



SECRETS MANAGER

(Agentless Central Credential Provider CCP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION TEMPLATE

DOCUMENT PURPOSE: THIS TEMPLATE IS TO BE COMPLETED BY PARTNER AND IS REQUIRED FOR CYBERARK SECURED CERTIFICATION. THE SECRETS MANAGER 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: LoadGen

Website: <https://www.loadgen.com>

Name of Product: LoadGen Load and Performance Testing

Version: Q1 – 2024, build 5.0.0.9015 and up

Date: 01-25-2024

PARTNER SOLUTION OVERVIEW

Document Purpose: This document details the technical integration of LoadGen Suite with CyberArk Secrets Manager, aimed at achieving secured certification. The integration leverages CyberArk's robust secrets management capabilities to enhance LoadGen's performance testing, functional testing, and monitoring solutions with advanced credential security.

LoadGen Suite Overview: The LoadGen Suite is a comprehensive software solution designed for performance testing, functional verification, and monitoring of Server Based Computing (SBC), Virtual Desktop Infrastructure (VDI), traditional desktop-server environments, and native webtesting environments. LoadGen simulates user activity to test and measure the performance and resilience of IT environments. Its key components include LoadGen Director, LoadGen Studio, and LoadGen Analyzer, which together provide an performance testing framework.

Integration Context: The integration with CyberArk Secrets Manager ensures the secure handling of credentials within the LoadGen Suite. As LoadGen executes tests that involve various user types and accounts, including administrative and database accounts, the need for secure credential management is paramount. By integrating with CyberArk, LoadGen ensures that all credentials used during testing are securely stored and managed, accessed only when necessary, and in compliance with the organization's security policies.

By completing this integration, LoadGen can offer its users an additional layer of security, ensuring that sensitive data is protected throughout the testing lifecycle. This not only improves the overall security posture but also streamlines the testing process by automating the retrieval and management of credentials, thus minimizing potential human error and increasing efficiency.

Version: Q1 – 2024, build 5.0.0.9015 and up (not RTM yet)

Platform components:

- **LoadGen Director (integration with CyberArk):** Centralized control panel for managing and orchestrating the LoadGen Suite, providing a user-friendly interface for scheduling tests, managing user profiles, and monitoring test executions.
- **LoadGen Studio (integration with CyberArk):** A versatile script development environment where testers can create and manage their test scenarios, integrating with various web technologies and frameworks.
- **LoadGen Analyzer (integration with CyberArk):** An analytical tool that offers post-test analysis with detailed reports and dashboards, displaying key performance indicators and insights into system behavior under load.
- **LoadGen Agent:** A lightweight client that executes the test scripts generated by LoadGen Studio, simulates user actions, and collects test data.
- **LoadGen Core Agent:** Designed for Linux environments, it functions similarly to LoadGen Agent by running test scripts and gathering performance metrics.
- **LoadGen End-to-End Monitoring – Cloud edition (works with Azure Keyvaults):** Monitors applications and IT infrastructure continuously to provide real-time feedback on system performance and availability.

- **LoadGen Virtual User (vUser):** Simulates real user actions to test the performance and functionality of applications, mimicking human interaction with the system.
- **LoadGen Data Collector:** Aggregates performance data from various sources, enabling comprehensive analysis within LoadGen Analyzer.
- **LoadGen CyberArk Integration:** Enhances credential security by securely retrieving and managing credentials through CyberArk integration for all test-related activities.
- **LoadGen API:** Allows programmatic interaction with the LoadGen Suite for test management, execution, and results retrieval.
- **LoadGen WebTesting:** Provides capabilities for recording, scripting, and executing web application tests across multiple browsers and platforms.
- **LoadGen Cloud Services:** Offers cloud-based services for test management, execution, and monitoring, allowing scalability and remote access.
- **LoadGen Repository:** SQL Database for storing results.

