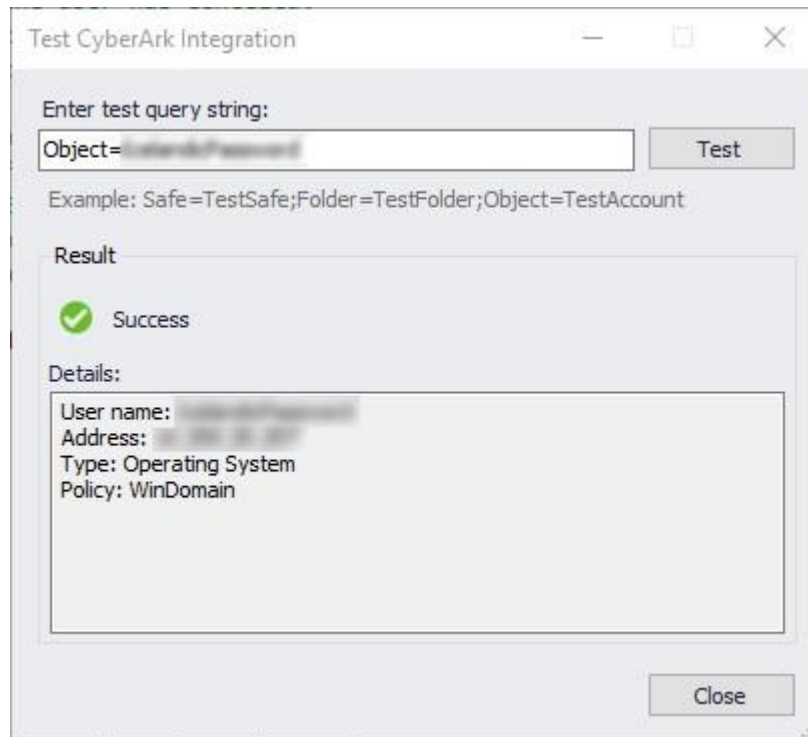


- In the Hash edit box, paste the application's unique hash value, or specify multiple hash values with a semi-colon. To obtain the unique hash value, copy the **Beacon executable hash** value from FlexNet Beacon on your inventory beacon. You can add additional information in a comment after each hash 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.
- Click **Add**. The Hash is added as an authentication characteristic with the information that you specified.

- ☐ To test that the configuration is successful, click **Test CyberArk integration...** in the **Password management** page of FlexNet Beacon.
- ☐ A separate **Test CyberArk Integration** dialog appears.
 - Enter a query for which the credential already exists in CyberArk (depending on how the credential is secured, specifying `Object=accountName` may be sufficient, provided that the answer is exactly one credential), and click **Test**.

After a moment, the dialog displays the results:

For success, several attributes of the account in CyberArk (but not, obviously, its password) are displayed.



For failure, the error message received from CyberArk is displayed unchanged. You should fix the error(s) and repeat the testing until successful.

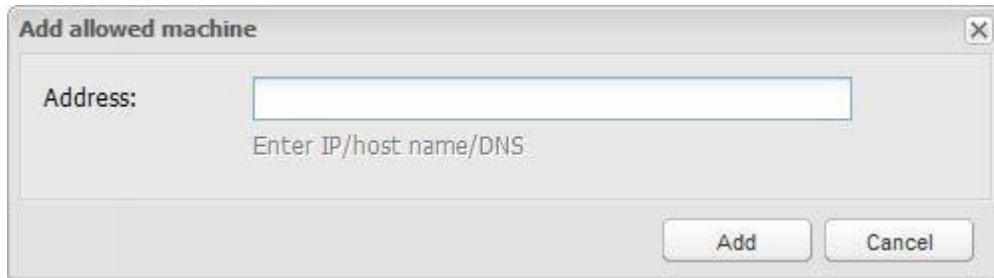
Tip: If the Credential Provider service is not running on the inventory beacon, the response waits 30 seconds and then times out.

- ☐ The basic application record now exists in CyberArk. This application record can now be referenced by all your inventory beacons that need access to credentials stored in CyberArk. As you register additional inventory beacons in PVWA (hint: click **Search** to populate the application list under the **Applications** tab), validate that:
 - The OS user account that runs the inventory beacon engine is unchanged. If a different account has been used on a particular inventory beacon, update the application record in PVWA with the additional OS user.

- The installation path of the executable is unchanged on the new device. If an inventory beacon has a non-standard installation, add the different path to this application record.
- The hash value is unchanged for the executable. The value remains consistent for a given release of the Beacon engine; but of course, you should expect the hash to change when an inventory beacon is updated with a later version of FlexNet Beacon. If your environment during upgrade has a mixture of inventory beacon versions, keep the old hash value in the application definition for the time being, while adding another hash for the updated version.

This requires logging in to each inventory beacon to check the relevant details on the **Password management** page of FlexNet Beacon.

- ☐ Register each inventory beacon as a device using the registered application details in PVWA:
- ☐ 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.
 - 



- In the **Address** box, 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.

Repeat this registration of the machine details for each relevant inventory beacon.

Make sure the servers allowed include all mid-tier servers or all endpoints where the Secrets Manager Credential Providers were installed.

Tip: The IPv4 address of the inventory beacon is another method of identification, but beware of using this method in situations where dynamic IP address allocations may alter the IP address of your inventory beacons over time.

- ☐ Configure the required safe and its memberships:
 - If it does not already exist, create the safe that will store credentials needed by your inventory beacons (navigate to **Policies > Access Control (Safes)**, and click **Add Safe**). If the safe already exists, select it from the list of safes, and in the bottom right, click **Members**.
 - In the **Members** tab, click **Add Member**, search for the application you saved, select it in the list of results (the default privilege levels are adequate, and must include **Retrieve accounts**), and click **Add**.

Tip: Look for the success message at the bottom of this dialog, and then click Close. Once the dialog is closed, the list of members is updated and displays your application as a member permitted to access this safe.

CyberArk Secrets Manager is now configured with the appropriate application record, the registered inventory beacons that may request credentials, and the safe that is to hold related credentials. You may now save the credentials in CyberArk. You may also now save references to these credentials in Password Manager on each inventory beacon.

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.

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**.

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.

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.

☐ 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 the application (the APPID) as a Safe Member with the following authorizations:

- Retrieve accounts

☐ 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.

RECORDING CREDENTIALS

- The actual account name (user name) and password must be saved in the appropriate CyberArk Vault and safe, where they are known as "accounts".

- A reference (query string) to retrieve that credential must be saved in Password Manager on the appropriate inventory beacon.

As both systems provide different types of credential, some mental mapping is also required to keep the different type descriptions aligned.

For simplicity, only the manual processes for declaring credentials are documented here. Both products also offer script-based loading of credentials, for details of which see the respective documentation of each.

TO MANUALLY RECORD CREDENTIALS FOR USE BY INVENTORY BEACONS

1. Ensure that the credentials needed for the remote execution activities of every inventory beacon are recorded as CyberArk “accounts”.
 - a. In the **Account** tab of PVWA, click **Add Account**.
 - b. In the **Add Account** page, in the **Store in Safe** drop-down, select the safe you created for credentials accessed by inventory beacons.
 - c. Select the **Device Type** and resulting **Platform Name** for this credential.
 - i. Here are suggested mappings between the **Account type** saved in the FlexNet Beacon Password Manager and these two fields in PVWA:

Account type (FlexNet)	Device Type (PVWA)	Platform Name (PVWA)
Windows domain account	Operating System	Windows Domain Account
Local account on Windows device	Operating System	Windows Server Local Accounts (or Windows Desktop Local Accounts if you are targeting desktop computers)
SSH account (password)	Operating System	Unix via SSH
SSH account (key pair)	Operating System	Unix via SSH Keys
Account on VMware ESX server	Operating System	VMWare ESX Account API

Account on VMware VirtualCenter	Application	VMWare vCenter Shared Accounts
Account on Oracle database	Directory (This choice does not	[None]
	require a user name for the credential.)	
Oracle VM management API account	Database	Oracle Database
	Operating System	VMWare ESX Account API or Unix via SSH (see note)

Note: The Oracle VM management API account is likely to be a local account on Linux, and currently PVWA does not offer a matching platform name. Your CyberArk administrator may perhaps create a custom platform name for your use, or you can use other platform names (such as either of the two suggested above) that provide the correct set of data fields.

- d. Complete the remaining properties for the credential and click **Save**.
 - i. **Address** may identify the device that requires this credential, either using an IP address, a host name, or a fully qualified domain name. In cases where this isn't particularly meaningful (such as a Windows domain password), enter free text such as the domain name.
 - ii. **Name** must be unique in context (for example, within the safe), and is typically used in query strings. For this reason, you may prefer to provide a custom, simpler name rather than use the one that is automatically generated.
 - iii. For Unix via SSH Keys, after saving, click **Add SSH Key** (upper right), and provide the required details.
- e. Take note of the query string parameters that uniquely identify this credential.

The query strings must be entered in FlexNet Beacon Password Manager, and are used to request each credential from CyberArk. If the query string does not return a single, unique credential, the request fails. Query string elements that may be used include:

- i. **Safe** — where the credentials for inventory beacon use are stored
- ii. **Address** — the same value you provided for this parameter for the credential, identifying the target device where the credential is to be used
- iii. **Object** — shown in the **Account Details** page in PVWA as the **Name**.

These values should be sufficient to uniquely identify the credential. For other elements that are possible in a query string, see the CyberArk documentation.

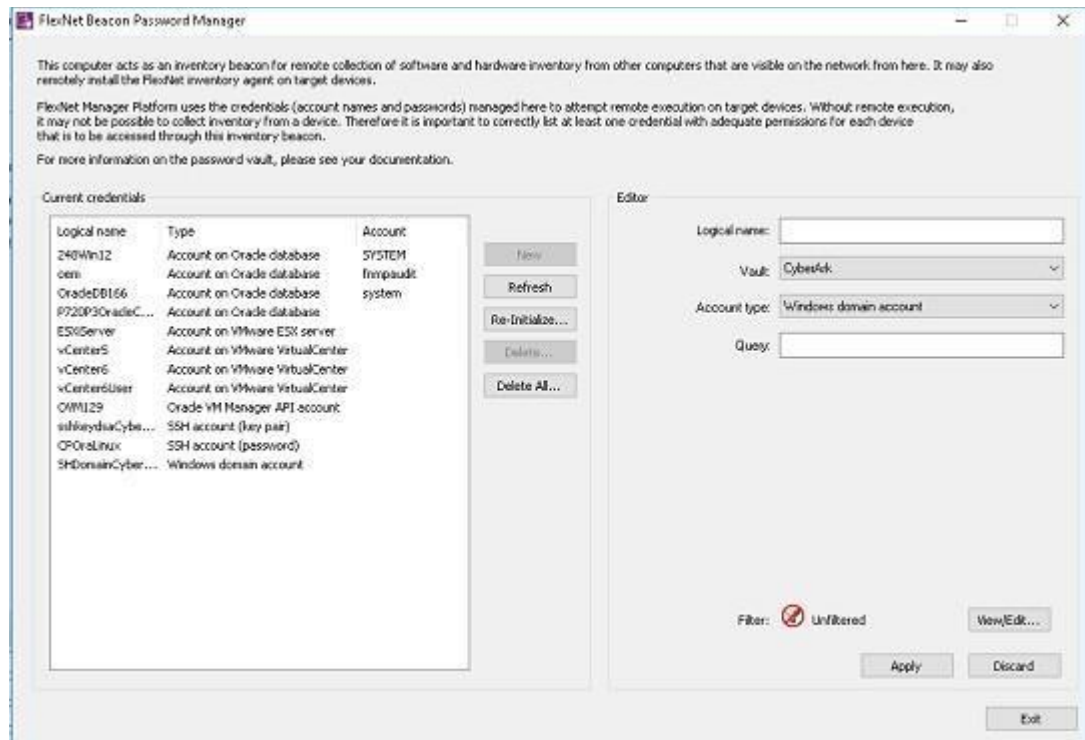
Repeat for as many credentials as required. This completes configuration of CyberArk. The last remaining step is to record the various credentials in Password Manager on the various inventory beacons from which they will be used for remote execution.

2. On each inventory beacon in turn, access Password Manager, and create records of the credentials used from this inventory beacon.

- a. Log into the FlexNet Beacon interface (this requires an account with administrator privileges on the inventory beacon), select the **Password management** page, and click **Launch Password Manager**.

Tip: The **Password management** page also shows that the CyberArk Credential Provider has been correctly identified on this inventory beacon. Your CyberArk administrator must have also identified this inventory beacon as a computer permitted to access the required credentials (as described in Configuring Application Identity Manager).

- b. In the **Current credentials** group, click **New**.



- c. For a new credential, supply a **Logical name** that you will recognize in listings over time.

This descriptive, friendly name for a credential (that is, an account name and password pair) must be unique on this inventory beacon. You may repeat logical names on other

inventory beacons, since they do not share credential data; but within each Password Manager, the logical name must be unique.

Logical names allow flexibility, in conjunction with filter settings, to specify a credential for exactly one computer, or a credential that you may use on a group of computers.

- d. Specify the kind of credential in the **Account type** field.

These are the same account types as are listed in the table above.

- e. Complete any additional details that appear because of your choice of **Account type**.

For detailed information, see the online help for the Password Manager. The most important value for CyberArk integration is the **Query** string, which must be specific to exactly one credential saved in the CyberArk Vault.

- f. Optionally, click **View/Edit filter...** if you want to restrict the target devices on which this named pair of account name and password should be tested.

The filter is checked against the current target device (where a remote execution task is scheduled), so that the inventory beacon can request a credential for exactly the correct machine. Several filters can be specified for the same credential. For detailed information, see the online help for the Password Manager.

- g. Complete your editing by clicking **Apply**. You may either repeat the process for another credential or click **Exit** to close the Password Manager.

The details you have specified are encrypted and saved in the registry on this inventory beacon as a reference to a credential previously saved in CyberArk. Repeat to save other credentials referenced from this current inventory beacon; and then move on to repeat for each of your inventory beacons that require CyberArk integration.

Tip: There is also a command-line interface to the FlexNet Password Manager that allows scripting the process of creating credentials in Password Manager. For detailed information, see the System Reference PDF file, available through the title page of the online help for FlexNet Manager Suite.

This completes the integration and configuration of both systems. The inventory beacons are now able to receive schedule remote execution tasks (downloaded from the central application server for FlexNet Manager Suite), retrieve appropriate credentials from CyberArk, complete the tasks, and upload the results.

PARTNER CONTACT INFO

Business Contact (Principal Product Manager)	Name	Aamer Sharif
	Email	asharif@flexera.com
	Tel	+61 (03) 9895 2000

Technical Contact	Name	
	Email	
	Tel	
Support Contact	Name	Flexera Support
	Email	flexeracommunity.force.com/customer
	Tel	+1 (408) 969-5441 (United States Local) +1 (877) 969-5441 (Toll-Free)