



CYBERARK SECRETS MANAGER

(Agentless Central Credential Provider CCP)

SECRETS MANAGER INTEGRATION – TECHNICAL DOCUMENTATION

Name of Company: ITRS Group Ltd

Website: www.itrsgroup.com

Name of Product: Geneos

Version: GA5.1 +

Date: March 2020 (1 March 2021)

GENEOS SOLUTION OVERVIEW

Business critical services are enabled by an increasingly complex and interconnected IT estate. The health of the business is dependent on the health of the devices, the infrastructure, the connectivity, the applications and the data flows that serve it.

ITRS Geneos provides real-time insight into the performance of the technology that drives businesses to ensure maximum level of performance and availability of business technology.

Version: GA5.x

Platform components:

- Red Hat
- SUSE
- Ubuntu
- Centos
- Red Hat on IBM Power8
- Windows
- AIX
- IBM i
- macOS

KEY BENEFITS

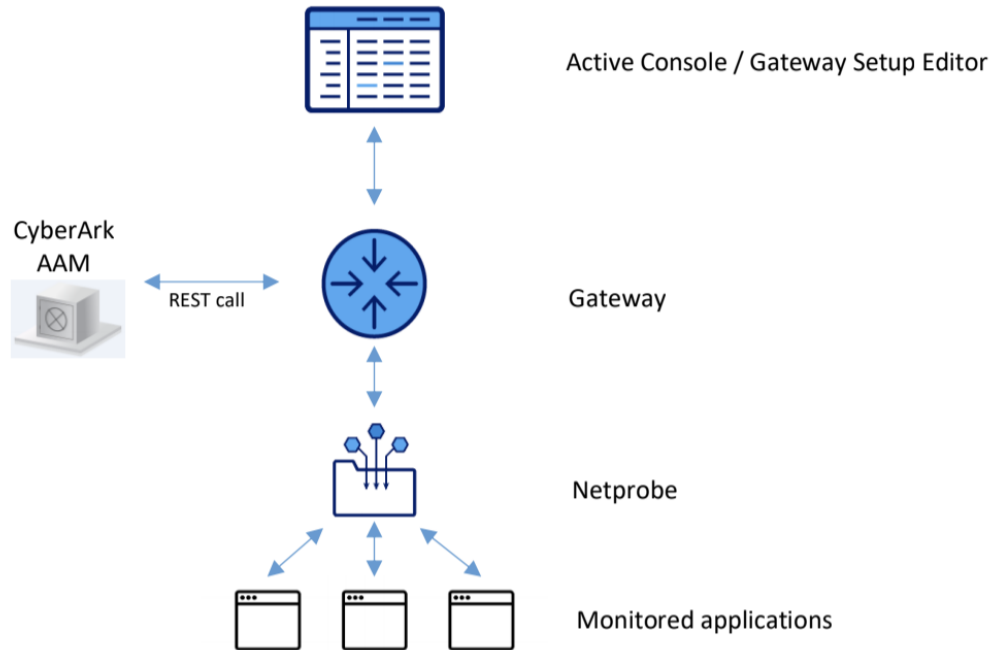
Benefits of Geneos:

- Monitor infrastructure and application in cloud and highly dynamic environments
- Build to run in time-critical, secure, regulated environments
- Seamless pre-built integrations with hundreds of applications
- Highly customizable enterprise scale solution
- Single pane of glass invisibility with a user level customizable views
- Drill down from business impact to detailed view
- Powerful and flexible rule and alert engine
- Interactive commands and automated actions to remedy issues
- Complete observability combining metrics, events, logs and traces

Benefits of integrating Geneos with CyberArk Secrets Manager:

- Password-less configuration of Geneos, providing more secure access to critical applications and infrastructure
- Comply with enterprise level security standards and audit requirements

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



SECRETS MANAGER INTEGRATION

Geneos CyberArk Secrets Manager integration is implemented in the Geneos middle-tier component called the Gateway. The Gateway is the 'core' of a Geneos installation and sits between the other two major Geneos components - Netprobes and Active Console.

Gateways provide configuration for, and gather data asynchronously from, the various Netprobes installed on the machines that are being monitored. Gateways can be connected to multiple Active Consoles, the GUI that provides you with a control and monitoring interface for your Gateways. The Gateway can be configured to connect to CyberArk Secrets Manager to obtain passwords, where required, by itself or through its connected Netprobes.

Typically, a large Geneos deployment will have thousands of Netprobes, hundreds of Gateways and tens of Active Console users. A single Gateway typically will connect to about one hundred Netprobes (based on best practice and average load).

CREDENTIAL RETRIEVAL

Password Lifecycle:

- Gateway is configured with connection details for CyberArk Secrets Manager service and the password queries (the strings which are used to retrieve password values from an external provider). These are added to the Gateway setup via Gateway Setup Editor (GSE) or otherwise.
- As setup validation progresses, external password queries are added to a validation list and queried against CyberArk.

- As results are received, the password values are held in memory as AES-encrypted strings.
- Post-validation step: The Gateway waits for the results of the queries and reports setup validation errors for any that could not be looked up.
- When a Netprobe connects, the AES-encrypted passwords are included in the setup that is sent down to the Netprobe. The Netprobe then uses the provided setup (including the password) to connect to applications it needs to monitor.
- When a Gateway component which supports external passwords needs to use a password, it accesses and decrypts (if required) the current AES-encrypted value.

Gateway retrieves credentials from CyberArk at start-up, restart, any changes to CyberArk integration configuration and any changes to configuration that uses CyberArk external password. In production environments, restarts and setup changes are kept to minimal. Typically, changes are applied outside business hours.

The Gateway is supported on Linux (RedHat, Centos, Ubuntu and SUSE) platforms only.

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 Geneos 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: ▼

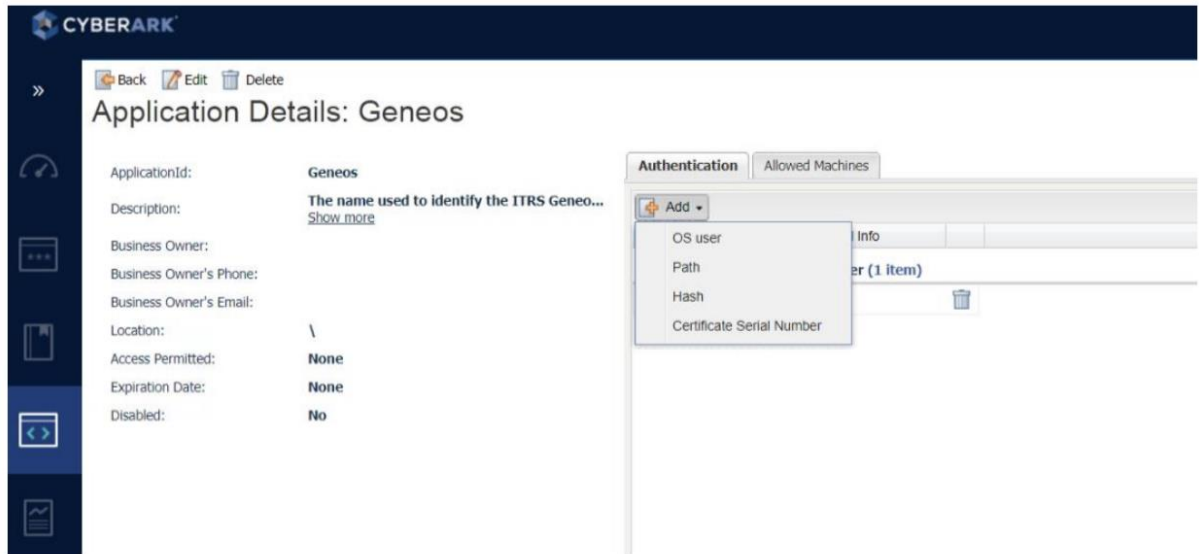
☐ Expiration Date:

☐ Disabled

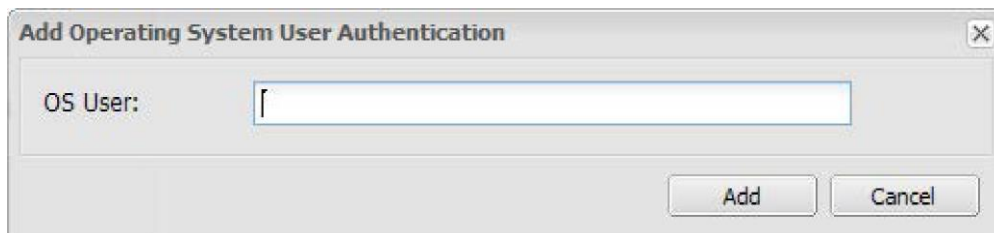
☐ Specify the following information:

- In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: APP ID = Geneos
- 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.

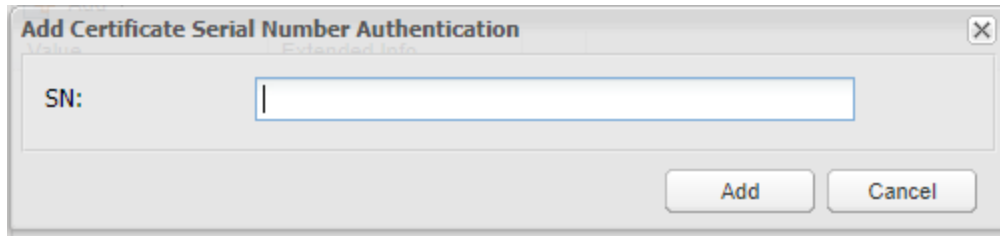
- ☐ Click **Add**. The application is added and is displayed in the Application Details page.



- ☐ 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. Partner should suggest the authentication details to secure the access by the partner's application.
- ☐ 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

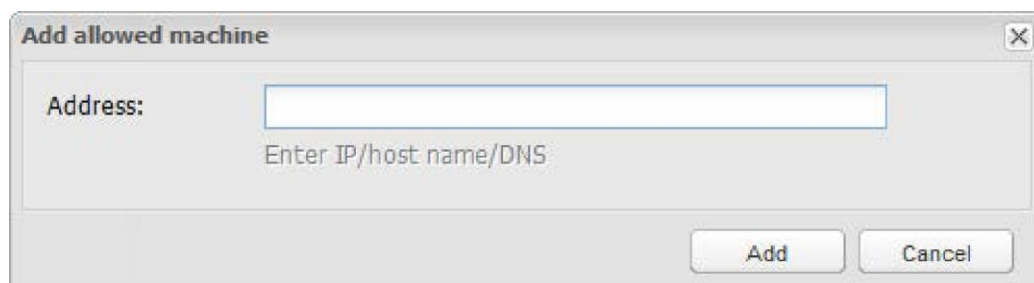
OpenSSL

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 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

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

- ☐ 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**.

GENEOS INSTALLATION & INTEGRATION CONFIGURATION

Refer to Gateway documentation for Gateway CyberArk integration setup.

In order to configure a Gateway to connect to Secrets Manager, the Gateway configuration requires the following:

Field	Description
-------	-------------

Server Name	URL of the CyberArk server. Example: https://cyberark_server_url.com . Include the port number, unless this is the default https port (443). Do not append any other part of the CyberArk URL (such as "/AIMWebService/api/Accounts").
Application id	The name used to identify the Gateway to CyberArk. This must be the same as the application id set in the CyberArk web interface.
Client certificate	Path to the <your-cyberark-cert>.pem file containing the certificates needed to connect to CyberArk securely.
Client key (optional)	Path to the file containing the client key. This is not required if the client key has been provided as part of the <your-cyberark-cert>.pem file.
Client key passphrase (optional)	Passphrase used to decrypt an encrypted client key.

Partner Application UI:

Example configuration to connect to Secrets Manager:

Operating environment - Modified

Basic
Advanced
Debug
Connections
Data Quality

- Log archive script
- Log time format Iso-8601
- Timezone
- Timezone abbreviations [Add new](#)
- Internal queue size limit 4000
- Num rule evaluation threads 0
- History files 10
- Data directory
- Duplicate row alerts Ticker_and_status

External passwords

Provider cyberArk

CyberArk

Server name https://services-uscentral.skytap.com:16776

Application id Geneos

Client certificate cyberark.pem

Client key

Client key passphrase

Validation timeout 30

- Insecure password level Warning
- Allow compute engine ☒

Write stats to file

Filename stats.xml

Enable periodic write ☐

Write interval 20

Example configuration to use CyberArk password:

The screenshot shows the 'sql-toolkit' application interface. At the top, there's a 'Plugin' dropdown set to 'sql-toolkit'. Below it are 'Basic' and 'Advanced' tabs, with 'Basic' selected. The 'Queries' section contains a table with columns 'Name', 'Sql', and 'Row limit'. It has one entry: 'TimeNow' with the SQL query 'select 'time' as time, now() as now' and a row limit of 200. An 'Add new' link is at the bottom. The 'Options' section has a 'connection' dropdown. Under 'Connection', there's a 'Database' dropdown set to 'mysql'. Below that is a 'Mysql' section with fields for 'Server Name' (myserver.itrs), 'Database Name' (geneos_db), and 'Port' (3306). Below these is 'User Name' (mysqluser). The 'Password' field is set to 'extPwd' and has a text box containing 'Safe=Test;Folder=root\Databases;Object=mysql', which is highlighted with a red rectangle. At the bottom, there's a checkbox for 'Close connection after query'.

Geneos supports both hard-coded passwords (stored as encrypted strings in the Gateway setup) and external passwords, sourced from CyberArk. To use a CyberArk password, select "External password" from the drop-down and copy the query string provided by your CyberArk administrator into the text box provided.

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	Lokesan Balakrishnan
	Email	lbalakrishnan@itrsgroup.com
	Tel	+44 20 7638 6700
Technical Contact	Name	Roland Young
	Email	ryoung@itrsgroup.com
	Tel	+44 20 7638 6700
Support Contact	Name	Marcos Galinanes
	Email	mgalinanes@itrsgroup.com
	Tel	+34 9 5125 5080