CyberArk
Application Guide

Contact Information
Go to the RSA corporate website for regional Customer Support telephone and fax numbers: www.emc.com/domains/rsa/index.htm.
For technical support, contact RSA at support@rsa.com.

Trademarks

License agreement

Third-party licenses
This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed by launching the product and selecting the About menu.

Note on encryption technologies
This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution
Use, copying, and distribution of any EMC software described in this publication requires an applicable software license. EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

Table of Contents

Preface

The purpose of this guide is to provide the user with an overview of how to setup Collectors and Connector for integrating CyberArk Privileged Account Security with RSA Via Lifecycle and Governance (RSA Via L&G). This guide will help the user understand the required configurations, parameters, mappings of different attributes in the connector and collectors, and how to use the AppWizard to create various components. The guide also covers use cases and troubleshooting tips.

Supported RSA Via L&G versions:

- Identity Management & Governance version 6.9.1 Patch 12 or later
- RSA Via Lifecycle and Governance version 7.0.0 Patch 02 and later

Audience

This guide is intended for the users of RSA Via L&G, including security administrators, CyberArk application owners, and system configuration administrators.

What is covered in the guide

- **Prerequisites section l**ists the required software that needs to be installed on the CyberArk server box in order to integrate CyberArk Privileged Account Security with RSA Via L&G.
- **Using CyberArk AppWizard section** will help in understanding how the connector and collectors can be configured.
- **Connector and Collectors configuration section** details how to configure or change settings, if required.
- **Tips & Troubleshooting section** has information about probable errors and their solutions. It will also help in understanding how to run CyberArk's Export Vault Data utility to generate CSV files which can be used to collect data from this endpoint.

1. Prerequisites for CyberArk

For this integration between RSA Via L&G and CyberArk, you will need to install CyberArk ExportVaultData Utility and CyberArk Command Line Interface (PACLI). RSA does not provide these packages; these may be obtained from your CyberArk representative.

- **CyberArk ExportVaultData Utility for collector**

  - **Requirements**

    1. **Operating System:** Windows 2003R2, Windows 2008R2, Windows 7, Windows 8, Windows 2012R2

    2. **CyberArk Vault:** Version 7.2 or higher

    3. **ExportVaultData Utility package content**

       The CyberArk ExportVault utility package includes following files:

       - **ExportVaultData.exe** – The main utility that retrieves information from the vault and generates reports.
       - **Vault.ini** – The Vault parameter file that specifies from which Vault the information will be taken.
       - **CreateCredFile** – The utility used to create the user credentials file so that the user, who will retrieve information, to log into the Vault.

  - **Creating the ExportVaultData Utility Environment**

    1. Create a new folder on the machine where the ExportVaultData utility will run, and copy the contents of the installation package to this folder.
    2. In the Vault, create a Vault user with the following authorizations:

       Note: RSA recommends using either the Auditor or Vault user who belongs to the Auditors group.

       - The user requires the following Vault authorizations:
         - Audit All
       - The user requires the following Safe authorizations that will have access to export data:
         - View Audit – for the Owners List, Files List, User and Safe Activities, and Events List
         - Retrieve Files – on the System Safe for the System Log List
         - Update Files – on the System Safe for the System Log List
         - Access Safe without Confirmation
         - Confirm Safe Requests – for the Requests List and Confirmation List

3. Use the CreateCredFile utility to create a logon file that will enable the ExportVaultData Utility to log onto the Vault automatically. For more information, refer to "*Appendix A: Creating a User Credential File"* of the ExportVaultData Utility Implementation Guide (CyberArk Documentation.)
4. Check that Vault parameter file, Vault.ini, contains the correct Vault connection properties.

- **CyberArk Command Line Interface (PACLI) for connector**

  - **Requirements**

    1. **Operating System:** Windows 200/NT/XP (32-bit), Windows 2003 (32-bit), Windows 7 (64-bit), Windows 2008 R2 (64-bit)

    2. **CyberArk Vault:** v7.2 and higher.

    3. **PACLI package content**
       - PACLI.exe
       - The following DLL files are distributed as part of the PACLI package:
         - calibeay32.dll
         - cassleay32.dll
         - msvcr71.dll

    These DLL files must be stored in the same folder as the PACLI.exe file or in the system path.

  - **Creating the PACLI Environment**

    1. Create a new folder on the machine where the CyberArk Command Line Interface will run, and copy the contents (PACLI.exe along with DLL files) of the installation package to this folder.
    2. In the Vault, create a Vault user with the following authorizations:

       Note: RSA recommends using either the Auditor user or a Vault who belongs to the Auditors group.

