SECRETS MANAGER INTEGRATION

(Agentless Central Credential Provider CCP)

SECRETS MANAGER - TECHNICAL DOCUMENTATION TEMPLATE

DOCUMENT PURPOSE: THIS TEMPLATE IS TO BE COMPLETED BY PARTNER AND IS REQUIRED FOR CYBERARK SECURED CERTIFICATION. THE AAM INTEGRATION TECHNICAL DOCUMENTATION WILL BE MADE AVAILABLE TO PARTNERS, CUSTOMERS AND PROSPECTS. **AS YOU COMPLETE EACH SECTION, PLEASE REMOVE THE DIRECTIONS PROVIDED.**

Name of Company: Gluware

Website: https://gluware.com/

Name of Product: Gluware Control

Version: 5.2

Date: 10/25/2023

PARTNER SOLUTION OVERVIEW

Gluware® Control is the centralized control panel for Gluware® Intelligent Network Automation applications. It is an on-premises or cloud-based software platform and orchestration engine that includes Dashboards, Data Explorer and Device Manager to service the Gluware Intent-Based Networking applications. Gluware Control helps network engineering and operations easily manage devices and software across dozens of vendors and operating systems including routers, switches, firewalls, load-balancers, WAN optimizers and wireless LAN controllers. Cloud-based or on-premises, Gluware Control lets you easily load and manage software packages and applications, create organizations for multi-tenant network management, administer users with role-based access, easily import devices and perform inventory.

Version: 5.2

Platform components:

- Gluware Control
- Device Manager
- Data Explorer
- Config Drift & Audit
- Config Model Editor
- OS Manager
- Topology
- Network RPA

KEY BENEFITS

Benefits of Gluware Control:

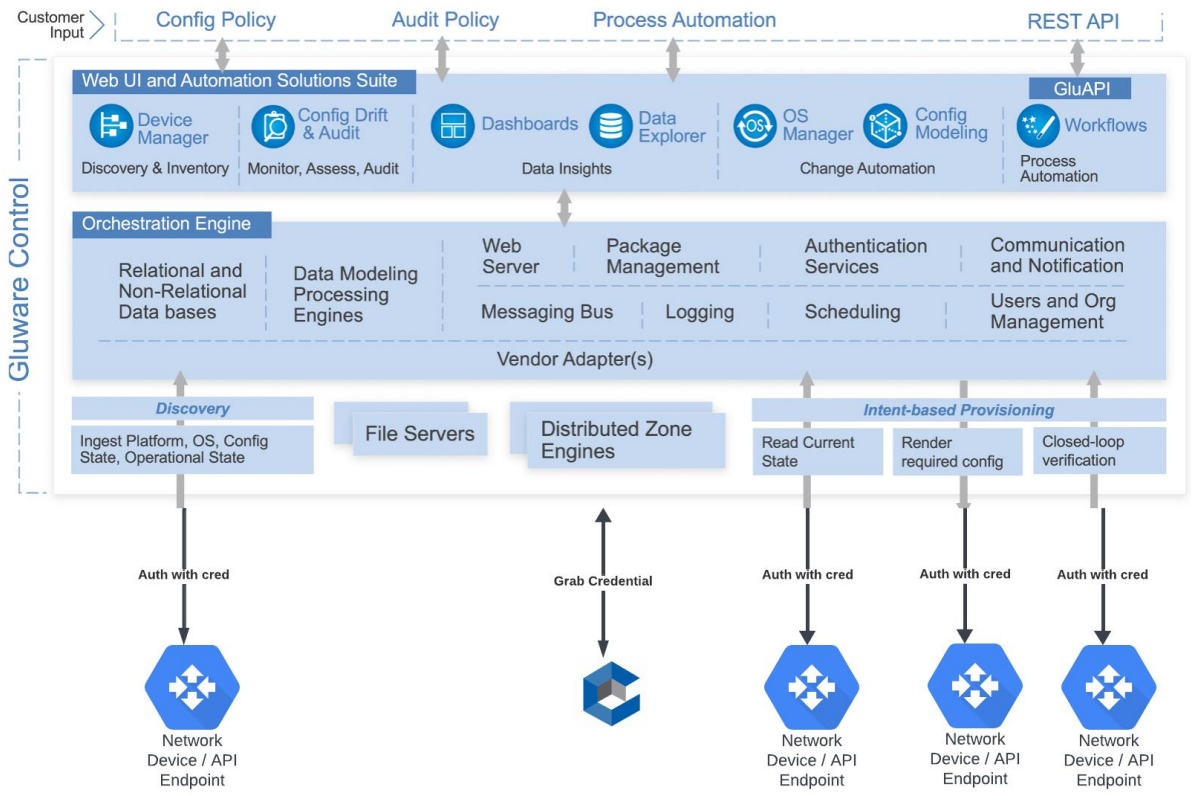
- Centralize and Automate network management
- Audit network device configs to maintain compliance
- Detect when drift from configuration standards occurs and auto-remediate
- Automate firmware updates
- Visualize network topology

