



CYBERARK SECRETS MANAGER

(Agentless Central Credential Provider CCP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Kofax Inc.

Website: www.kofax.com

Name of Product: Kofax RPA

Version: 11.0

Date: December 2019 (Revised 22 May 2021)

KOFAX RPA OVERVIEW

Kofax RPA is the market-leading, AI-powered solution that combines robotic process automation, business process management, process mining, and cognitive document automation. Kofax RPA drives organizational efficiencies and empowers organizations to achieve operational excellence, optimize customer engagement and retention, and control business costs.

Kofax RPA is the fastest and most efficient way for you to acquire, enhance and deliver information from virtually any application or data source—including websites, portals, desktop applications, and enterprise systems—without any coding.

Version: 11.0

KEY BENEFITS

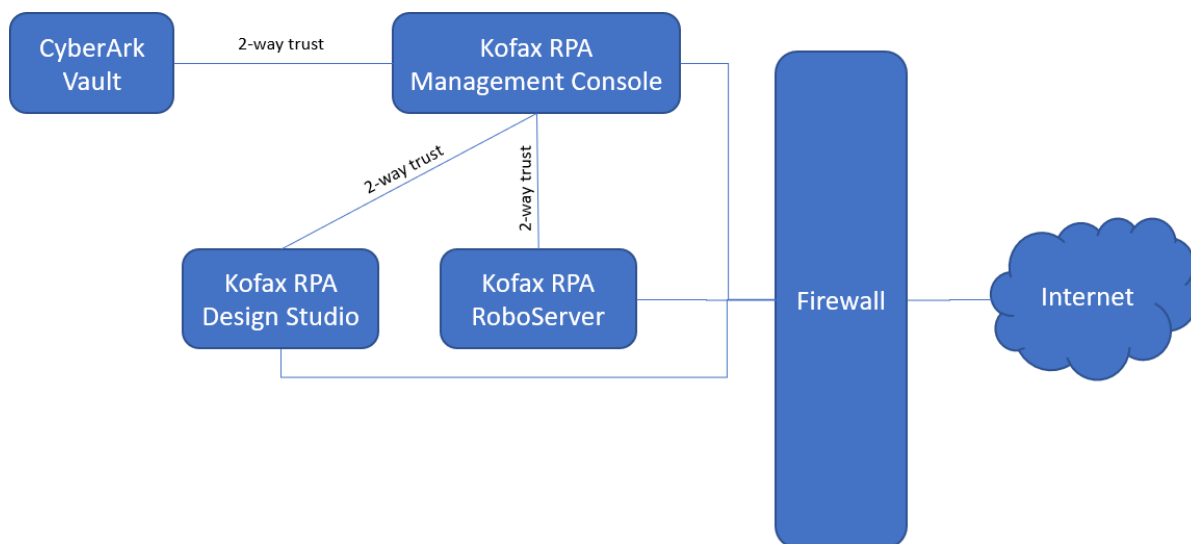
Benefits of Kofax RPA:

- Delivers leap-level robotic process automation that empowers you to achieve operational excellence with your workforce of the future—combining the desired mix of employees and digital robots
- Delivers efficient, accurate processes that optimize the quality of your customer engagement and improves customer loyalty and retention
- Integrates legacy systems and streamlines processes to maximize the efficiency of your employee and digital workforce and, more precisely, control business costs

Benefits of integrating Kofax RPA with CyberArk Secrets Manager:

- Centrally secure and manage RPA administrator, robot designer, and software robot credentials in a secure digital vault

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



SECRETS MANAGER INTEGRATION

Three Kofax RPA components retrieve credentials information from the CyberArk vault. The three components are:

- The Kofax RPA Management Console
- The Kofax RPA Design Studio
- The Kofax RPA RoboServer

In a typical installation, all these components are typically on the same corporate intranet. The Kofax RPA RoboServer and Kofax RPA Design Studio execute processes (called robots) that, in some cases, require credentials from the CyberArk vault.

An administrator can access the Kofax RPA Management Console and allow individual Design Studio instances or individual robots access to a specific set of credentials.

CREDENTIAL RETRIEVAL

When the Design Studio instance or the RoboServer instance executes the robot, retrieval of the credentials is initiated by requesting the credentials from the Management Console through a secure connection and carrying a secure token.

The Management Console acquires the credentials from the CyberArk vault using the REST API provided that the mapping between the requested credentials and the security token in the request match. The credentials are sent in clear text to the Design Studio or the RoboServer executing the robot.

SECRETS MANAGER INSTALLATION

Refer to the “Credential Provider Implementation Guide” for CyberArk Agentless installation and configuration.

SECRETS MANAGER CONFIGURATION

The following sections provide details on [Product Name] 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.

Add Application

Name: ManagementConsole

Description: Kofax RPA Management Console

Business owner

First Name:

Last Name:

Email:

Phone:

Location: \

☐ Access Permitted: From: To:

☐ Expiration Date:

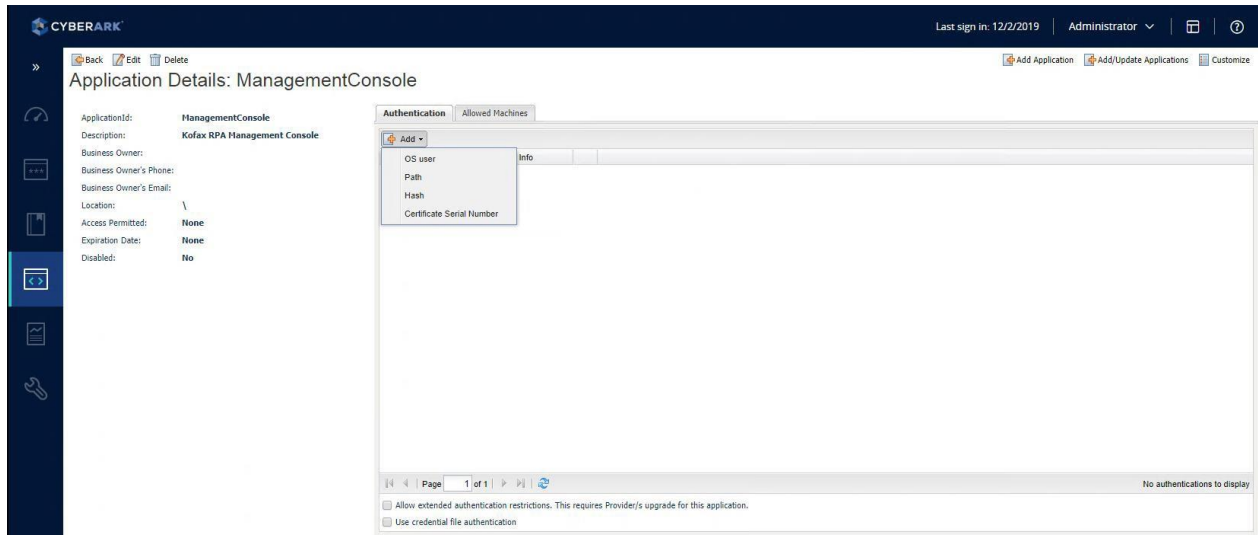
☐ Disabled

Add Cancel

☐ Specify the following information:

- In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: ManagementConsole
- 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.
- ☐ 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**. The OS user is listed in the Authentication tab.
- ☐ Specify the Certificate Serial Number.

Instructions on how to get the Certificate Serial Number:

Windows:

Start -> certmgr.msc (Current User) -> expand Personal -> select Certificates -> double-click on certificate to open

Start -> certlm.msc (Local Computer) -> expand Personal -> select Certificates -> double-click on certificate to open

If the first two options do not work in your env:

Start -> mmc.msc -> File; Add/Remove Snap-in -> Certificates -> Add -> OK -> you may be prompted to choose Local Computer or Current User -> OK

Expand Certificates -> Personal -> Certificates -> Double-Click on a certificate to open.