       - The user requires the following Vault authorizations:
         - Audit Users: to be able to "read" users properties, and activities.
         - Add/Update Users: For provisioning users/groups
         - Activate Users: To be able to activate users.
       - The user requires the following Safe authorizations that will access to export data:
         - View Audit
         - Access Safe without Confirmation

- For provisioning actions, the user will be required to have the safe's permissions to be granted

3. Use the CreateCredFile utility (from ExportVaultData, CPM, or other CyberArk component) to create a logon file that will enable the CyberArk Command Line Interface (PACLI) to log onto the Vault automatically. The same procedure that was used for ExportVaultData Utility can be followed. You can also use the PACLI CreateLogonFile to create a logon file, equivalent to the one created with CreateCredFile.
4. Check that Vault parameter file, Vault.ini, contains the correct Vault connection properties.
5. SSH server with administrator privileges (like Cygwin, PowerShell ssh server etc.) should be installed and running on CyberArk component (or on the machine which has command line access to CyberArk Vault) machine.

2. Using CyberArk AppWizard to configure Connector and Collectors

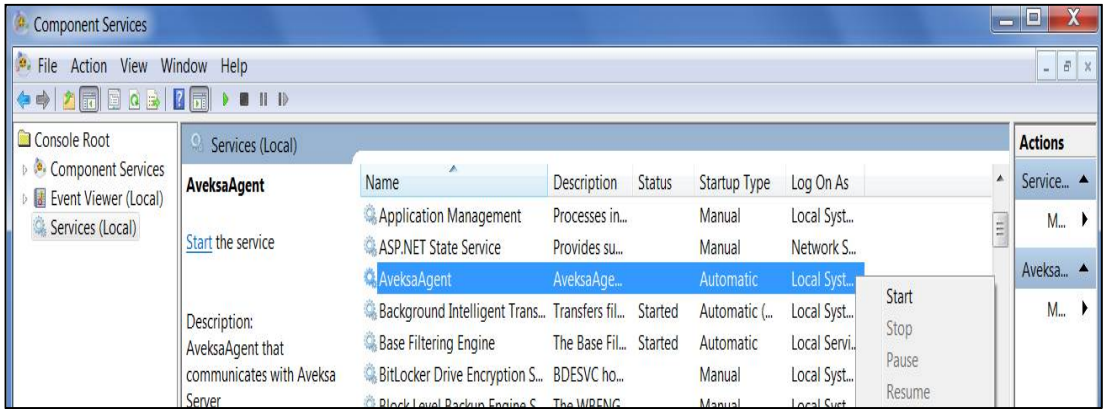
RSA Via L&G provides an Application Wizard which simplifies the process of setting up CyberArk Connector and Collectors. RSA recommends that you use the Application Wizard to initially setup CyberArk Connectors and Collectors. If you need to modify these Connectors/Collectors later on, then please refer to next section.

2.1. Pre-requisites

2.1.1. Install and configure Remote Aveksa Agent

- **How to create Aveksa Agent**
  1. Login to your RSA L&G server.
  2. Go to Collectors > Agents.
  3. Click Create Agent.
  4. Provide a suitable name for the new agent (e.g. CyberArk Agent).
  5. Provide a suitable name for a new agent (e.g. CyberArk Agent).
     Note: When the agent is created, it will appear in agents list.
  6. Select the created agent and click Download Agent. . This will download AveksaAgent.zip file.
  7. Copy the AveksaAgent.zip file to the CyberArk machine from where data need to be fetched.

- **Installing agent:**
  1. Make sure that environment variable JAVA_HOME is set and pointing to the correct JDK version (JDK 1.7.0 and above).
  2. Extract the AveksaAgent.zip.
  3. To install the agent as a service, go to the AveksaAgent → bin folder, right click InstallAvAgent-NT.bat, and select "Run as Administrator".
  4. To start the service, go to the Services control panel and start 'AveksaAgent' service by right-clicking on it.



After successful installation of an agent on the remote machine, the status of the agent on RSA L&G server will be shown as "Running".

2.1.2. Using CyberArk ExportVault Utility and RSA's CSV Transformer

This section describes the steps required to be performed on Cyberark box for generating the CSV files using 'ExportVaultUtility' which will be transformed using RSA's 'CSVTransformer' and then, used for collection by RSA's CyberArk collectors.

- **Download RSA's CSVTransformer**

  To download RSA's CSVTransformer:

  1. Login to an RSA Via L&G instance.
  2. Go to Resources → Applications and click "Create Application" button.
  3. From the list of applications, select 'CyberArk'.
  4. Click Next.
  5. Click "Download" button, to download the artifacts (contained in a .zip file) necessary for the CyberArk collector. Extract the zip file; this zip file contains CSVTransformer JAR, Sample config.properties file, and readme file.
  6. Click 'Cancel'.