Benefits of integrating [Product Name] with CyberArk AAM:

- Securely store network device credentials for Gluware in your preferred vaulting solution
- Conduct password lifecycle procedures with network device passwords used for Gluware

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

Insert Partner Product architecture diagram. Diagram should depict where the AAM integration is located within Partner Product architecture. Diagram should show how the AAM integration will be licensed with the partner product, where the main connection takes place.



AAM INTEGRATION

CyberArk is integrated as a password source for device or API credentials. We store all credentials in a vault and CyberArk is being added as an optional vault source.

- Integrated as a vault
- Integrated into Gluware Control (main server)

CREDENTIAL RETRIEVAL

- When Gluware Control needs to talk to a network device or an API endpoint, it connects with CyberArk to retrieve the proper credential.
- Every time a device or API endpoint connection is made CyberArk will be contacted for the most recent credential

REQUIREMENTS

List software, network, and hardware requirements. Provide context of requirements and team expertise for user planning needs.

- Requirement 1
- Requirement 2

AAM INSTALLATION

Refer to CyberArk Agentless installation and configuration.

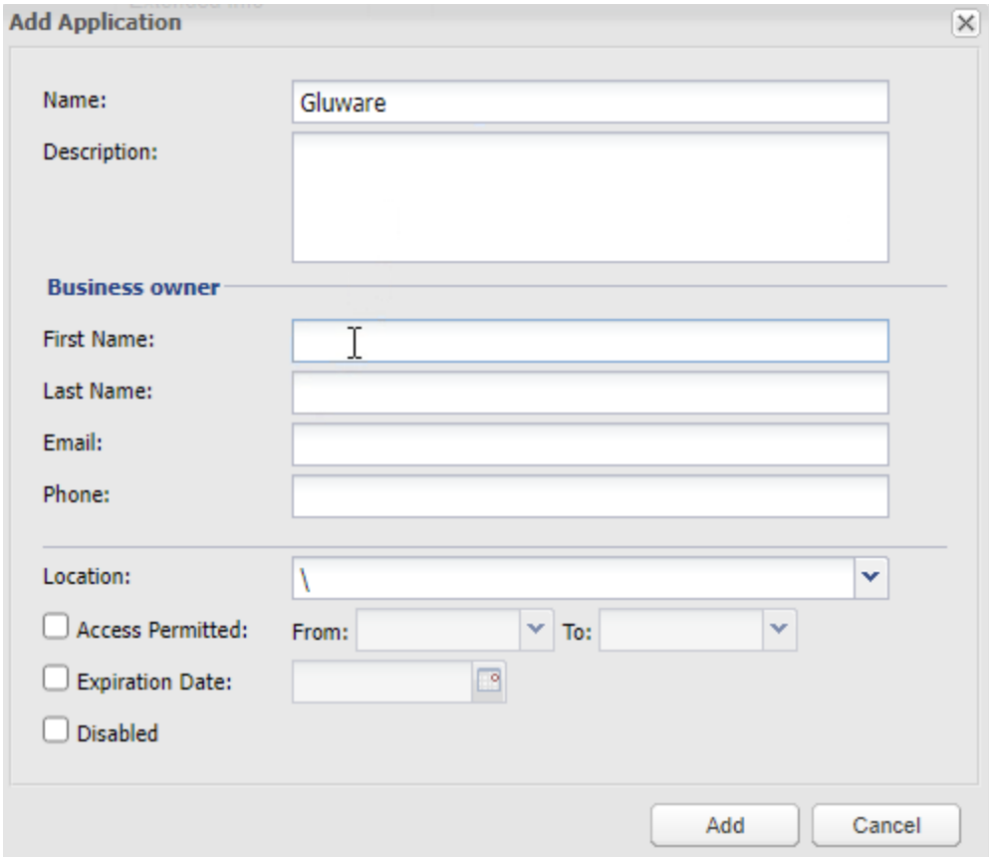
AAM CONFIGURATION

The following sections provide details on Gluware configuration with CyberArk AAM.

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: Gluware
  - 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.

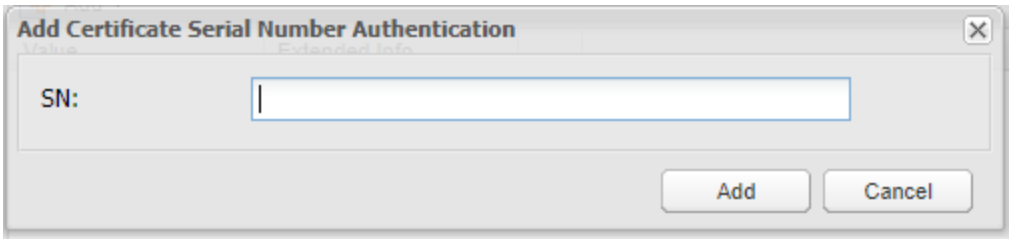
☐ Authentication from Gluware is handled in two ways – we use client certificates to authenticate the SSL session to the IIS and then we use vault user authentication to authentication Gluware and retrieve a token to be used in subsequent vault requests.

☐ Additionally you may configure certificate serial number authentication and allowed machines. This is not required for Gluware but may be useful to secure your AAM instance.

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

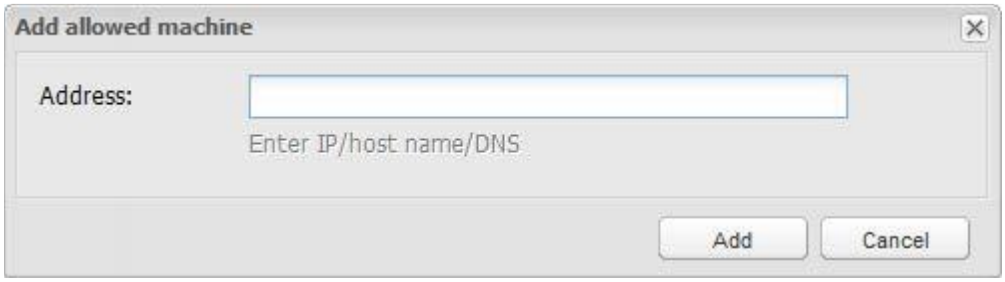
☐ Select the authentication characteristic to specify.

☐ Specify the Certificate Serial Number.