KEY BENEFITS

Benefits of LoadGen Load and Performance Testing Suite:

1. **Realistic User Simulation:** LoadGen simulates real user behavior, providing accurate insights into how applications and systems perform under various load conditions.
2. **Scalable Load Testing:** Capable of simulating thousands of virtual users (vUsers) to stress test applications and determine scalability and capacity limits.
3. **Multi-Platform Support:** Offers support for a wide range of platforms, including Citrix, VMware, Microsoft RDS, traditional desktop-server environments, and WebTesting ensuring comprehensive testing across different infrastructures.
4. **Integrated Analysis Tools:** Comes with powerful analysis and visualization tools like LoadGen Analyzer, enabling users to dissect performance data and identify bottlenecks.
5. **Browser and OS Compatibility:** Supports web testing across major browsers and operating systems, ensuring applications perform well for all users regardless of their technology choices.
6. **Automated Testing Workflows:** Facilitates the automation of testing processes, from script creation and test execution to result analysis, saving time and reducing manual effort.
7. **Continuous Monitoring:** Provides continuous End-to-End monitoring capabilities, allowing teams to detect and resolve issues before they affect end-users, Cloud only.
8. **Customizable Test Scenarios:** Allows for the creation of customized test scenarios that closely mirror the real-world use of applications, enhancing the relevance of test outcomes.
9. **Flexible Licensing Model:** Offers a subscription-based licensing model, which provides flexibility and cost-effectiveness by aligning with the specific testing needs and duration.
10. **No-code Workload Creation:** Enables fast and easy workload creation without the need for complex scripting, making it accessible to users with varying technical expertise.

11. **Proactive Performance Optimization:** By predicting the impact of system changes, LoadGen helps organizations to proactively optimize performance and avoid potential issues.
12. **Global Testing Reach:** With the capability to test from different geographic locations, LoadGen ensures that applications can handle global user traffic with consistent performance.
13. **Expert Support and Training:** Provides professional training and support to ensure users can leverage all features of the suite effectively, maximizing their investment.

Benefits of integrating LoadGen Load and Performance Testing Suite with CyberArk SECRETS MANAGER:

1. **Secure Credential Storage:** CyberArk SECRETS MANAGER securely stores sensitive credentials used during testing, mitigating the risk of exposure and ensuring compliance with industry security standards.
2. **Automated Credential Retrieval:** Credentials are automatically retrieved from CyberArk's secure vaults when needed, streamlining the testing process and reducing manual intervention.
3. **Enhanced Access Control:** Integration allows for granular access control, ensuring that only authorized users and systems can access sensitive test data and credentials.
4. **Centralized Management:** All credentials can be managed from a central location, simplifying administration and reducing the overhead associated with credential management.
5. **Password Rotation and Management:** CyberArk's robust password management features allow for automatic password rotation and policy enforcement, which are critical for maintaining security in dynamic testing environments.
6. **Reduced Credential Exposure:** By retrieving credentials on-demand and only when necessary, the exposure of sensitive information is minimized, further securing the testing environment.
7. **Streamlined Configuration:** LoadGen's interface simplifies the configuration of CyberArk integration, making it easier to establish and maintain the connection between systems.
8. **Error Reduction:** Automating credential management reduces the potential for human error, such as entering incorrect credentials during test setup.
9. **Improved Productivity:** Testers can focus on designing and executing tests rather than managing credentials, improving overall productivity.
10. **Bogus Password Elimination:** With CyberArk integration, the correct credentials are injected at runtime, ensuring tests are always run with current, valid data.
11. **Immediate Incident Response:** Integration with CyberArk enables immediate action in case of detected anomalies or security breaches, allowing for rapid containment and resolution.
12. **Scalability:** As the number of users and complexity of testing scenarios grows, the integration scales to manage an increasing number of credentials without additional complexity.
13. **Seamless Updates:** Credential updates in CyberArk automatically propagate to LoadGen tests without manual changes, ensuring tests are always run with the most recent credentials.
14. **Secure Testing Lifecycle:** From test development to execution and reporting, the entire testing lifecycle is secured, maintaining the integrity and confidentiality of test scenarios and results.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

Insert Partner Product architecture diagram. Diagram should depict where the SECRETS MANAGER integration is located within Partner Product architecture.

CyberArk Credential Provider Service Installation:

- The CyberArk Credential Provider Service needs to be installed on the same machine where LoadGen Director, Studio, and Analyzer are deployed. This service acts as an intermediary that facilitates secure communication between LoadGen applications and the CyberArk Vault.
- When LoadGen requires credentials for its operations, it doesn't directly store or handle them. Instead, it makes a real-time request to the CyberArk Credential Provider Service.
- The CyberArk Credential Provider Service then interacts with the CyberArk SDK to retrieve the necessary credentials securely. This interaction is based on predefined access policies and only occurs when a password is requested.