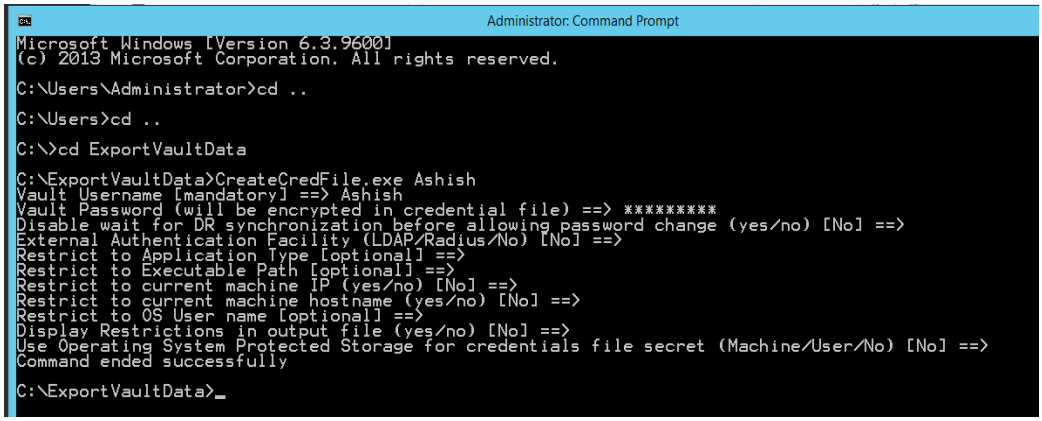
- **On CyberArk Side**

  1. Create .ini file in CyberArk server
  2. Generate Data using ExportVaultData Utility.
  3. Convert those files created by ExportVaultData Utility using CSVTransformer.jar

  1. Create .ini file in CyberArk server

  1. Using the Administrator account, login to Vault in CyberArk Component server.
  2. Go to Tools > Administrative Tools > Users and Group.
  3. Create a new user and provide username, password, and roles.
  4. Using CreateCredFile.exe, create the .ini file for the user.
  5. Open Command line prompt as Administrator.
  6. Execute 'CreateCredFile.exe <username> '.

Example:



In the above example an ini file is created named “Ashish.ini”in the folder “C:\ExportVaultData”. You are required to specify the full path while using ExportVaultData utility.

2. Generate Data using ExportVaultData Utility

1. Run Export Vault Data utility using following command:

Note: Export Vault Data Utility should be installed on CyberArk server box.

```
ExportVaultData \VaultFile=<VaultFileName>
\CredFile=<CredentialFileName>
\LogFile=<LogfileName>
\Target=<File>
\LogNumOfDays=<NumberOfDaysForLogList>
\Separator=<SeparatorCharacter>
\Qualifier=<QualifierCharacter>
\UseQualifier=<All/None/Strings>
\timezone=<GMT/LocalTime>
\enabletrace\<OutputName>=<FileName> [{\<OutputName>=<FileName>} ]
```

The list of Input parameters:

Parameter	Specification
\VaultFile	Full path of the Vault configuration file (if not set, default value is ‘vault.ini’)

\CredFile	Full path of the user credentials file. The user should have at least audit entitlement. (if not set, default value is 'user.ini')
\Logfile	Full path of the log file (if not set, default value is 'log.txt')
\Target	The output of the utility will be saved in a file.
\LogNumOfDays	The number of previous days that will be included in the Safe and user log activities report. The default number is 1.
\Separator	The character that is used as the separator between fields. The default separator is a comma (,).
\Qualifier	The character that is used as the text qualifier. The default qualifier is quotation-marks ("). Note: Some characters are not valid as qualifiers (e.g: |).
\UseQualifier	Specifies whether to use the text qualifier in all types of fields, none of the fields, or only with string fields. Valid values are "All", "None" or "Strings"). The default value is "Strings".
\timezone	The time zone that is used in all the reports time fields. Specify one of the following: • Local time • GMT – This is the default value.
\enabletrace	Specifies whether or not Casos log files will include Casos transaction information. Specify one of the following: • Yes - Casos log files will include Casos transaction information. This is the default value. • No - Casos log files will not include Casos transaction information. Note: This affects the size of the log files.
\OutputName	Lists a type of report and the name of the output file. At least one output file

	must be specified. Note: Specify the output type and file name directly, as shown in the following example which would generate a Safes List report: ExportVaultData \VaultFile=Vault.ini \CredFile=user.cred \Target=File \OwersList=ownerList.csv \GroupsList=groupList.csv \GroupMemberList=groupMembersList.csv

The list of Output files Name:

File	**Specification**
FilesList	A files list report will be generated
LogList	A log activities report will be generated
*OwnersList	An owners list report will be generated
RequestsList	An incoming requests list report will be generated
SafesList	A Safes list report will be generated
*GroupsList	A groups list report will be generated
*GroupMembersList	A group members list report will be generated
*UsersList	A users list report will be generated
LocationsList	A locations list report will be generated
ConfirmationsList	A request confirmations list report will be generated
Italogfile	A system log (ITAlog) file will be generated

EventsList	An events list report will be generated
*ObjectProperties	A file categories list will be generated

Note: * Marked files are mandatory for the ADC (Account Data Collector) and EDC (Entitlement Data Collector).

3. Convert those files created by ExportVaultData Utility using CSVTransformer.jar

1) Configure the config.properties file before running csvtransformer.jar:, otherwise it will take default parameters.