☐ Specify the application's Allowed Machines. This information enables AAM 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.**

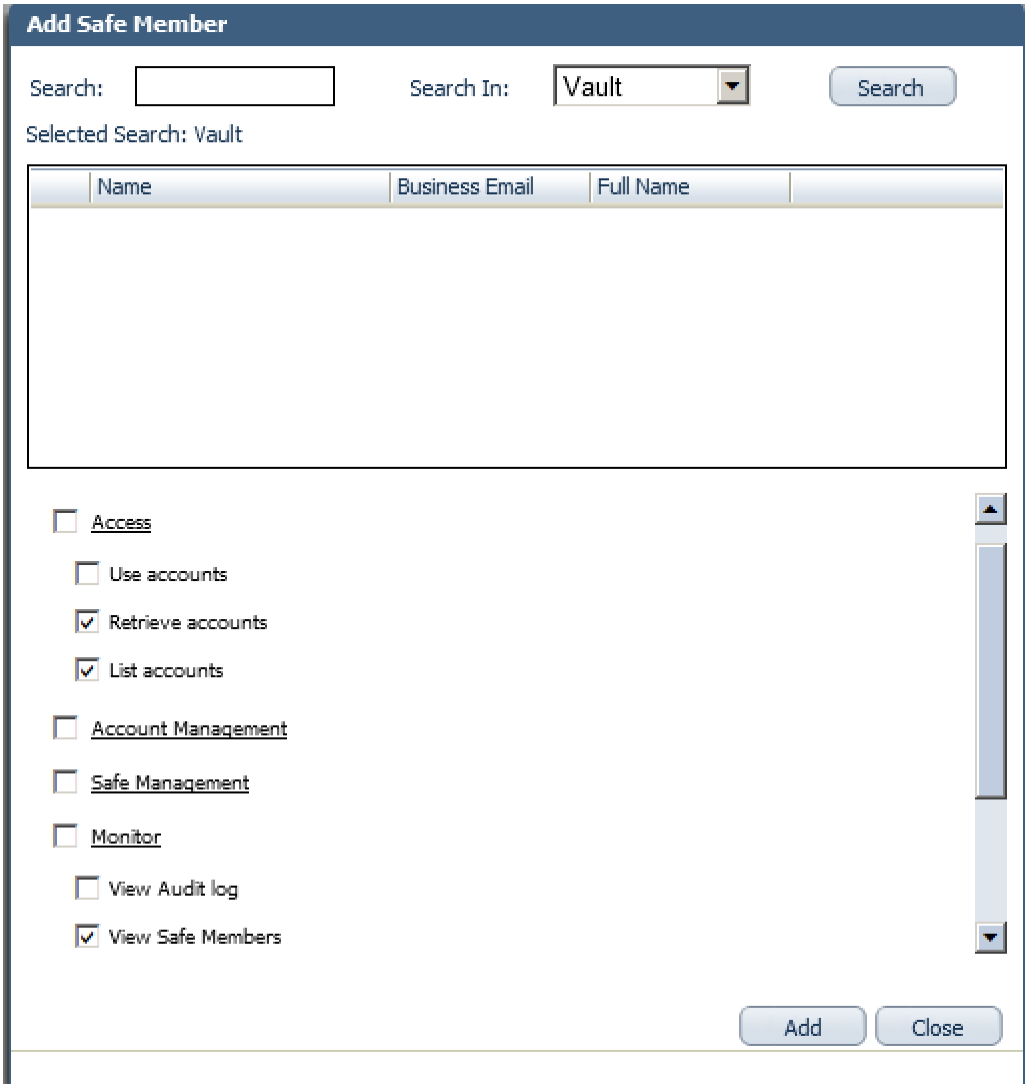
Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application.

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:

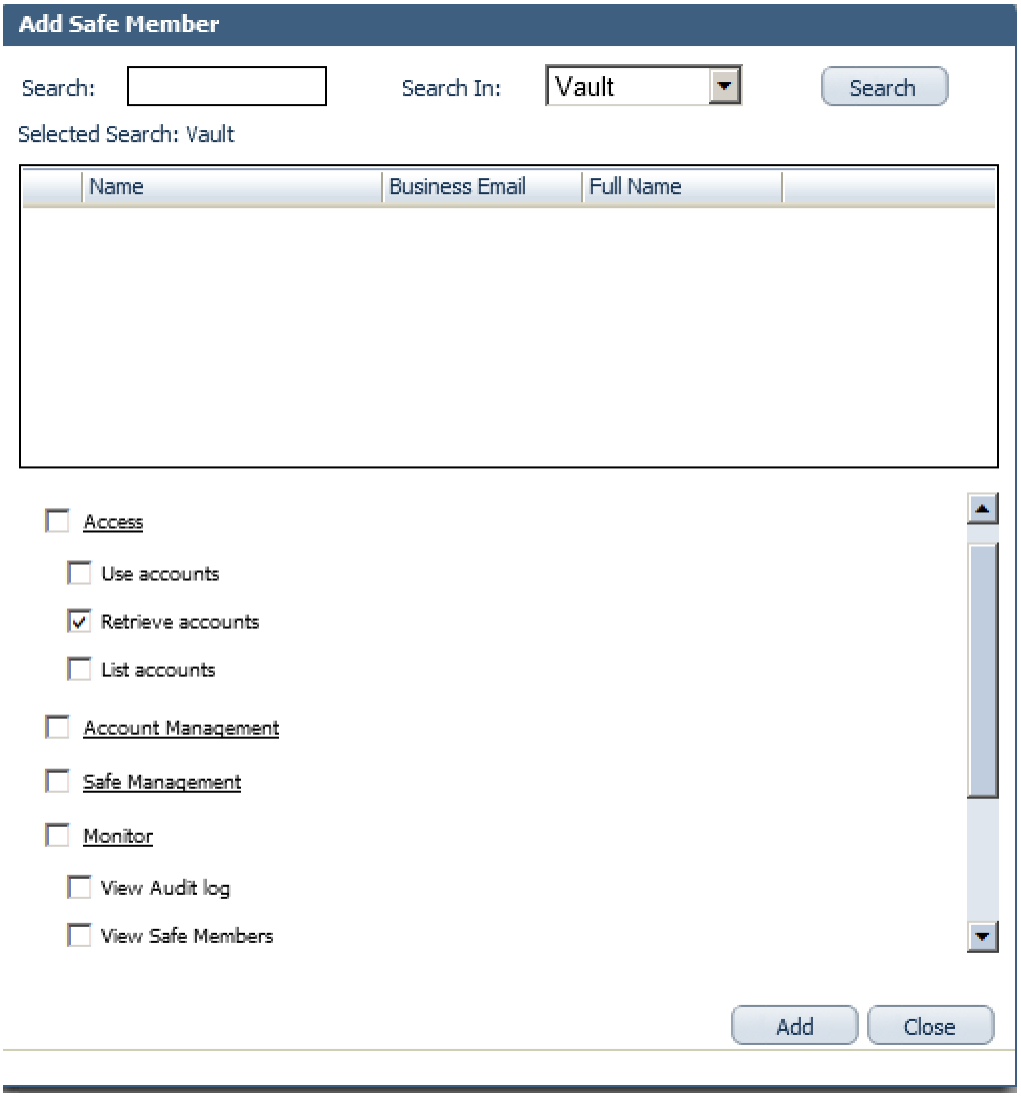
- List accounts
- Retrieve accounts
- View Safe Members

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 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.

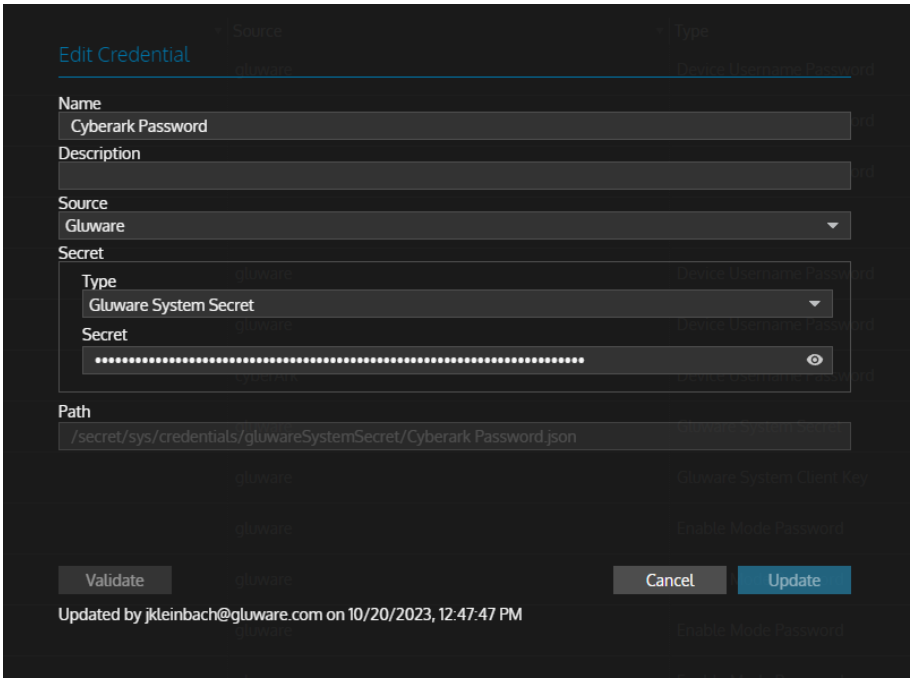
For more information about configuring Safe Members, refer to the **Privileged Access Security Implementation Guide.**

PARTNER PRODUCT INSTALLATION & INTEGRATION CONFIGURATION

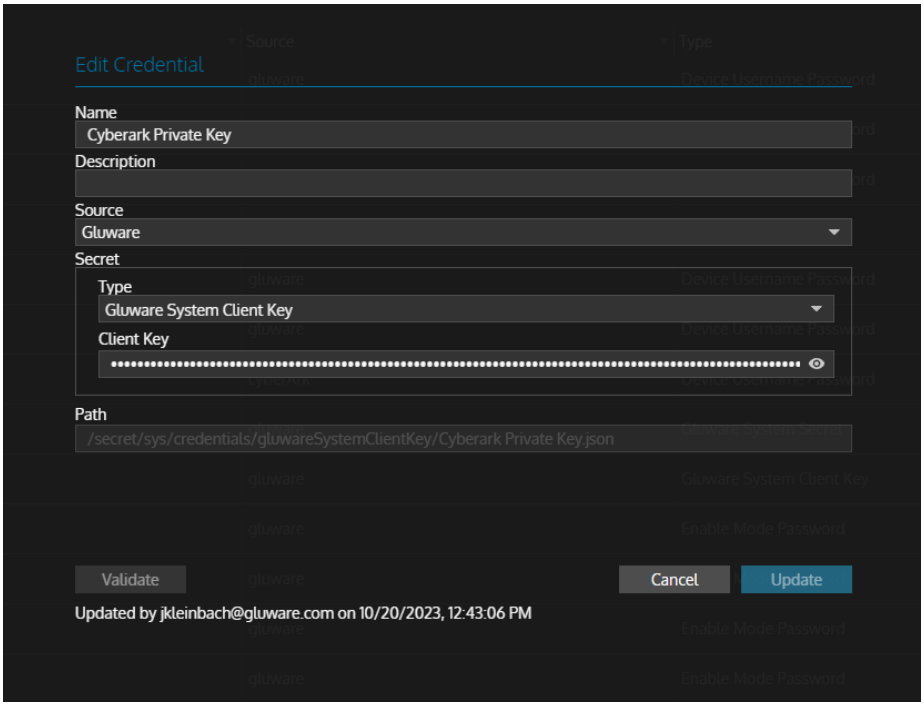
Refer to Gluware User Guide v5.2 or higher for Partner Product installation. This can be found at https://gluware.com/techdoc/.

First Step, create the vault integration:

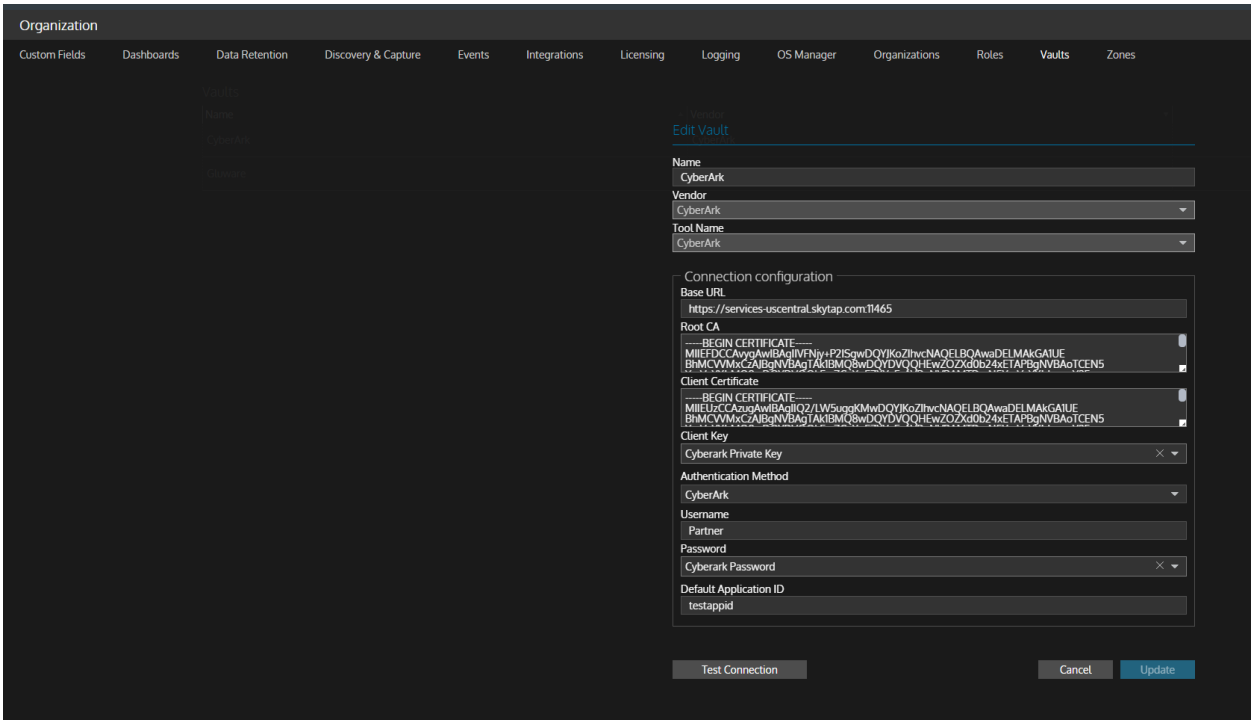
1. Create the CyberArk integration credential as a secret in the Gluware Vault:



2. Add the CyberArk private certificate key as a secret in the Gluware Vault:

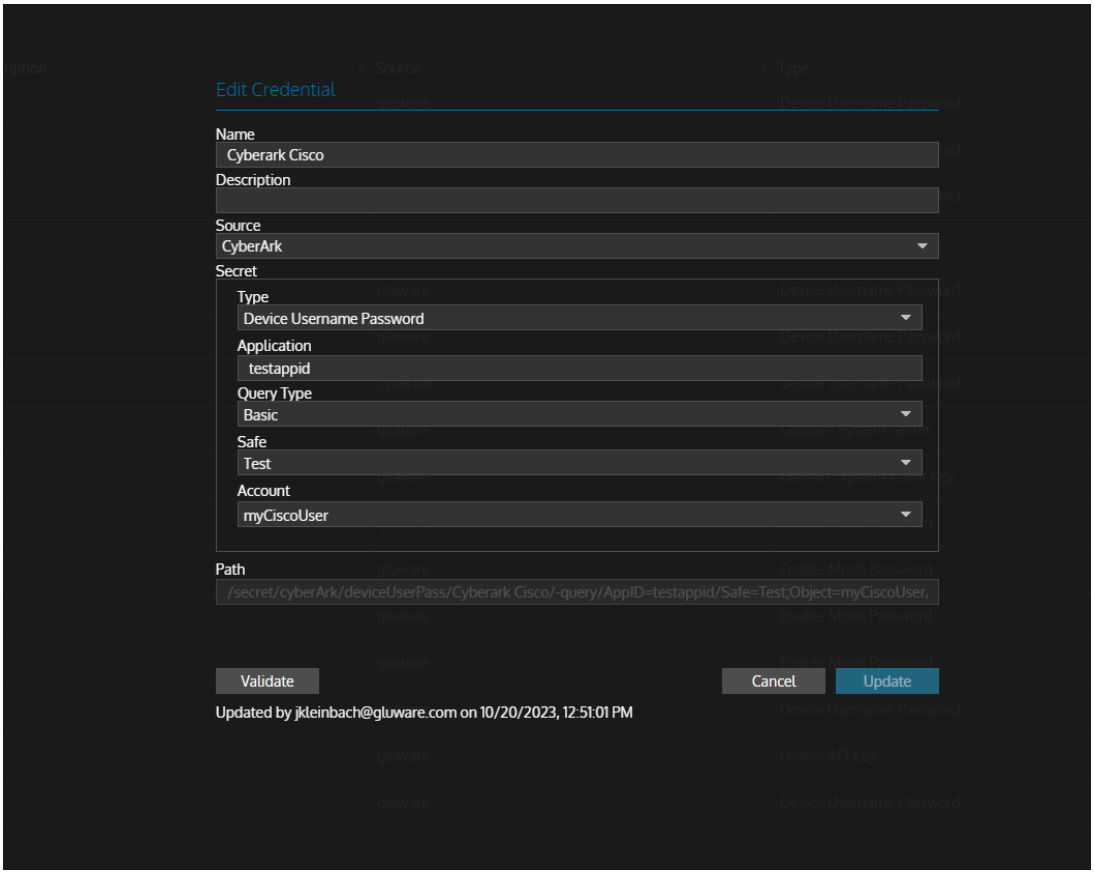


3. Go to Settings > Organization > Vaults.
4. Click Add Vault +.
5. Enter a user-friendly name for the vault.
6. Paste the URL of the vault in the Base URL field. For example, paste the URL of the CyberArk Enterprise Platform Vault.
7. Paste the server-side certificate in the Root CA field.
8. Paste the client certificate in the space provided.
9. Select the Gluware System Client Key you established in Credentials for the client certificate.
10. Enter the username for connecting to the vault.
11. Select the Gluware System Secret password for that username.
12. For the Default Application ID, enter an application name for the integration.
13. Optional: Click Test Connection to make sure Gluware can access the vault.
14. Click Create.



Next Step: Add a credential from the CyberArk Vault:

1. Go to Settings > Credentials.
2. Click Add Credential +.
3. Enter a name for the credential. It will appear in Gluware as the reference. For example, in Device Details.
4. Describe the credential.
5. Select Gluware System Client Key for the Type from the drop-down list.
6. Enter the Gluware System Client Key, the client certificate entered in CyberArk.
7. Click Create.



Common use cases:

1. Device Username Password
    a. Key used when making a device CLI connection
2. Enable Mode Password
    a. Key used for device enable mode password
3. Device API Key
    a. API Key for making a REST connection
4. Client Key
    a. Key used in making an API connection when integrating to a third-party system
5. Gluware System Client Key
    a. Key used for a client certificate
6. Gluware System Secret
    a. The password used in Gluware Settings
7. Secret
    a. Used anywhere an @Display.password is used in a JType

PARTNER CONTACT INFO

Business Contact	Name	Hamish Butler
	Email	hbutler@gluware.com
	Tel	916-312-6933
Technical Contact	Name	Tim Silverline
	Email	tsilverline@gluware.com
	Tel	415-596-2160
Support Contact	Name	Gluware Support
	Email	support@gluware.com
	Tel	855-458-3822