LoadGen User Types:

LoadGen utilizes three primary types of user accounts, each serving a distinct purpose within the LoadGen Suite:

1. Test Accounts:

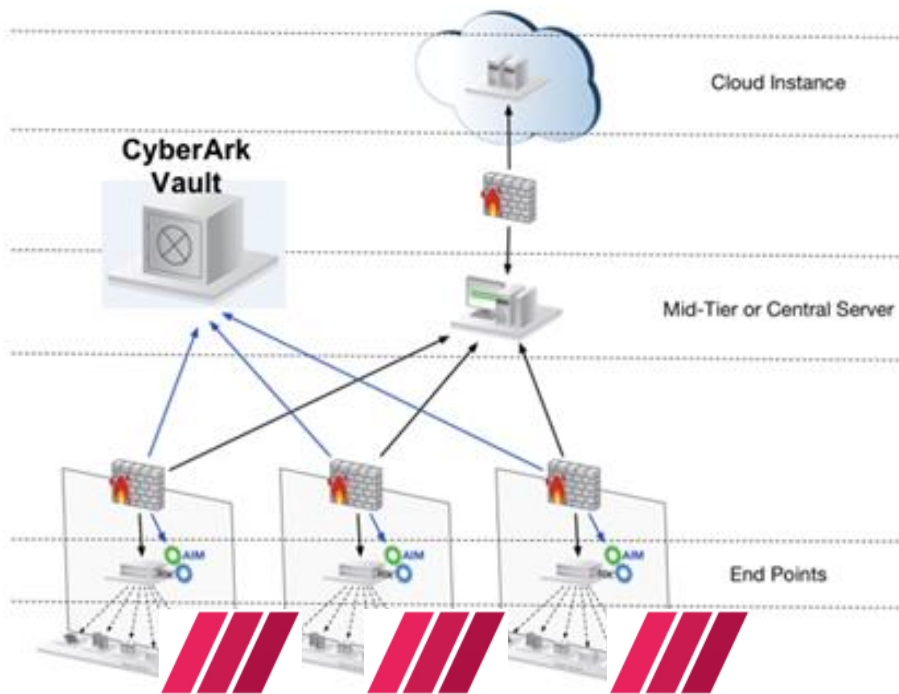
- These accounts represent the typical end-users in a testing scenario.
- They exist within Active Directory and are used within LoadGen to simulate real user actions and behaviors during testing.

2. Run as Profile Accounts:

- Run as Profile accounts are essentially local administrator accounts that have elevated rights.
- They are used to establish connections to various machines, distribute LoadGen Agents, and retrieve Systems Under Test (SUT) performance counters.

3. SQL Database Accounts:

- SQL Database accounts are specialized accounts used for interactions with SQL databases.
- These accounts are critical for managing the data within LoadGen, including storing test results, configuration settings, and historical performance data.



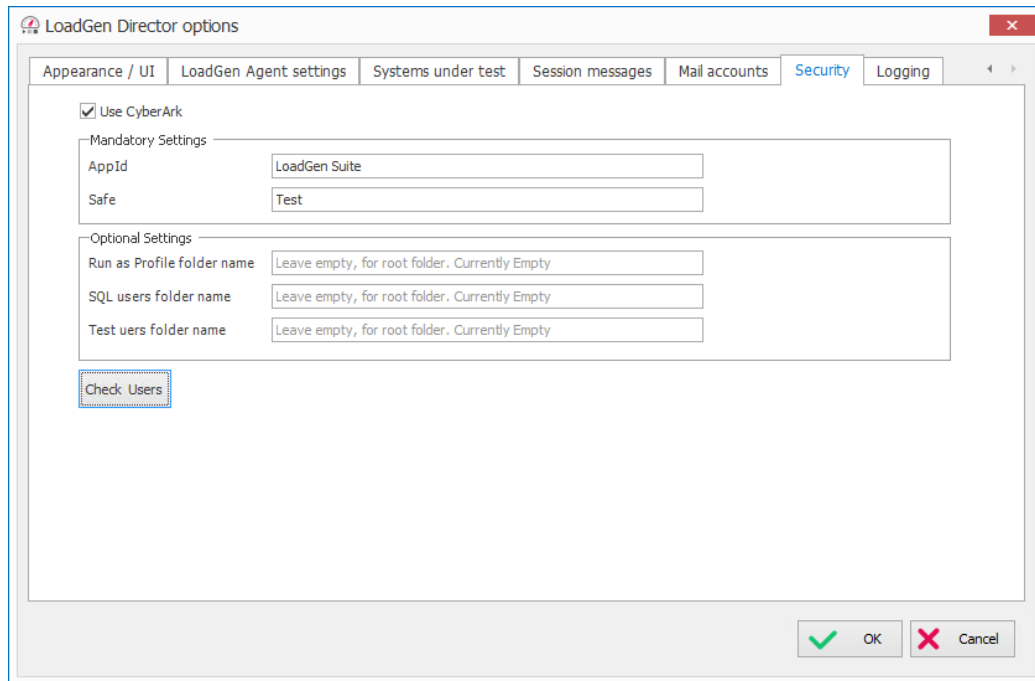
SECRETS MANAGER INTEGRATION

Describe Partner Product and depict where SECRETS MANAGER integration lies. Description might include:

Integration Points with SECRETS MANAGER:

1. LoadGen Director:

- The LoadGen Director serves as the central management console for orchestrating and monitoring test scenarios. It provides a user-friendly interface for setting up, executing, and reviewing the outcomes of various testing processes.
- In terms of configuration and data storage, settings for the LoadGen Director are stored in %ProgramData%\LoadGen\Options.xml. This file contains configuration data but does not store any sensitive information.
- The integration with CyberArk ensures that sensitive data, particularly credentials required for testing scenarios, are not stored locally within the Director's configuration files. Instead, these credentials are securely managed and accessed through the CyberArk Credential Provider service.
- This approach aligns with best practices in security, ensuring that sensitive information like usernames, passwords, and other credentials are stored and handled securely outside of the LoadGen environment. The use of CyberArk's Credential Provider service adds an additional layer of security, ensuring that credential management adheres to stringent security standards and reduces the risk of unauthorized access or data breaches.



2. LoadGen Studio:

- LoadGen Studio is where test scripts and scenarios are created and edited.
- Integration with SECRETS MANAGER in the Studio facilitates the secure handling of credentials within test scripts, ensuring that sensitive data like user names and passwords are managed securely.

3. LoadGen Analyzer:

- The Analyzer component processes and visualizes test results.
- While Analyzer's direct interaction with SECRETS MANAGER might be limited, it benefits from the secure data handling processes established in other components.

Location of Integration:

- The integration of SECRETS MANAGER with LoadGen primarily occurs at the endpoint level, where individual machines running the LoadGen components interact with the CyberArk SECRETS MANAGER to retrieve or store credentials securely.

Typical Installation Setup:

- A typical installation of the LoadGen Suite with CyberArk SECRETS MANAGER integration would include:
 - One central server hosting the LoadGen Director, LoadGen Studio and LoadGen Analyzer, which serves as the main control hub.
 - Multiple mid-tier servers or endpoints, each running either LoadGen Studio or Analyzer, depending on the organizational requirements. The exact number can vary based on the scale of operations and testing needs.

CREDENTIAL RETRIEVAL

Describe how the credential retrieval plays a role within the Partner product. Describe the flow in detail.

Credential Retrieval Trigger:

1. **LoadGen Director, Studio, and Analyzer:** The credential retrieval is initiated by these LoadGen components whenever a password is needed for specific user types – Test User, Run as Profile, or SQL User.
 - In **LoadGen Director**, this typically occurs during the setup and execution of test scenarios where user credentials are necessary for authenticating within the tested environment or system.
 - In **LoadGen Studio**, the retrieval is triggered when a Test User's credentials are required for recording or scripting test cases.
 - For the **LoadGen Analyzer**, the need arises when accessing the SQL database for data analysis and report generation.

Circumstances/Frequency of Credential Retrieval:

1. **Each Instance of Password Request:** The interaction with CyberArk's Vault occurs every time one of the LoadGen components requires a password. This ensures that credentials are always current and secure, adhering to the latest security policies and rotations managed by CyberArk.
 2. **Dynamic Retrieval:** The credentials are not stored locally within the LoadGen environment. Instead, each request dynamically fetches the required credentials from the CyberArk Vault. This approach is vital for maintaining security, especially in environments where credentials are regularly rotated or updated.
 3. **Real-Time Access:** The retrieval happens in real-time, ensuring minimal delay in the testing process. This real-time access is crucial for maintaining the efficiency of the testing workflow while ensuring the highest level of security for credential management.
- Describe specific properties required for queries on various platforms
 - We only support Windows at this moment.

REQUIREMENTS

List software, network, and hardware requirements. Provide context of requirements and team expertise for user planning needs. We will provide links to our support website as requirements can change over time.

- <https://support.loadgen.com/hc/en-us/articles/10195066984861-What-are-the-minimum-system-requirements-prerequisites-for-the-LoadGen-Products>
- <https://support.loadgen.com/hc/en-us/articles/16342567346333-CyberArk-Integration-with-LoadGen>

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.

LoadGen fully respects the unique setup requirements and preferences of each customer when it comes to the configuration of CyberArk integration. The process of defining the application manually via the CyberArk Password Vault Web Access (PVWA) is at the discretion of the customer. LoadGen ensures that its software suite is adaptable to various installation and setup approaches that customers may choose based on their CyberArk configuration. This flexibility includes accommodating the specific methods customers wish to use for managing applications within CyberArk, including the use of the PVWA interface for adding and configuring applications as required.

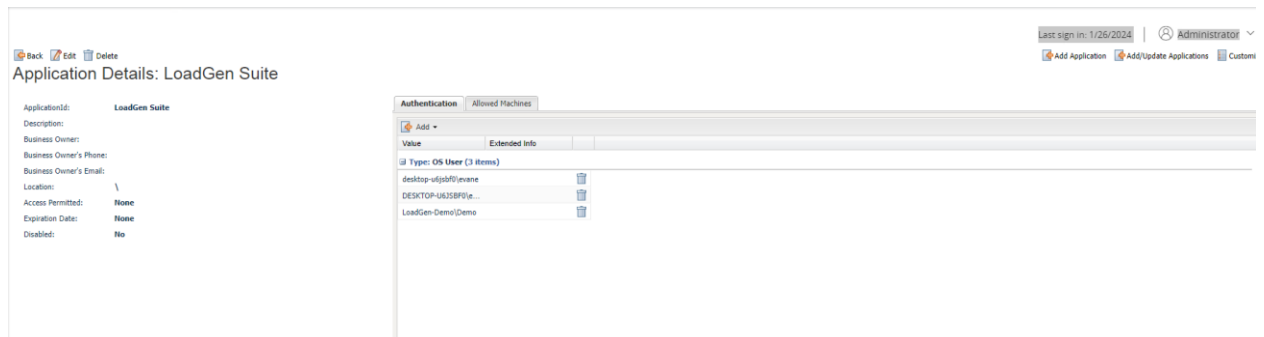
The screenshot shows the 'Edit Application' window with the following details:

- Name:** LoadGen Suite
- Description:** (Empty text area)
- Business owner:**
 - First Name: (Empty text field)
 - Last Name: (Empty text field)
 - Email: (Empty text field)
 - Phone: (Empty text field)
- Location:** (Dropdown menu showing a backslash symbol)
- Access Permitted:** From: (Dropdown) To: (Dropdown)
- Expiration Date:** (Calendar icon)
- Disabled:** (Checkbox)
- Buttons:** Update, 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: **APP ID = LoadGen Suite**
- 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.

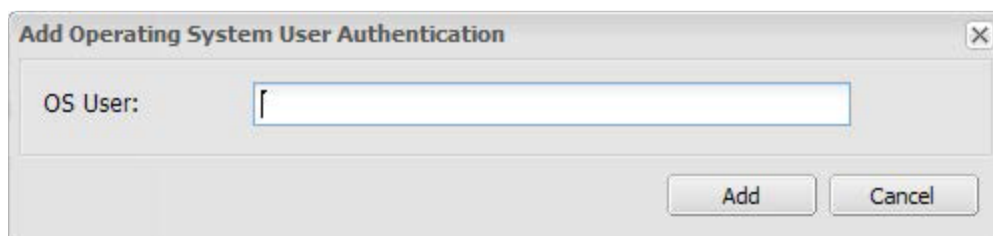
☐ Specify the application's **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password.

We advise the customer to use OS User for the authentication.

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

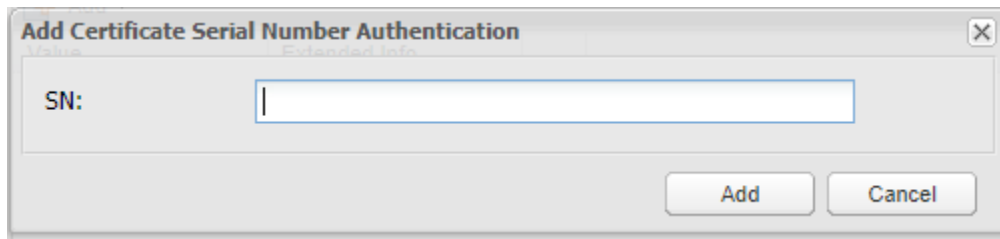
☐ Select the authentication characteristic to specify.

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



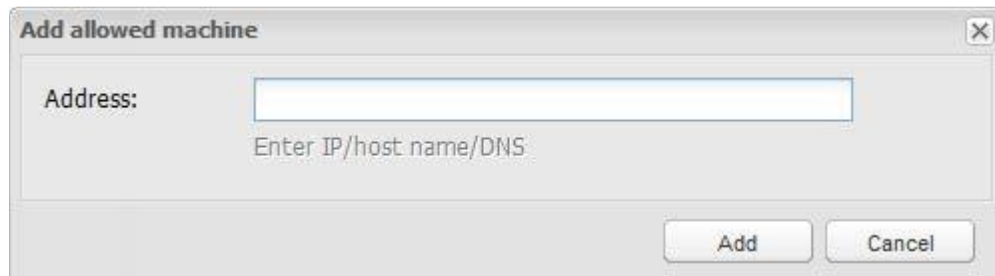
☐ Specify the name of the OS user who will run the application, then click **Add**. The OS user is listed in the Authentication tab.

- ☐ Specify the Certificate Serial Number.



The dialog box is titled "Add Certificate Serial Number Authentication" and has a close button (X) in the top right corner. It contains a label "SN:" followed by a text input field. At the bottom right, there are two buttons: "Add" and "Cancel".

- ☐ 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.



The dialog box is titled "Add allowed machine" and has a close button (X) in the top right corner. It contains a label "Address:" followed by a text input field. Below the input field, there is a hint text "Enter IP/host name/DNS". At the bottom right, there are two buttons: "Add" and "Cancel".

- 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

☐ 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.

PARTNER PRODUCT INSTALLATION & INTEGRATION CONFIGURATION

List specific steps to configuring Partner Product to work with SECRETS MANAGER, including:

- 14

2. How to specify credentials for scanning, that are stored in the Vault (instead of providing usernames and passwords) – include screenshots and description of steps

Partner Application UI:

The screenshot shows the 'LoadGen Director options' dialog box with the 'Security' tab selected. The 'Use CyberArk' checkbox is checked. Under 'Mandatory Settings', 'AppId' is set to 'LoadGen Suite' and 'Safe' is set to 'Test'. Under 'Optional Settings', 'Run as Profile folder name', 'SQL users folder name', and 'Test users folder name' are all set to 'Leave empty, for root folder. Currently Empty'. A 'Check Users' button is located below the optional settings. At the bottom right are 'OK' and 'Cancel' buttons.

Category	Field	Value
Mandatory Settings	AppId	LoadGen Suite
	Safe	Test
Optional Settings	Run as Profile folder name	Leave empty, for root folder. Currently Empty
	SQL users folder name	Leave empty, for root folder. Currently Empty
	Test users folder name	Leave empty, for root folder. Currently Empty

The screenshot shows the 'CyberArk user check' dialog box. It has two buttons: 'Retrieve users' and 'Perform password check'. Below the buttons is a table with two columns: 'Username' and 'Type of User'.

Username	Type of User
demo	RunAsProfile
beh_dnikolic	RunAsProfile
vUser0001	TestUser
vUser0002	TestUser
vUser0003	TestUser
vUser0004	TestUser
vUser0005	TestUser

PARTNER CONTACT INFO

Business Contact	Name	Roel Moonen
	Email	r.moonen@loadgen.com
	Tel	+31 88789 00 00
Technical Contact	Name	Daniel Nikolic
	Email	d.nikolic@loadgen.com
	Tel	+31 88789 00 88
Support Contact	Name	support@loadgen.com
	Email	support@loadgen.com
	Tel	+31 88789 00 88