Config.properties file contains following fields:

Input file:

Field	Specification
inputFolder	Input folder path where the unmodified CSV(s) are placed.
accountFilename	input account file name
groupFilename	input group list file name
ownerFilename	input owner file name
groupMemberListFilename	input group Member list file name
objectPropertiesFilename	object properties file name

Output file:

Field	Specification
outputFolder	Output folder path where modified CSV(s) have to place.
entFilename	output entitlement file name
out_accountFilename	output account file name
out_groupFilename	output group list file name
out_groupMemberListFilename	output group Member list file name

Column locations for ownerslist:

Field	Specification

safeidCol	column no. of safe id column
safenameCol	column no. of safe name column
owneridCol	column no. of safe owner id column
ownernameCol	column no. of safe owner id column
ownertypeCol	column no. of owner type column

Note The collector query configuration addresses these output file names.

Default configuration parameters:

config.properties

```
seperator=,

#Input filenames
inputFolder=C:\\ExportVaultData\\
accountFilename=userslist.csv
groupFilename=groupslist.csv
ownerFilename=ownerslist.csv
entFilename=entitlement.csv
groupMemberListFilename=groupmemberslist.csv
objectPropertiesFilename=objectproperties.csv

#Output filenames
outputFolder=C:\\ExportVaultData\\
entFilename=entitlement.csv
out_accountFilename=userslist_mod.csv
out_groupFilename=groupslist_mod.csv
out_groupMemberListFilename=groupmemberslist_mod.csv

#column locations for ownerslist

safeidCol=1
safenameCol=2
owneridCol=3
ownernameCol=4
ownertypeCol=5
```

2) Run the executable JAR using the following command:
`java -jar csvtransformer.jar <path to config.properties file>`

This will transform the CyberArk generated CSV(s) the form consumable by RSA Via L & G CyberArk collectors.

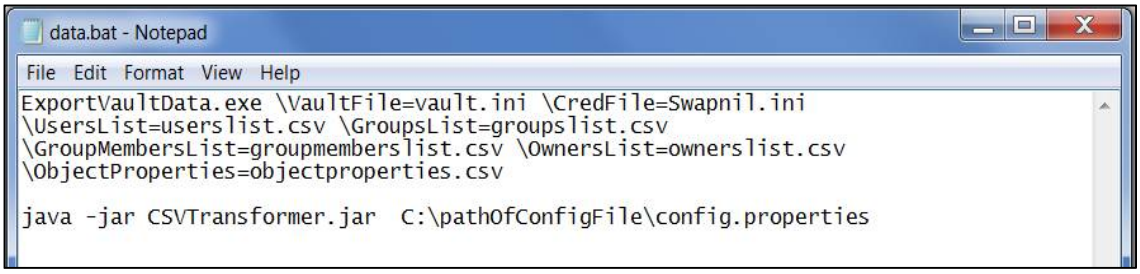
Now, above configured Aveksa Agent(Section 2.1.1) can be used to help collect data from the remote location using generated CSV files.

Recommended approach for synchronizing ExportVaultUtility generated data and transformed data:

Run 'ExportVaultData Utility' and the 'Transformer Utility' together in a scheduled fashion. Following steps will help to run both utilities in scheduled fashion.

i. Create a batch file which contains the commands to run the ExportVaultData utility and then CSVTransfomer Utility.

E.g. data.bat



ii. On the CyberArk service box (windows based), Open Task Scheduler by clicking the Start button, then go to Control Panel > System and Security > Administrative Tools and then double-click on Task Scheduler. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.

iii. Click the Action menu, and then click 'Create Basic Task'.

iv. Type a name for the task and an optional description, and then click 'Next'.

v. To select a schedule based on the calendar, click Daily, Weekly, Monthly, or one time, now click 'Next'; specify the schedule you want to use, and then click 'Next'.

vi. To schedule a program to start it automatically, click 'Start a Program', and then click next.