Once the certificate is open -> Details tab -> Serial Number is in the list of values shown

Once the certificate is open

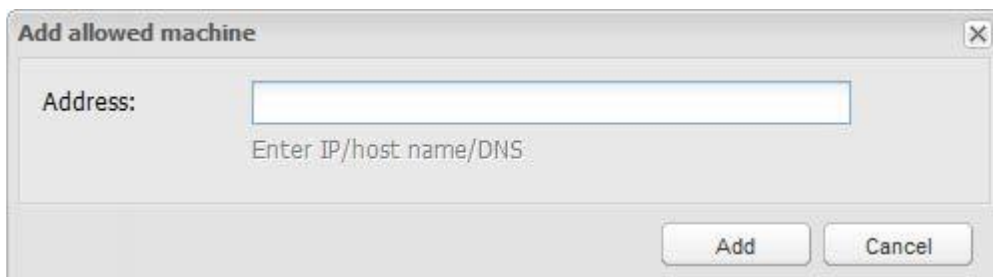
OpenSSL

openssl x509 -in <cert file name> -serial -noout

- This is the most secure way to authenticate the application for CCP
- The following are enhanced ways of authenticating

☐ Specify the application's Allowed Machines. This information enables Secrets Manager 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.

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 provider user (where the Central Credential Provider is installed) 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.

keystore for each purpose) are intended to be used for the Central Credential Provider web service and for Kofax RPA (the client).

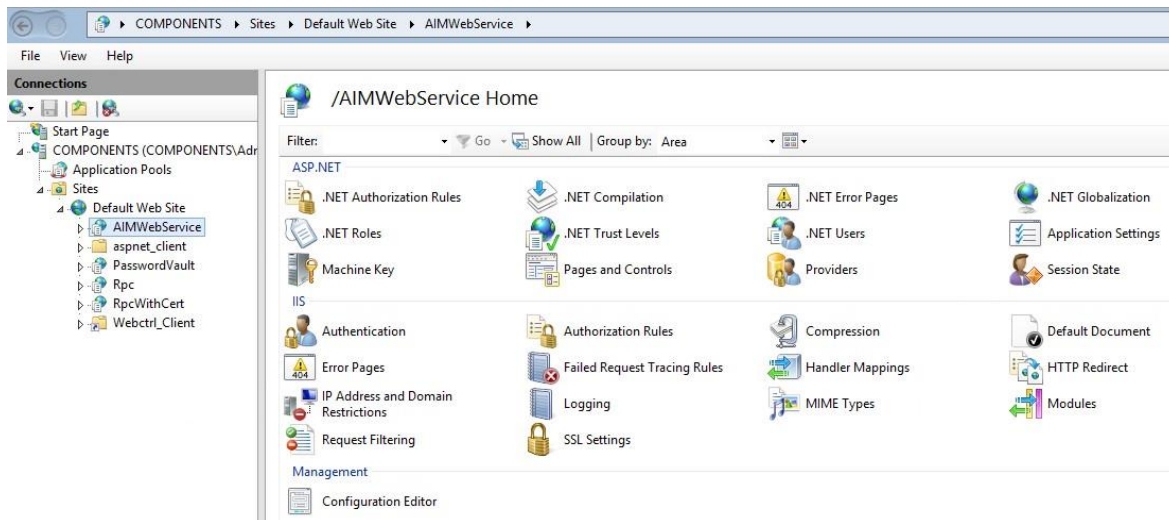
To generate a keystore, you can use, for example, a Java Runtime Environment keytool or an OpenSSL library.

Important: Always use strong passwords for the keystores to ensure maximum security of your data.

Then, extract the certificates from the keystores for further configuration.

2. Install the CyberArk Central Credential Provider application. See the CyberArk Central Credential Provider Implementation guide for more information on how to install the application.

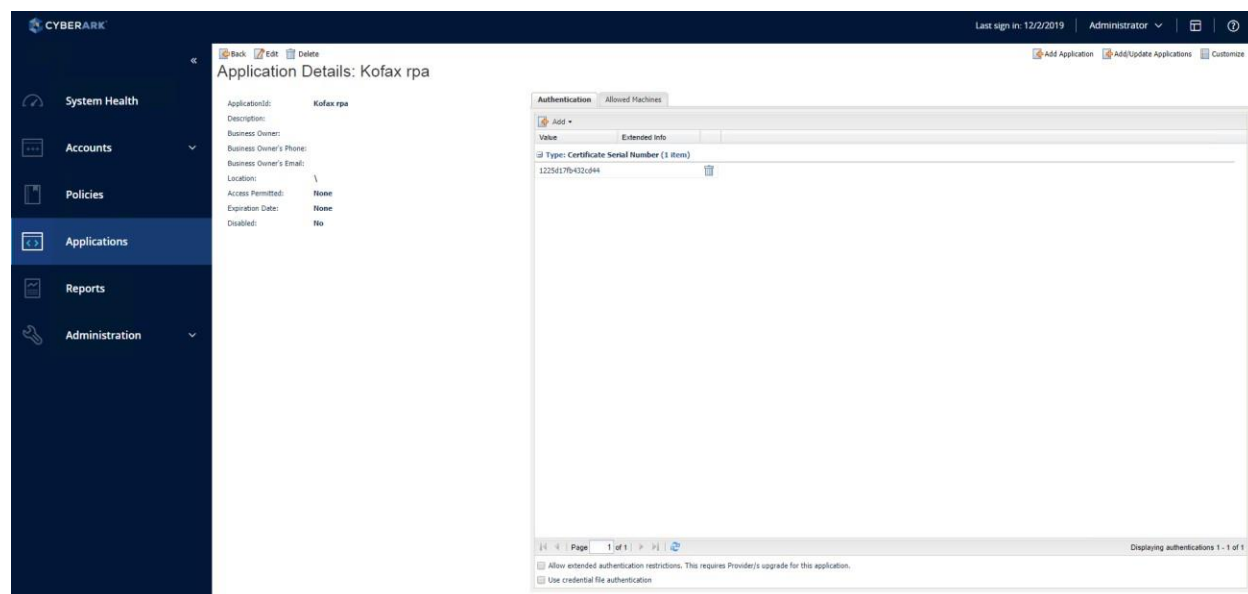
By default, an instance of the installed application is titled *AIMWebService* and looks similar to the following:



Note that Kofax RPA communicates with the Central Credential Provider through TLS (SSL) using client authentication for Kofax RPA.

3. Configure the CyberArk Password vault. For example, you can configure it in the Privileged Vault WebAccess under the Application tab.

Add an application to use with Kofax RPA. Navigate to the Applications tab and click **Add Application** in the upper right corner of the page to add an application.

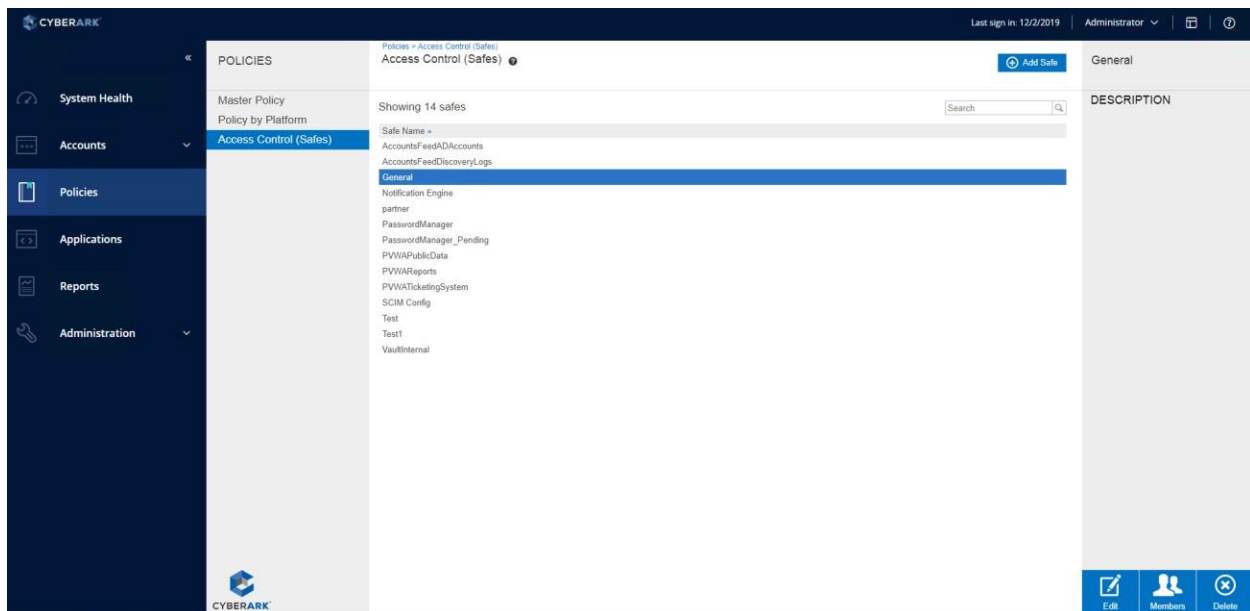


CyberArk provides the following application authentication methods. We recommend that you use one of these authentication methods or both methods together:

- Client certificates: A signed certificate that enables Kofax RPA authentication of the requesting application against the Central Credential Provider web service. Applications can authenticate with either a self-signed certificate or a certificate signed by a Certificate Authority
- Allowed machines: The list of allowed machines, based on IP or DNS, from where an application can run. Multiple addresses can be specified for a single application ID, which enables multiple instances of a single application to run on different machines and use the same application ID

The Central Credential Provider verifies the specified addresses each time it receives a request from the application.

Each application needs access rights to the account entry safe. To grant the rights, navigate to **Policies > Access Control (Safes)** and select an application to grant access rights to.



Click **Members** in the lower right corner of the page to provide a credential provider identificatory for the safe record. Use the provider user name that you specified in the Credentials Provider installation. Then, provide the Application IDs to grant access rights to.

4. Finally, edit the Configuration.xml file located under /WEB-INF to use CyberArk as an external password manager instead of the Kofax RPA built-in password manager.

By default, the configuration is as follows:

```
<bean id="passwordStore" class="java.lang.String">
<constructor-arg value="STANDARD"/>
</bean>
```

Change it to:

```
<bean id="passwordStore" class="java.lang.String">
<constructor-arg value="CYBERARK"/>
</bean>
```

Save the Configuration.xml file to complete the configuration.

For further information on using CyberArk with Kofax RPA, see *Help for Kofax RPA*.

When Kofax RPA is deployed using Docker, specify the following variables in the environment section of the Management Console service of docker-compose file:

environment:

- CONFIG_PASSWORDSTORE=CYBERARK
- SETTINGS_CYBERARK_URL=https://localhost
- SETTINGS_CYBERARK_PORT=443
- SETTINGS_CYBERARK_IISAPPLICATIONNAME=AIMWebService

For the configuration with a self-signed certificate, specify the following variables:

environment:

- CONFIG_PASSWORDSTORE=CYBERARK
- SETTINGS_CYBERARK_URL=https://localhost

- SETTINGS_CYBERARK_PORT=443
- SETTINGS_CYBERARK_IISAPPLICATIONNAME=AIMWebService
- SETTINGS_CYBERARK_CERTIFICATEPATH=/usr/local/tomcat/root.cer

Important: If the parameters are changed or not provided, connection to the CyberArk server cannot be established, and the Management Console does not start.

CYBERARK CONFIGURATION IN KOFAX RPA

In the Kofax RPA Management Console, open the CyberArk tab and fill in the following properties to configure the credentials.

Property	Description
CyberArk URL	Specify the URL of the CyberArk's Central Credential Provider host.
CyberArk Port	Specify the port number for the CyberArk's Central Credentials Provider host.
IIS Application Name	Type the CyberArk application name specified in the Internet Information Services (IIS).
Server Certificate	Upload the TLS server certificate of the CyberArk Central Credential Provider.

Then open the CyberArk Key Stores tab and upload CyberArk key stores.

1. Click the Upload CyberArk Key Store button.
2. Fill in the following properties to configure credentials.

Property	Description
Application ID	Type the ID specified on the CyberArk Applications list.
Key Store File	Upload the key store with a certificate private key pair to authorize the application in the CyberArk.
Store password	Type a key store password.

3. Click Upload to upload a CyberArk Key Store file.

4. Click Save.

PARTNER CONTACT INFO

Business Contact	Name	Niki Mench
	Email	Niki.Mench@kofax.com
	Tel	
Technical Contact	Name	Kofax Sales Support
	Email	Sales Support - Americas: SSR.AMS@kofax.com Sales Support - EMEA: SSR.EMEA@kofax.com Sales Support - Asia: SSR.APAC@kofax.com
	Tel	
Support Contact	Name	Kofax Technical Support
	Email	Detailed contact information Support
	Tel	