

Storing passwords in a vault

You can use a vault to store the OpenPages database user password, the OPSysSystem user password, or both.

This topic applies to IBM OpenPages with Watson traditional on-premises and IBM OpenPages with Watson on Cloud.

Before you begin

- You need a [CyberArk](#) vault.
- Request an SSL certificate from your CyberArk administrator. The certificate is required to authenticate the connection between OpenPages and CyberArk.
- In CyberArk, create an Application for OpenPages. For more information, see the [CyberArk documentation](#).
- In CyberArk, add one or both of the following user accounts to the vault. Put the accounts into the same safe within the vault.
 - The OpenPages database user, for example `openpage`
 - The OPSysSystem user

About this task

When OpenPages needs a password, it retrieves it from the vault. When you need to change the password, you update it in the vault.

Procedure

1. Set up the SSL certificate keystore with the client certificate and server certificates:
 - a) Add the client certificate to the keystore. If the client certificate is in `.crt` or `.pem` format, convert it:

In this example, the client certificate is `cyberark-client.p12` and the keystore is `cyberark-ssl8.p12`.

```
keytool8 -importkeystore -srckeystore cyberark-client.p12 -srcstoretype pkcs12  
-destkeystore cyberark-ssl8.p12 -deststoretype pkcs12
```

- b) Add any server certificates to the same keystore by running the following command:

In this example, the server certificate is `cpd-cyberark1-chain.pem`.

```
keytool8 -importcert -file cpd-cyberark1-chain.pem -alias cpd-cyberark -keystore cyberark-  
ssl8.p12 -storetype pkcs12
```

- c) Copy the keystore file to the following directory on each application server: `<OP_HOME>/aurora/conf/`.
For example: `<OP_HOME>/aurora/conf/cyberark-ssl8.p12`

2. Configure the vault properties.
 - a) Log in to the application server and go to the `<OP_HOME>/aurora/conf/` directory.
 - b) Create a file called `vault.properties`.
 - c) Copy the following text into the file:

```

implementation=CyberArk
cyberark.safe=
cyberark.account=
cyberark.db.user=
cyberark.db.object=
cyberark.opsystem.object=
cyberark.keystore.file=
cyberark.keystore.pass=
cyberark.url=
cyberark.ssl.disable.hostname.verification=true|false
cyberark.keystore.type=pkcs12
cyberark.db.folder=
cyberark.opsystem.folder=

```

d) Configure the following properties in the file:

Table 208. Vault properties	
Property	Description
cyberark.safe	Type the name of the vault. For example: OpenPagesSafe
cyberark.account	Type the unique ID of the application (App ID) that you created in CyberArk for OpenPages.
cyberark.db.user cyberark.db.object	If you are storing the OpenPages database user password in the vault, complete these fields. • cyberark.db.user: Type the username of the OpenPages database user. The name must match the name in the vault. • cyberark.db.object: Type the account name (unique ID) of the object in your vault that stores the database password. For example: <pre>cyberark.db.user=openpage cyberark.db.object=Database-Oracle- openpage</pre>
cyberark.opsystem.object	If you are storing the OPSysytem password in the vault, type the account name (unique ID) of the object in your vault that stores the OPSysytem password.
cyberark.keystore.file	Type the absolute path to the keystore that contains the CyberArk server certificates. For example: <pre>/home/opuser/OP/OpenPages/auroara/conf/ cyberark-ssl8.p12</pre> An absolute file path is required because the same properties file will be used by multiple components that will have different relative path locations.
cyberark.keystore.pass	Type the password of your client certificate keystore.

Table 208. Vault properties (continued)	
Property	Description
cyberark.url	Type the HTTPS URL for CyberArk. For example: https://myserver-cyberark.com
cyberark.ssl.disable.hostname.verification	Set to false (default) unless the SSL server certificate and the hostname of the CyberArk environment are not the same. You might encounter this situation in non-production environments that use self-signed certificates.
cyberark.keystore.type	This property must be set to pkcs12.
cyberark.db.folder	Optional Specifies the CyberArk folder in the safe under which cyberark.db.object is located. Leave blank if you don't need this property.
cyberark.opsystem.folder	Optional Specifies the CyberArk folder in the safe under which cyberark.opsystem.object is located. Leave blank if you don't need this property.

3. If you're storing the database password in the vault, update the Liberty database data source files (op-ora.xml or op-db2.xml) on each application server.
 - a) Go to the <OP-HOME>/wlp-user/servers/<server-name>-OPNode1Server1 directory.
 - b) Open the op-ora.xml or op-db2.xml file.
 - c) Add the following jaasContextEntry elements:

```

<jaasLoginContextEntry id="vaultJAASLoginEntry" name="vaultJAASLoginEntry"
loginModuleRef="vaultLoginModule" />
<jaasLoginModule id="vaultLoginModule"
className="com.ibm.openpages.vault.jaas.VaultDBLoginModule" controlFlag="REQUIRED"
libraryRef="vaultJaasLibrary">
  <options VaultPropertiesPath="${openpages.home}/aurora/conf/vault.properties"/>
</jaasLoginModule>

<library id="vaultJaasLibrary">
  <fileset dir="${openpages.home}/aurora/lib" includes="com.ibm.openpages.vault.jar"/>
  <fileset dir="${openpages.home}/aurora/lib"
includes="com.ibm.openpages.vault.jaas.jar"/>
  <fileset dir="${openpages.home}/aurora/lib" includes="httpclient-*.jar"/>
  <fileset dir="${openpages.home}/aurora/lib" includes="httpcore-*.jar"/>
  <fileset dir="${openpages.home}/aurora/lib" includes="commons-logging-*.jar"/>
  <fileset dir="${openpages.home}/aurora/lib" includes="jackson-annotations-*.jar"/>
  <fileset dir="${openpages.home}/aurora/lib" includes="jackson-core-*.jar"/>
  <fileset dir="${openpages.home}/aurora/lib" includes="jackson-databind-*.jar"/>
  <fileset dir="${openpages.home}/aurora/lib" includes="bcprov-jdk15to18-*.jar"/>
  <fileset dir="${openpages.home}/aurora/lib" includes="aurora-tools.jar"/>
</library>

```

- d) Update both of the <dataSource...> elements in the file to add the following attribute:

```
jaasLoginContextEntryRef="vaultJAASLoginEntry"
```

- e) Remove the op.jdbc.password attribute from the nested properties of each of the dataSource elements.
 - f) Open the <OP-HOME>/wlp-user/servers/<server-name>-OPNode1Server1/bootstrap.properties file and remove the op.jdbc.password property.

- g) Repeat these steps on each application server.
- 4. If you're storing the database password in the vault and you are using an Oracle database, do the following steps:
 - a) Edit the `/home/opuser/OP/OpenPages/aurora/bin/op-backup-restore.env` file.
 - b) Set the following property:

```
VAULT_IMPLEMENTATION=CyberArk
```
 - c) Comment out or remove the `DB_OP_PWD` property.
 - d) Repeat these steps on each application server.
- 5. If you're storing the database password in the vault and you use Global Search, do the following steps:
 - a) If the global search server is on a different host than the application server, copy the `vault.properties` file and the certificate `.p12` file to the search server.
 - b) Edit the `/home/opuser/OP/OPSearch/opsearchtools/openpages_search.properties` file.
 - c) Change the line `OPSearchTool.DatabaseVaultProperties=` to the absolute path of the `vault.properties` file on the search server.
 - d) Comment out the `OPSearchTool.DatabasePassword` property.
 - e) Restart the search server.
- 6. If you're storing the OPSys password in the vault, do the following steps:
 - a) Open the `aurora.properties` file.
 - b) Remove or comment out the following property:

```
security.system.password
```
 - c) Repeat these steps on each application server.
- 7. Restart all application servers.
- 8. If you use Global Search, restart the search server.

What to do next

When you need to change the database password, update it in the vault. Next, update IBM Cognos Analytics with the new password. See [“Modifying the OpenPages database password in Cognos ”](#) on page 645.

Note: If you're using Global Search, do not use the `opsearchtool.sh` script to change the database password for the search server.

When you need to change the OPSys password, update it in the vault, and then run the `chn-g-sys-pswd` utility. See [“Changing the OPSys password”](#) on page 643.