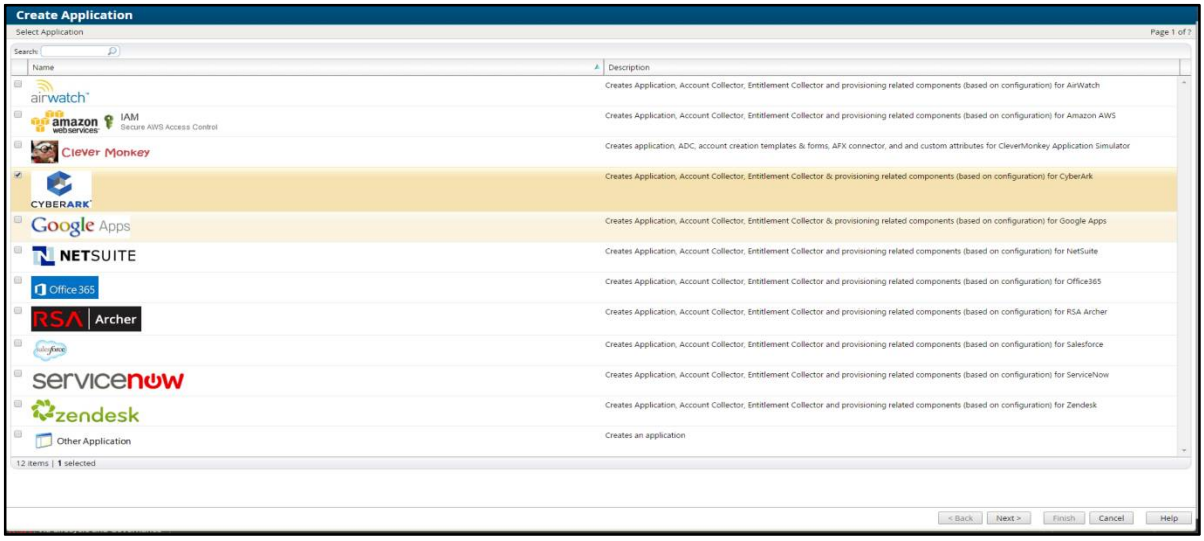
vii. Click 'Browse' to find the batch file that is created in step i., and then click 'Next'.

viii. Click 'Finish'.

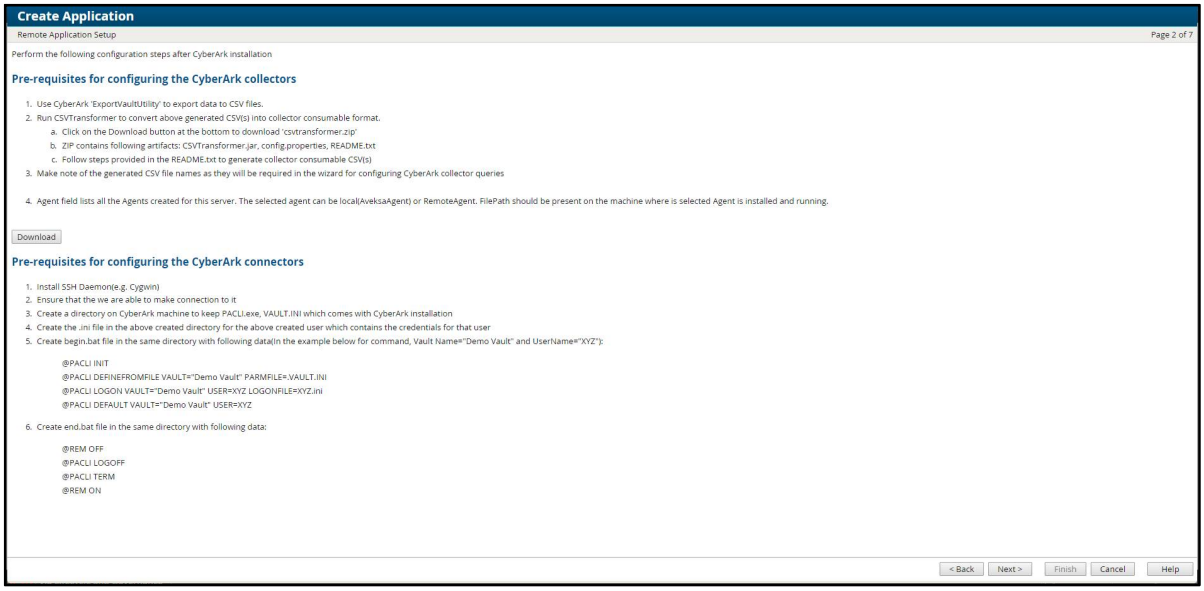
2.2. Configuring CyberArk Application Wizard

RSA Via L&G provides an Application Wizard to configure CyberArk Connector and Collectors.

1) Login to your RSA Via L&G instance if not already logged in.
2) Go to Resources → Applications and click “Create Application” button.
3) From the list of applications, select ‘CyberArk’.

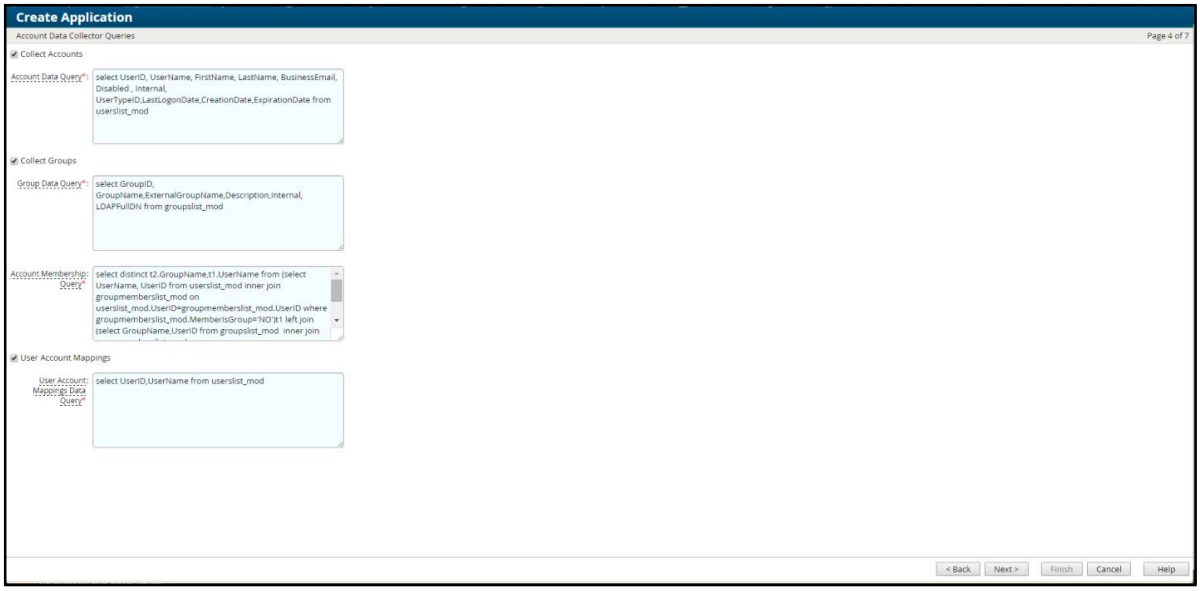


4) Click Next.
5) The Setup page provides an overview of the CyberArk end point, as well as collector and connector information. The ‘Download’ button is for the collector needed artifacts, which you have already downloaded in section 2.1.2.

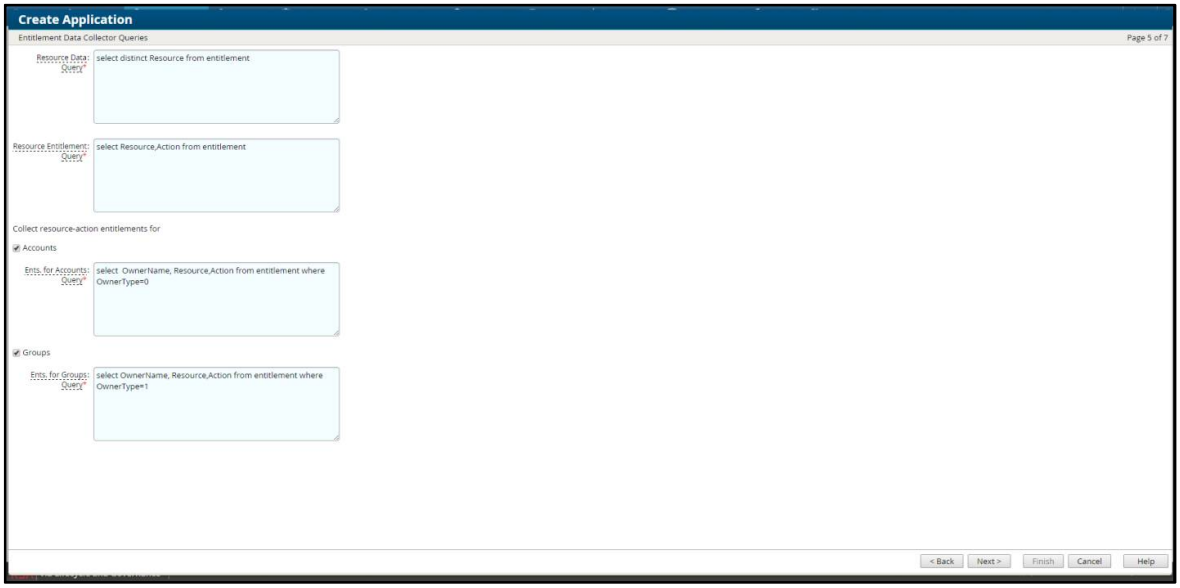


6) Click Next.
7) Fill out the 'Connect' page with information regarding connecting to the CyberArk end point. Here, select the 'Agent' you have created in section 2.1.1.
8) Click on Test Connection button to confirm that the connection to CyberArk endpoint can be established successfully.

9) Click Next.
10) On Account Data Collector Queries page, select the appropriate checkboxes and fill in the query textboxes. Default values are already provided in the query textboxes.



11) Click Next.
12) On 'Entitlement Data Collector Queries' page, fill in the query textboxes. Default values are provided in the query textboxes.



13) Click Next.
14) On the 'Confirm Changes' page, list of all the components (Connector, Collectors, Account template, Request Form) to be created will be displayed.

15) Click Next to view the list of all the created components.

16) Click Close.

After following the above steps, a CyberArk application will be created with all the components (Connector, Collectors, Request Form, Account Template etc.).

Now, CyberArk application is ready for collection and provisioning.

3. Creating new CyberArk Collectors - ADC & EDC (Optional)

The following diagram explains the data flow of the collector.

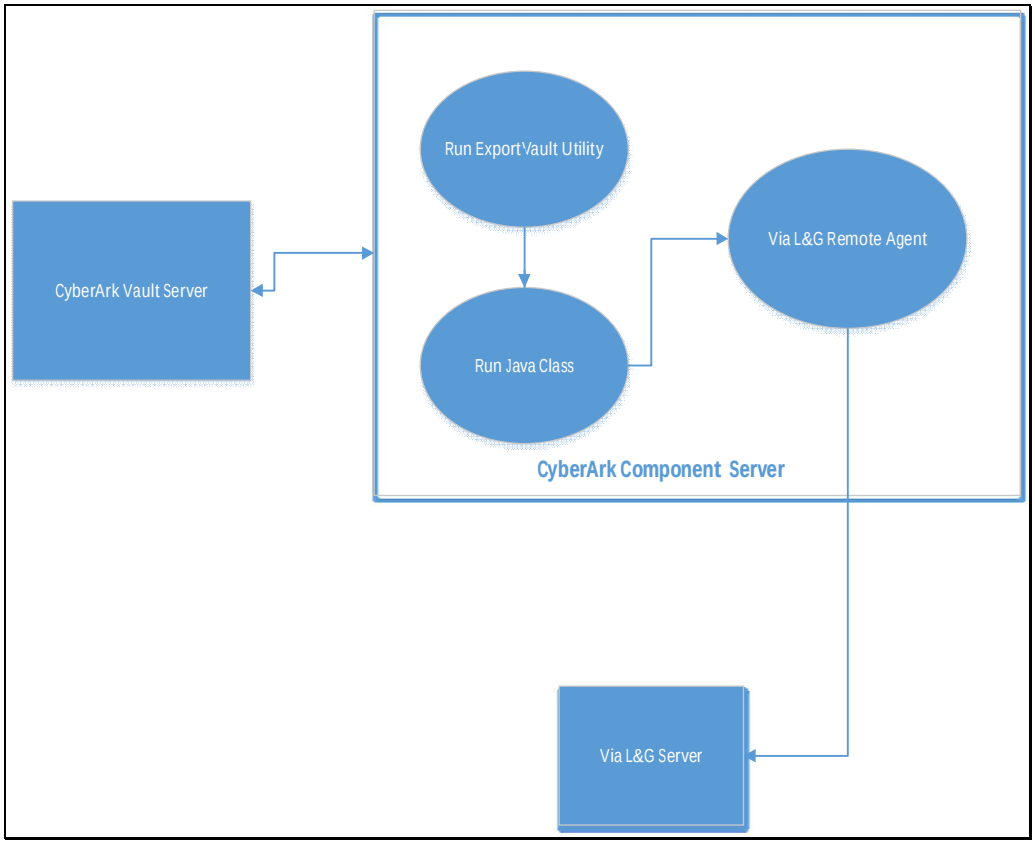


Figure 1: Data flow for collector

CyberArk Application wizard (refer to section 2) by default creates collectors (ADC, EDC). But, if you need to update configuration for your existing CyberArk Collectors (ADC & EDC) or selectively create new CyberArk Collectors (ADC & EDC), then refer to the steps below.

Collector Configuration

To set up new instances of the CyberArk Collectors (ADC/EDC) without using the Application Wizard:

1. Login to your RSA Via L&G instance.
2. Select the application already created (Resources > Applications).
3. Go to Collectors tab.
4. Click “Create Account Collectors” or “Create Entitlement Collectors”.
5. Configure the collectors based on your requirements:

- **Creating new Account Data Collector (ADC)**

  a. On the Collector Description screen complete the following fields:

Field Name	**Value**
Collector Name	Name for CyberArk Account Collector
Description	Description for the ADC. e.g. HR Department CyberArk Account Collector
Business Source	Select the required Directory or Application
Data Source Type	CyberArk
Agent	CyberArkAgent (Select the agent created in Step 4: Remote Aveksa Agent of the Prerequisites section).
Status	Active

Copy from	Select from dropdown if you want to copy settings from other existing CyberArk Collector
Scheduled	Select Yes if you want to schedule the collection

b. Click Next.
c. On CyberArk connection screen,

Field Name	**Value**
File Path	This refers to the Path of the folder where the CSV(s) are located. This path is of the machine where the Agent is installed and running. e.g.: C:/ParentFolder/CSVFolder

d. Click Next.
e. Select type(s) of account data to collect:
    - Accounts
    - User Account Mappings
    - Groups
f. Click Next.
g. Mapping for group attributes: Here, you can specify the attributes of CyberArk which should be mapped with RSA's attributes for groups.

Field Name	**Value**
Accounts Data Query	Query to return account data. The column names resulting from the query will be used in the fields. e.g.: select UserID, UserName, FirstName, LastName, BusinessEmail, Disabled , Internal, UserTypeID,LastLogonDate,CreationDate,ExpirationDate from userslist_mod

Account Name	Account Name column name resulting from <Accounts Data Query>. e.g.: UserName
Last Login Date	Last Login Date column name resulting from <Accounts Data Query>. e.g.: LastLogonDate
Expiration Date	Expiration Date column name resulting from <Accounts Data Query>. e.g.: ExpirationDate

h. Click Next.

i. On the Mapping User Account Data screen, provide values for fields given below.

Field Name	**Value**
User Account Mappings Data Query	Query to return user account mapping data. The column names resulting from the query will be used in the fields. e.g.: select UserID,UserName from userslist_mod
User ID	User ID column name resulting from User <Account Mappings Data Query>. e.g.: UserID
Account Name	Account Name column name resulting from User <Account Mappings Data Query>. e.g.: UserName

Note: Table reference for this page: **userslist_mod**.

j. Click on Next.

k. On the Mapping the group attributes screen, please provide values for the given fields.

Field Name	**Value**
Groups Data Query	Query to return group attribute values. The column names resulting from the query will be used in the fields. e.g.: select GroupID, GroupName,ExternalGroupName,Description,Internal, LDAPFullDN from groupslist_mod
Group Name	Group Name column name resulting from <Groups Data Query>. e.g.: GroupName

Note: Table reference for this page: **groupslist_mod**.

l. On the Account data Membership section, please provide values for given fields.

Field Name	**Value**
Account Membership Query	Query to return account members of groups. The column names resulting from the query will be used in the fields. e.g.: select distinct t2.GroupName,t1.UserName from (select UserName, UserID from userslist_mod inner join groupmemberslist_mod on userslist_mod.UserID=groupmemberslist_mod.UserID where groupmemberslist_mod.MemberIsGroup='NO')t1 left join (select GroupName,UserID from groupslist_mod inner join groupmemberslist_mod on groupslist_mod.GroupID=groupmemberslist_mod.GroupID where groupmemberslist_mod.MemberIsGroup='NO')t2 on t1.UserID=t2.UserID
Account ID/Name	Account ID or Name column name resulting from <Account Membership Query>. e.g.: UserName
Group ID/ Name	Group ID or Name column name resulting from <Account

	Membership Query>. e.g.: GroupName

m. Click Next.
n. On the Edit User Resolution Rules screen, use the table below to configure the parameters:

Field Name	**Value**
Target Collector	<Cloud IDC> Default: Users
User Attribute	<Email Address> Default: User Id

o. Click Next.
p. On the Edit Member Account Resolution Rules screen, use the table below to configure the parameters:

Field Name	**Value**
Target Collector	CyberArk Account Data Collector
Account Attribute	Name

q. Click “Finish” to save this Collector.

- **Creating new Entitlement Data Collector (EDC)**

  a. On the Collector Description screen, please provide values for the given fields.

Field Name	**Value**
Collector Name	<Name for CyberArk Entitlement Collector>
Description	Description of the EDC. e.g. HR Department Entitlement collector
Data Source Type	CyberArk
Agent	CyberArkAgent (Select the agent created in Remote Aveksa Agent step).
Status	Active
Copy from	Copy from <Select from Dropdown if you want to copy from other CyberArk Collector>
Scheduled	<Select Yes if you want to schedule the collection>

  b. Click Next.
  c. On the CyberArk connection screen, click on Download to download the 'CyberArkCSVTransformer.zip'.
     Note: Ignore this part if download has already been done in pre requisites(section 2.1)

Field Name	Value
FilePath	This refers to the Path of the folder where the CSV(s) are located. This path is of the machine where the Agent is installed and running. e.g.: C:/ParentFolder/CSVFolder

d. Click Next.
e. Select types of entitlement data to collect.

   Collect resource-action entitlements for Available entitlements - data type for this option are Groups, Accounts and Users. You can select multiple entitlements data type for this option as applicable

f. Click Next.
g. On the Define General column name screen, please provide values for given fields.

Field Name	Value
User Reference ID/Name	Default Value: OwnerName
Resource Fully Qualified Name	Default Value: Resource
Action ID/Name	Default Value: Action

h. Click Next.
i. On the Mapping for resource attributes screen, please provide valued for these fields.

Field Name	Value
Resources Data Query	Query to return resource attribute values for resource-action entitlements. The column names resulting from the query will be used in the fields below. e.g.: select distinct Resource from entitlement Collects Safes as Resource and accesses of users and groups on those safes as actions
Resource ID/Name	Resource ID or Name column name resulting from <Resources Data Query>. Value: Resource
Resource Fully Qualified Name	Resource Fully Qualified Name defined in Generic Column Names Value: Resource

j. Click Next

k. On the Map resource-action based entitlements screen, please provide values for these fields.

- Resource Entitlement Data

Field Name	Value
Resource Entitlements Query	Query to return entitlement attribute values for resource-action entitlements. e.g.: select Resource,Action from entitlement
Resource Fully Qualified Name	Resource Fully Qualified Name defined in Generic Column Names.
Action ID/Name	Action ID/Name defined in Generic Column Names.

Note: Table reference for this page: **entitlement**

- