



CYBERARK SECRETS MANAGER

(Agentless Central Credential Provider CCP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Liquibase

Website: www.liquibase.com

Name of Product: Liquibase Enterprise

Version: 7.4

Date: 25 June 2020 (Revised 26 October 2020)

LIQUIBASE ENTERPRISE OVERVIEW

Liquibase provides CI/CD for databases by automating database schema change. Liquibase runs on any platform that supports Java.

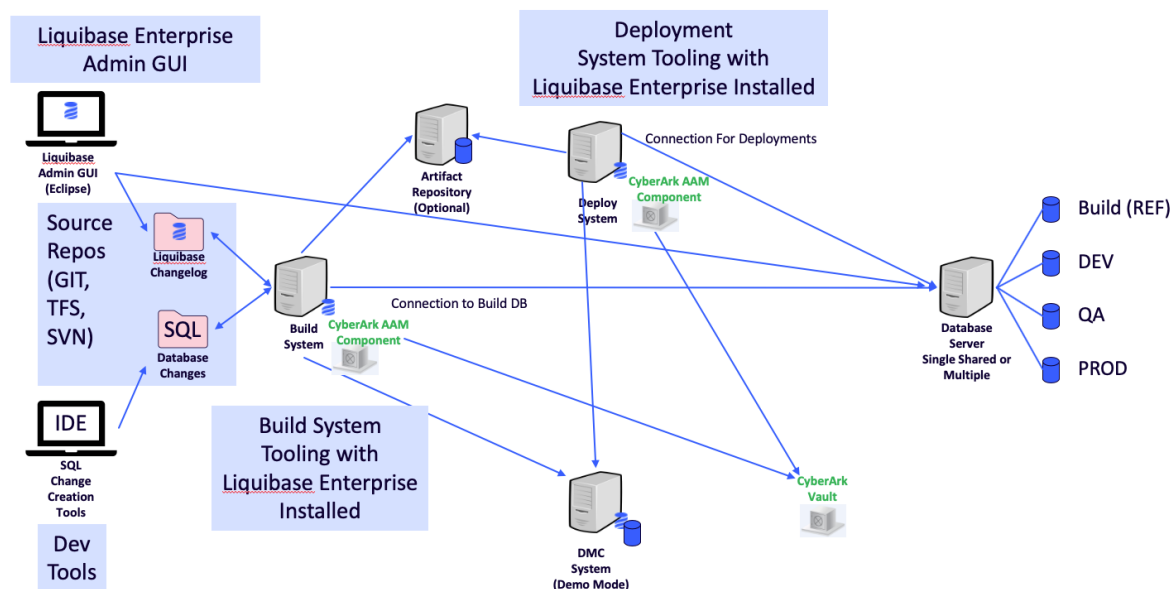
Version: 7.4

KEY BENEFITS

Database schema migration is a bottleneck for automating application delivery. Liquibase provides the “last mile of service” for automated CI/CD.

The primary reason Liquibase customers use CyberArk is to store and manage database credentials. Liquibase relies on CyberArk to provide credentials to connect and manage databases.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



SECRETS MANAGER INTEGRATION

Integration built into the deployment process of Liquibase Enterprise:

- CyberArk Secrets Manager is used to pull the user and password from the CyberArk Vault to connect to the databases that are built or deployed using the Liquibase Enterprise Command Line Interface

- Each agent that is deploying to a database will connect at deployment time to the Secrets Manager service. This connection allows the agent to gather the user and password and therefore connect and deploy updates to the database

CREDENTIAL RETRIEVAL

The credentials are retrieved at runtime. When the runtime credentials option is set for a project, Liquibase Enterprise checks where the credentials are specified. Credential locations are checked in the following order:

- Explicit credentials for an operation
 - CLI - You specify credentials in command options
- Environment variables

When using CyberArk to store database credentials, a new command called `hammer groovy getCyberarkCreds.groovy` command will be used to store the user and password in an environment variable to allow Liquibase Enterprise CLI to run

ENVIRONMENT VARIABLES

When the project is set to use runtime credentials and you run an operation from the GUI or the CLI, environment variables are checked.

Set the following environment variables to provide credentials for each database in your pipeline.

Environment variables	Description
DDB_USER DDB_PASS	Database credentials. Used for commands that operate on a single database: forecast, deploy, rollback, and package (<code>deployPackager.groovy</code>) operations.
DDB_USER_<dbDefName> DDB_PASS_<dbDefName>	Database credentials for an individual step (DbDef). Used only for groovy commands, including <code>deployPackager.groovy</code> . Note: The per-DbDef environment variables are checked first. If they are not set, then DDB_USER and DDB_PASS are checked.
DDB_REF_USER DDB_REF_PASS	Used with REFERENCE variables for commands that operate on two databases. <code>diff</code> <code>diffchangelog</code>
DDB_TARGET_USER DDB_TARGET_PASS	Used with TARGET variables for commands that operate on two databases.

	diff diffchangelog
DDB_DMCDDB_USER DDB_DMCDDB_PASS	Used to access the DMCDDB database. Operations cause entries to be entered in the DMCDDB database: forecast deploy

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 Liquibase Enterprise 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:

Description:

Business owner

First Name:

Last Name:

Email:

Phone:

Location:

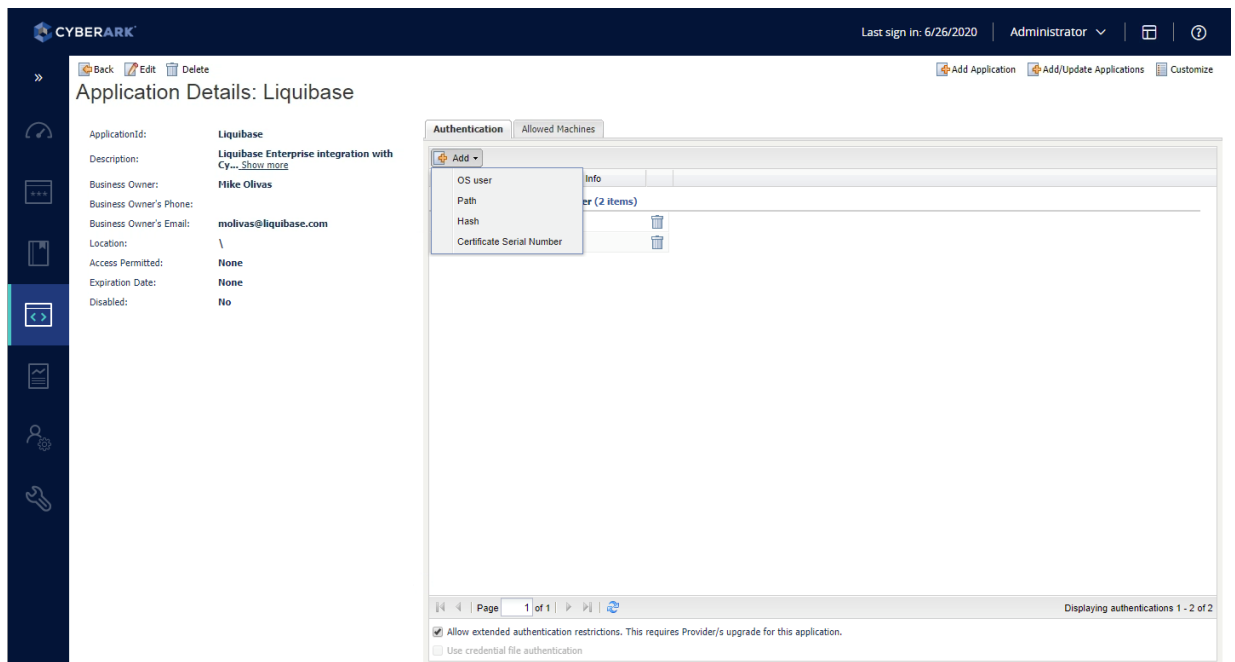
☐ Access Permitted: From: To:

☐ Expiration Date:

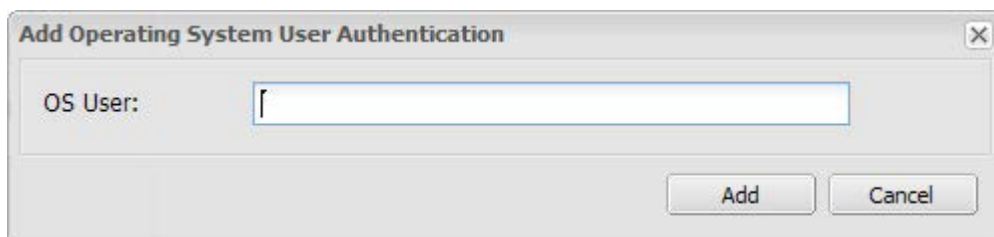
☐ Disabled

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

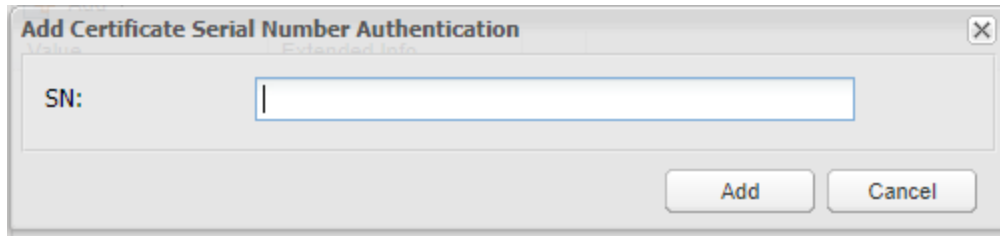
- ☐ Click **Add**. The application is added and is displayed in the Application Details page.



- ☐ 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. The use of certificate authentication is recommended.
- ☐ 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

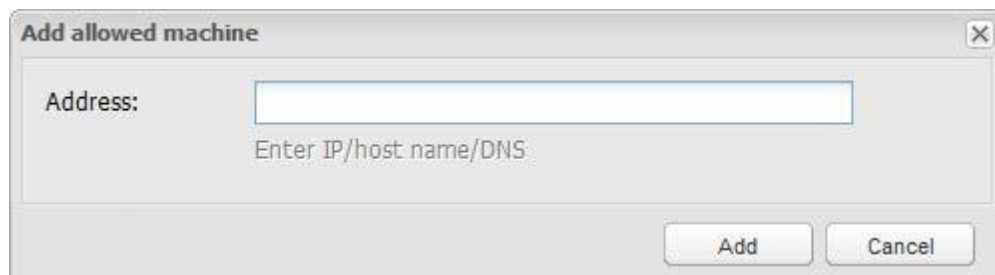
OpenSSL

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.

Add Safe Member

Search:

Search In:

Vault

Search

Selected Search: Vault

Name	Business Email	Full Name
------	----------------	-----------

☐ Access

☐ Use accounts

☒ Retrieve accounts

☒ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

☐ View Audit log

☒ View Safe Members

Add

Close

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

- Retrieve accounts

10

Add Safe Member

Search: Search In:

Selected Search: Vault Display 1 result(s)

Name	Business Email	Full Name
Liquibase	molivas@liquibas...	Mike Olivas

☐ Access

- ☐ Use accounts
- ☒ Retrieve accounts
- ☐ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

- ☐ View Audit log
- ☐ View Safe Members

☐ Workflow

- ☐ 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**.

LIQUIBASE ENTERPRISE INSTALLATION & INTEGRATION CONFIGURATION

Refer to [Datical Product Documentation](#) for Liquibase installation.

1. Download the getCyberarkCreds.groovy script from software.datical.com and copy it into the ..\DaticalDB\repl\scripts directory.
2. Download curl.exe or install curl on Linux
3. To use the command, use these parameters with your client certificate

```
hammer groovy getCyberarkCreds.groovy <cyberark_objectname> <caserver> <caserverport>  
<location_certfile> <location_pemfile> <dbDef> [location_rootca]
```

Required Parameters

<cyberark_objectname> - Object to lookup in Cyberark Vault

<caserver> - Fully Qualified Domain name of the Cyberark Server

<caserverport> - Port to use to connect to Cyberark Server (default: 443)

<location_certfile> - Fully qualified path to location of client certificate file

<location_pemfile> - Fully qualified path to location of client certificate pem file

<dbDef> - Database definition name as defined in the project file (for example: REF_DB)

[location_rootca] - Optional fully qualified location of rootca if the certificate is not in the truststore

Connect to Secrets Manager via hammer command to store database credentials in environment variables for hammer command line interface.

Partner Application UI:

Username:

Password:

☐ Use CyberArk Vault to fetch credentials:

Username:

Address:

Platform (PolicyID):

Safe:

Folder:

Object:

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	Robert Reeves
	Email	R2@liquibase.com
	Tel	(512) 422-2443
Technical Contact	Name	Mike Olivas
	Email	mike@liquibase.com
	Tel	(512) 656-3272
Support Contact	Name	Robert Reeves
	Email	R2@liquibase.com
	Tel	(512) 422-2443