CYBERARK SECRETS MANAGER

(Agent Based Credential Provider CP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

CORTEX LTD.

www.WeAreCORTEX.com

CORTEX 7 Automation & Orchestration Platform

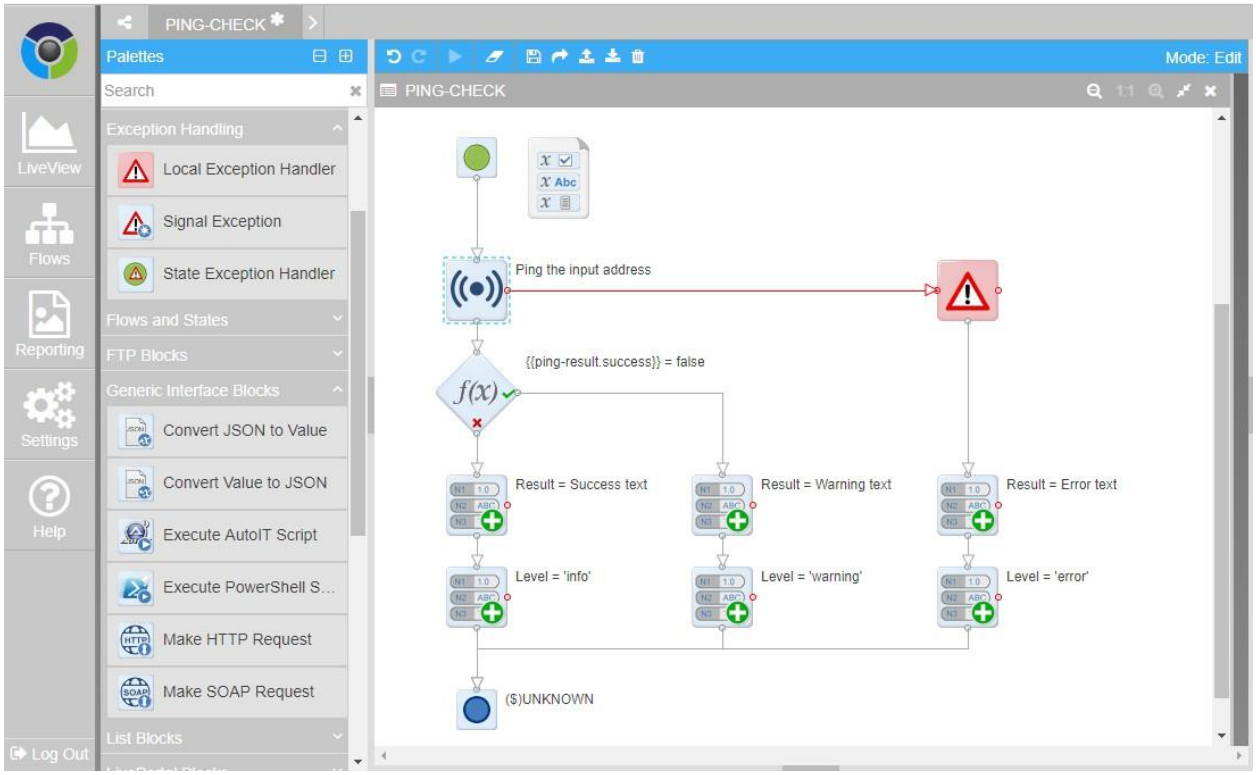
Version: 7.0 - 7.2

24 July 2024

CORTEX AUTOMATION & ORCHESTRATION PLATFORM OVERVIEW

The CORTEX platform is used by customers to implement Automation & Orchestration of workflows in an intuitive and graphical manner. Customers can automate time-consuming manual tasks while dramatically improving the speed and consistency of actions performed.

An example of a flow to do a ping check as viewed in the CORTEX Studio web UI is shown below.



A flow designer will implement a workflow using a drag-drop-configure-test-publish approach. The CORTEX platform includes essential features such as version control, flexible access control and LDAP integrated authorization. It also has extensive logging to enable reporting on the flows executed, interface interactions and outcomes.

Open standards interfaces enable CORTEX to interface with many third-party systems or devices. These include the following and more:

- Oracle
- SQL Server
- ODBC & OLEDB databases
- HTTP
- SOAP/REST web services
- SFTP/FTP
- SSH/Telnet
- LDAP
- CORBA
- SNMP
- TCP Sockets

Also included is CORTEX LivePortal, an interface for end users to initiate and interact with workflows, allowing the entry of necessary parameters that will be used during workflow execution, for example, employee details that need to be provisioned on a variety of target systems.

The CORTEX platform runs on the Microsoft Windows operating system and requires a Microsoft SQL Server database (various versions supported).

KEY BENEFITS

The CORTEX platform enables customers to rapidly design graphical workflows, and test and deploy these into a production automation engine, for direct execution by end users or when triggered by events.

The flows capture business rules, process logic and integration with external systems. CORTEX provides multiple levels of exception handling to ensure that unexpected situations are dealt with in a graceful manner.

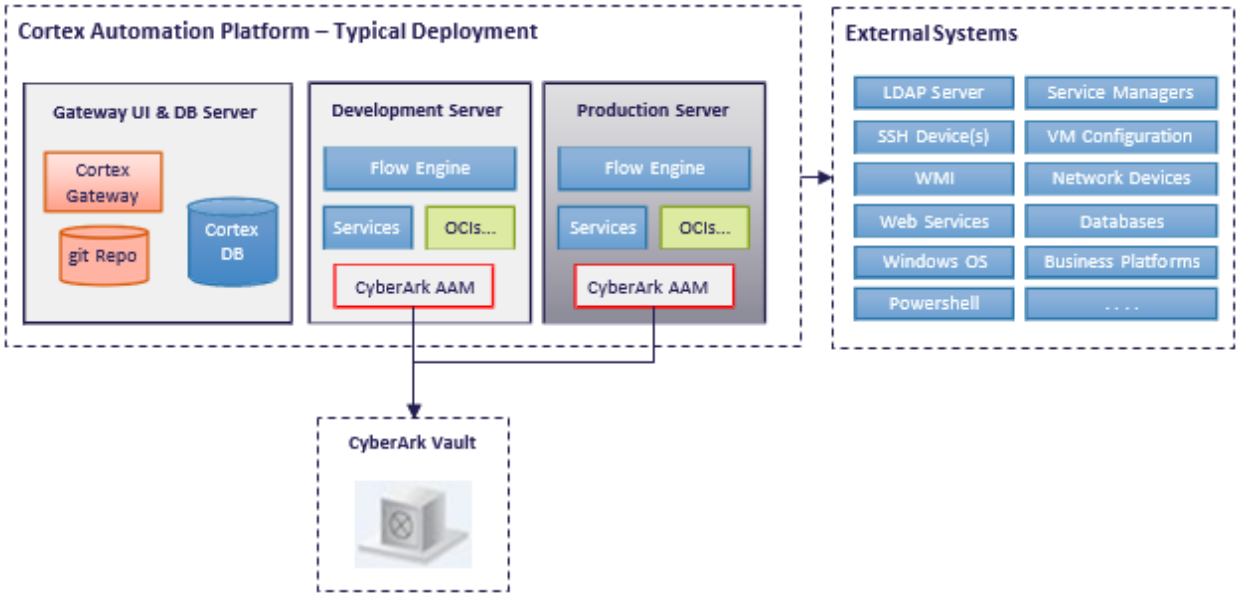
Privileged Credentials

The CORTEX platform typically needs to integrate with a broad range of third-party systems, and requires privileged credentials for interactions with these systems. Although CORTEX has the capability to securely store the required credentials to the third-party systems internally, a better approach that is more in line with modern security practices is for such credentials to be stored in a centralized Credential Management System.

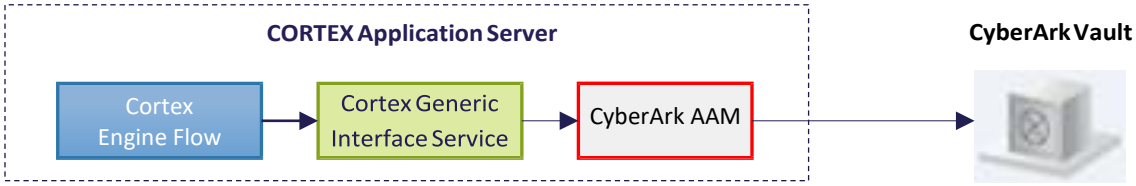
CORTEX LTD. recognized the need and introduced CyberArk integration into the suite of available interfaces, to be able to offer this capability to our customers.

Using the CyberArk integration improves security, allows centralized rather than distributed management of credentials and audits logging of all credential requests. It reduces the administrative burden on the CORTEX system administrators to comply with security policies such as password rotation.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



CORTEX integrates with the CyberArk Vault via the Secrets Manager Credential Provider. Secrets Manager is installed on each CORTEX Flow Engine server and provides an efficient local cache of credentials, which is critical for deployments where high volumes of workflows are executed and credentials need to be retrieved frequently.



SECRETS MANAGER INTEGRATION

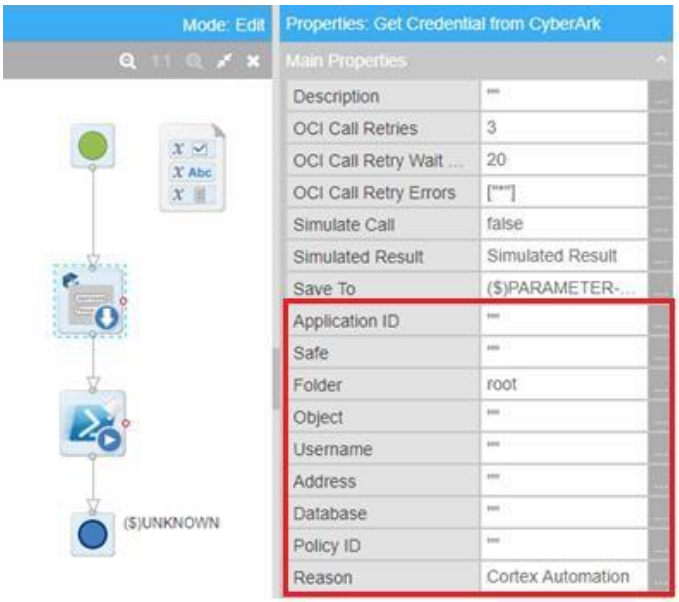
A typical CORTEX platform will consist of a Development server, a Production server, and a separate server with a system database and hosting the Gateway web portal to access the platform.

Depending on the demand to be serviced, additional Production servers (hosting the CORTEX Flow Engine) can be deployed and workload diverted to such servers. Additional servers will normally each have their own dedicated local CyberArk Secrets Manager installed, although a model of use where a shared Secrets Manager is used can also be supported.

CORTEX workflows are constructed using graphical blocks to configure actions or integration with external systems. The CyberArk integration has been implemented as a “Get Credential from CyberArk” block which is depicted below.

When there is need within a workflow to retrieve credentials to access external systems the flow designer will configure the block with the relevant details for the required credential. The block provides the full spectrum of query parameters supported by the Secrets Manager, namely Application ID, Safe, Folder, Object, Username, Address, Database, Policy ID, and Reason. There are also various other configuration properties, which are standard for CORTEX Interface blocks.

An example of what this will look like on the CORTEX Studio Flow Design UI is shown below, with the CyberArk specific properties outlined.



CREDENTIAL RETRIEVAL

The CORTEX workflow can be triggered in a variety of ways. This includes:

- By an end user from the CORTEX LivePortal web interface that gives access to a set of Service Requests (Flows), based on user authorization as centrally configured in Active Directory.
- From an external event sourced from a variety of platforms over protocols, such as SNMP.
- From an external user interface or platform. For example, a service desk application via an inbound REST web service call to CORTEX.

At runtime, the CORTEX engine will process the triggered workflow and during execution when it reaches a CyberArk "Get Credential" block it will call out to the CyberArk Secrets Manager to fetch the required credentials.

Such credentials will be returned in CORTEX proprietary encrypted format (using AES-256), to be used during the further execution of that flow. The credentials will typically be utilized in further CORTEX flow blocks for connecting to and interacting with external systems. Once the flow has been completed, the credential automatically goes out of scope and is cleared from memory.

Frequency of credential retrieval will vary depending on the customer flow implementation and the volume of flow executions. This can range from multiple requests per second, to infrequent requests.

SECRETS MANAGER INSTALLATION

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

The Secrets Manager Credential Provider should be installed on each CORTEX Application Server that hosts the CORTEX Flow Engine. Specific configuration steps are detailed in the next section.

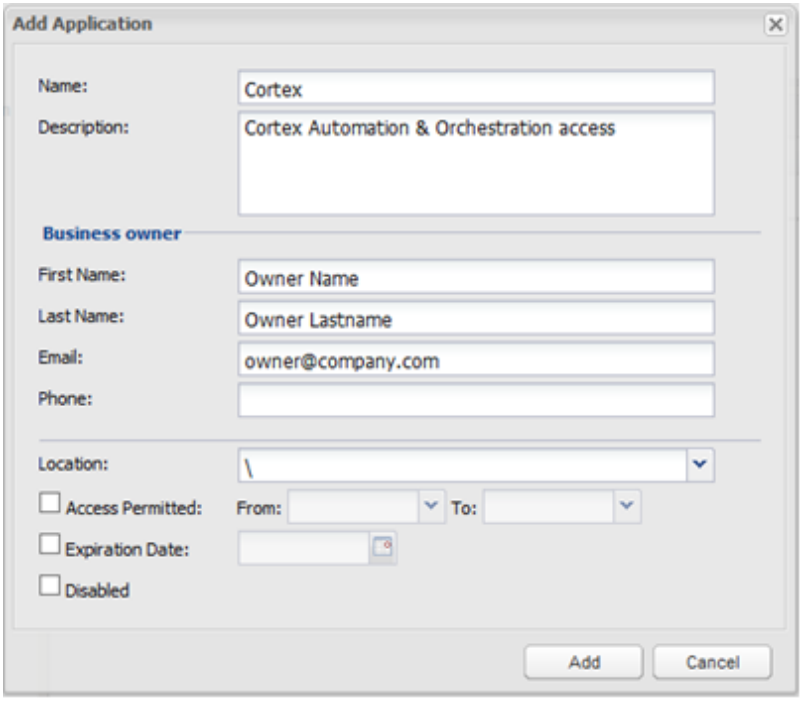
SECRETS MANAGER CONFIGURATION

The following sections provide details on CORTEX Automation & Orchestration Platform configuration with CyberArk Secrets Manager.

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

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

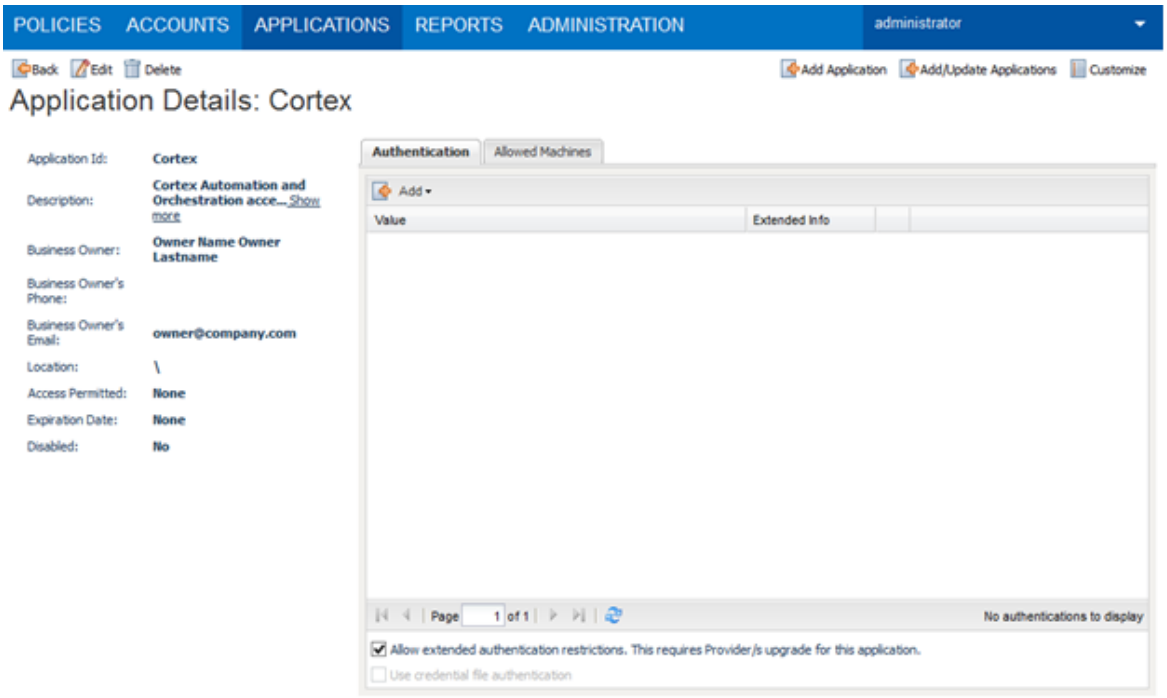
☐ Log in as user allowed to manage applications (it requires Manage Users authorization)
☐ In the Applications tab, click **Add Application**. The Add Application page appears.



☐ Specify the following information:

- In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: Cortex
- 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.

☐ Click **Add**. The application is added and is displayed in the Application Details 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. **Note:** CORTEX recommends that multiple authentication characteristics are specified to provide maximum security, in line with the customer's agreed CyberArk policies. As a minimum this should include the OS user, application path and application hash.
The values specified should match the relevant values as per the installation of the CORTEX Generic Interface service, which would normally be:

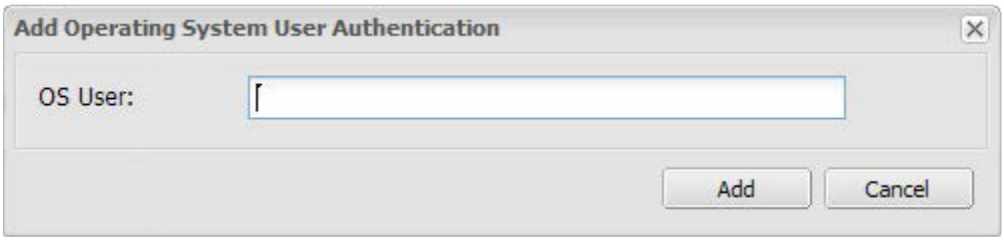
- OS user = The OS User that the CORTEX Generic Interface service is running under, typically "NT AUTHORITY\SYSTEM". Domain user accounts can also be used if required.
- Application path = The path that the CORTEX Generic Interface service is installed in, typically "C:/Program Files (x86)/Cortex/Cortex Generic Interface Service".
  Note: The directory\folder separator needs to be entered as a "/" character otherwise this will not work and access will not be possible.
- Application hash = As calculated in step 7 below.
  Note: For the CORTEX application the hash value for 4 different DLLs must be generated and individually added to the Application Authentication configuration, in order for authentication to succeed. The respective DLLs are:

- Innovise.Cortex.Server.Api.CyberArk.DLL
- Innovise.Cortex.Server.Api.CyberArkClient.DLL
- Innovise.Cortex.Server.Core.DLL
- mscorlib.dll

☐ In the Authentication tab, click **Add**. A drop-down list of authentication characteristics is displayed.

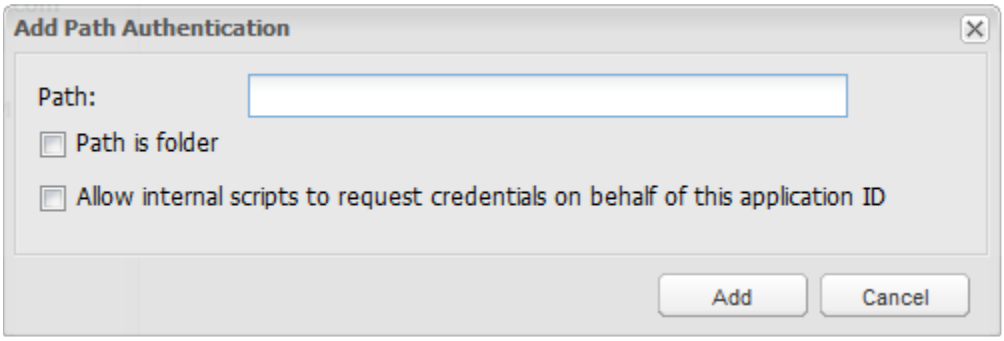
☐ Select the authentication characteristic to specify.

☐ Select **OS user**. The Add Operating System User Authentication window appears.



☐ Specify the name of the OS user who will run the application, then click **Add. T**he OS user is listed in the Authentication tab.

☐ Select **Path**. The Add Path Authentication window appears.

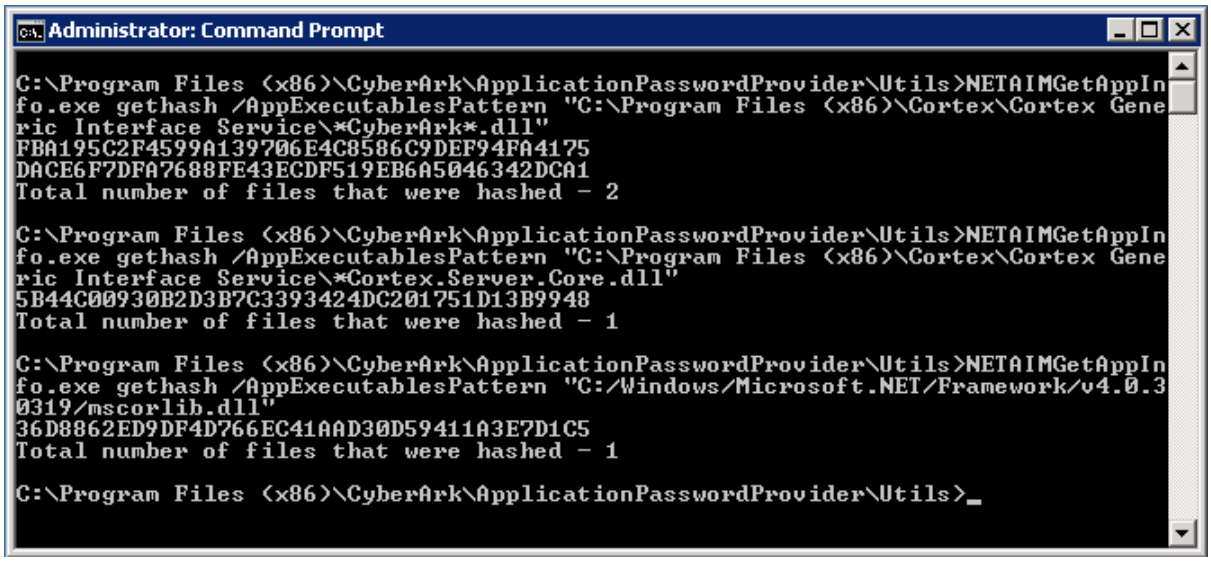


☐ In the **Path** box, specify the path where the application will run. To indicate that the specified path is a folder, select **Path is folder**. To allow internal scripts to retrieve the application password for this application, select **Allow internal scripts to request credentials on behalf of this application ID**.

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

☐ Specify a hash:

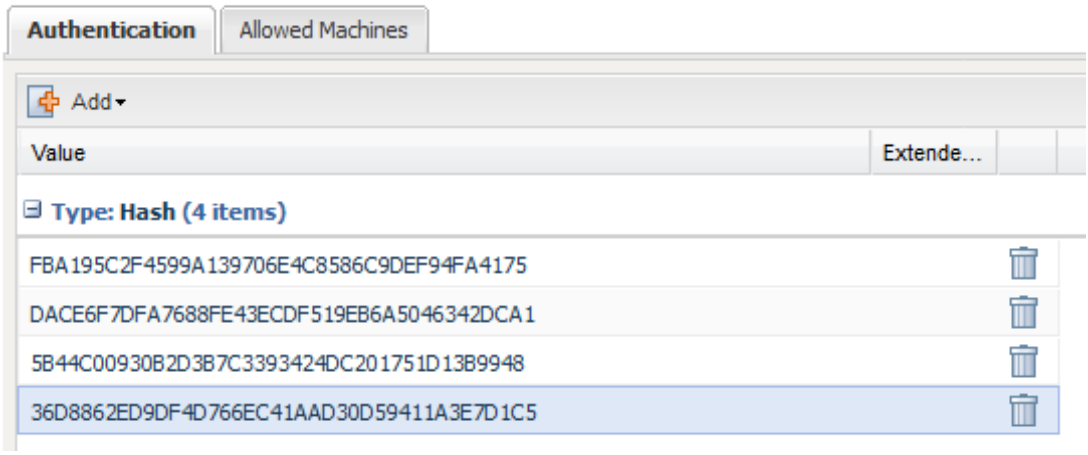
- Run the NETAIMGetAppInfo utility to calculate the application's unique hash. Copy the hash value that is returned by the utility.



- In the PVWA, select **Hash**. The Add Hash window appears.

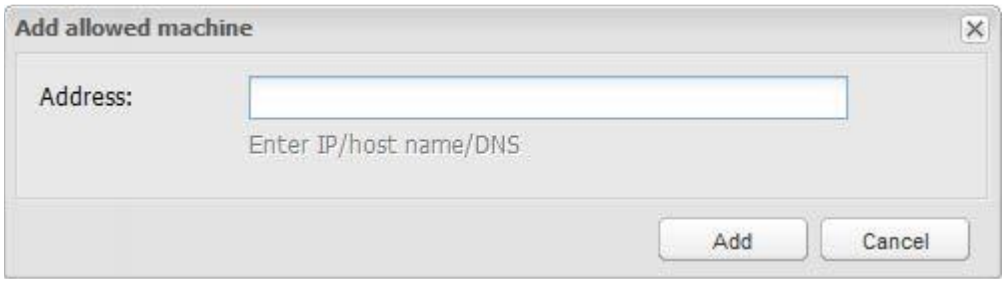
- In the Hash edit box, paste the application's unique hash value, or secify multiple hash values with a semi-colon. You can add additional information in a comment after each hash value specified for an application by specifying '#' after the hash value, followed by the comment.
  For example, OE883B7OD5B6E3EE37D37198049C9507C8383DB6 **#app2**
  Note: The comment must not include a colon or a semicolon.
- Click **Add**. The Hash is added as an authentication characteristic with the information that you specified.
- The hash value for each of the relevant DLLs must be entered as individual items, following the steps above.

  To illustrate, the configuration should be similar to the screenshot below once complete:



☐ 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.

  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.

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.**

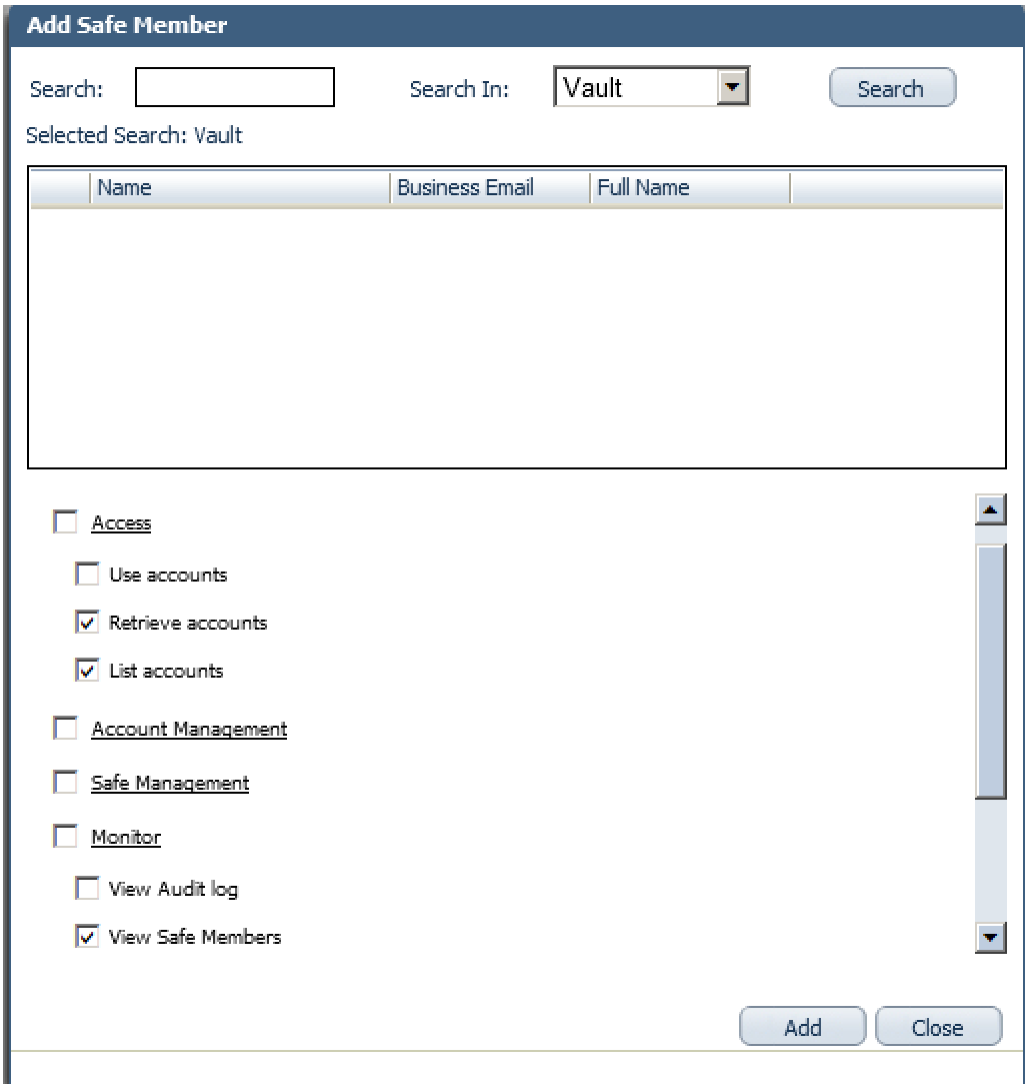
Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application.

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:

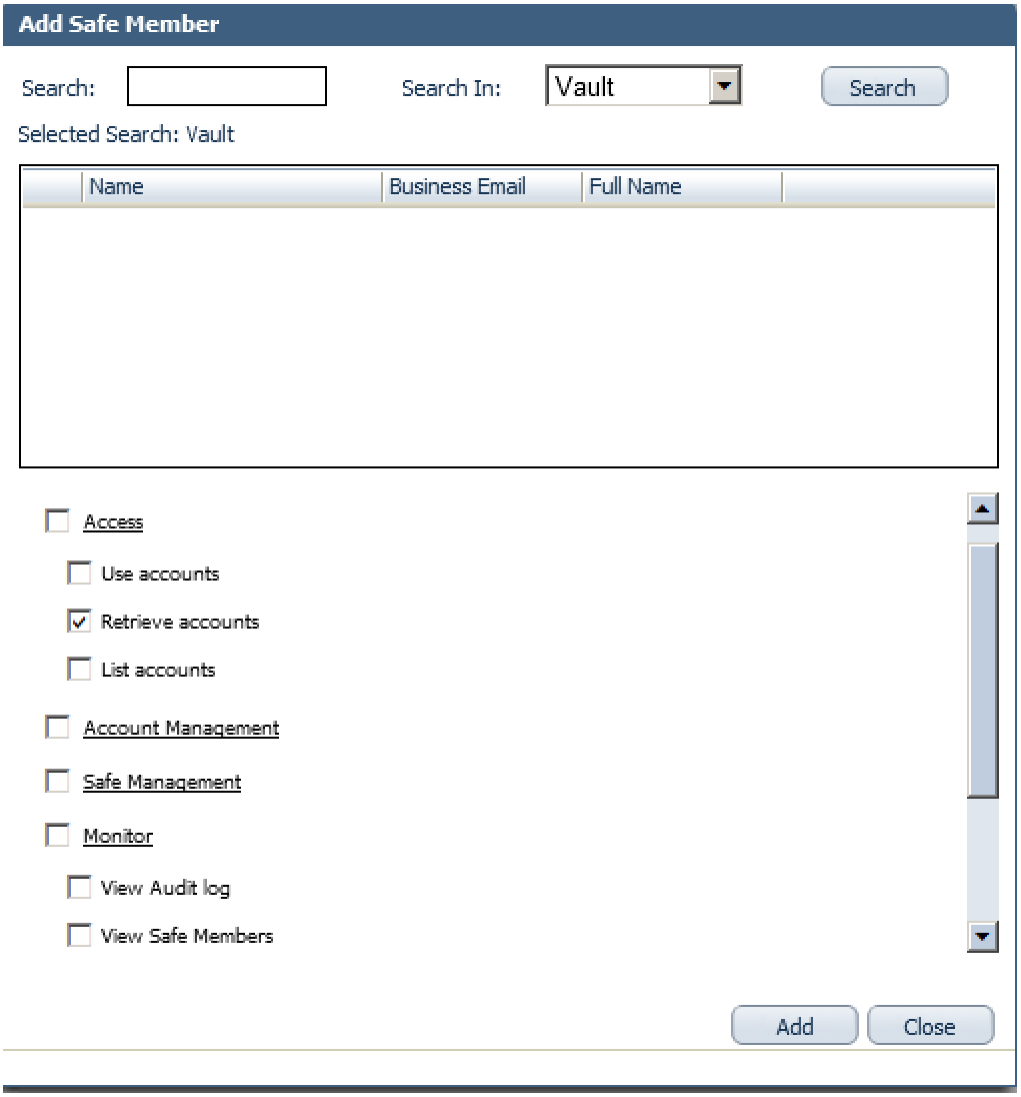
- List accounts
- Retrieve accounts
- View Safe Members

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.

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

CORTEX AUTOMATION & ORCHESTRATION PLATFORM INSTALLATION & INTEGRATION CONFIGURATION

Refer to **CORTEX Installation Guide** for CORTEX Automation & Orchestration Platform installation.

The CyberArk integration is handled by the CORTEX Generic Interface service which is part of a default CORTEX deployment and with installation details as per the **CORTEX Installation Guide**.

The configuration parameters that need to match up with the configuration within the CyberArk vault are covered in the previous section i.e. **Secrets Manager Configuration -> Defining the application id (Appid) and authentication details**. These parameters are:

- The **OS User**
- Installation **Path**
- **Hash keys** for the **CORTEX Generic Interface service DLLs**

When a flow designer needs to set up credential retrieval within a workflow, this is done by drag-dropping the "Get Credential from CyberArk" block from a palette onto a flow workspace and configuring a relevant subset of properties. The **CORTEX Block Help documentation** contains full details of the different options available.

For example, to retrieve credentials for an SSH server, the following can be specified:

Application ID	Cortex
Safe	TEST
Folder	""
Object	""
Username	root
Address	192.168.1.101
Database	""
Policy ID	""
Reason	Cortex Automation

In this example the **Application ID**, **Address**, **Username**, and **Reason** fields are populated and the others are left blank.

The "Get Credential from CyberArk" block supports any valid combination of the properties as supported by the CyberArk Secrets Manager.

When the flow is executed (at runtime) the call will be made to the CyberArk Secrets Manager to get the credentials. A structure with the relevant details will be returned, as illustrated below.

```
{
  "USERNAME": "root",
  "CONTENT": "#_1031190031071411!0112201342261860150441430531242111
  "ADDRESS": "192.168.1.101",
  "DATABASE": "",
  "PASSWORDPROPERTIES": {
    "CREATIONMETHOD": "PVWA",
    "CPMDISABLED": "NoReason",
    "DEVICETYPE": "Operating System",
    "USERNAME": "root",
    "POLICYID": "UnixSSH",
    "ADDRESS": "192.168.1.101"
  },
  "POLICYID": "UnixSSH"
}
```


Note that the “Content” field, which contains the password, is in CORTEX encrypted format and can only be decrypted and used by other CORTEX interface blocks to interact with the relevant target system. For example, when opening an SSH connection.

Any exceptions during the “Get Credential from CyberArk” operation will be tracked and handled in the configured exception handler for the flow, which could include making details available for troubleshooting purposes.

>>Replace this with your actual configuration options.

Common use cases:

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

2. Local accounts (windows/Unix)
    a. The user will specify: username & platform
    b. Safe name – optional but recommended for increasing performance
    c. When scanning, need to request in the API these username and platform, and add the address of the current machine being scanned

3. Non-standard credentials (can’t be unique with username+address+Platform)
    a. The user will specify: Safe and object name (folder is usually root by default)

PARTNER CONTACT INFO

Business Contact	Name	Paul Arnold
	Email	paul.arnold@wearecortex.com
	Tel	+44 (23) 8254 8993
Technical Contact	Name	Jaco de Wet
	Email	jaco.dewet@wearecortex.com
	Tel	+44 (23) 8254 8993
Support Contact	Name	Andrew MacDonald
	Email	servicedesk@wearecortex.com
	Tel	+44 (23) 8254 8993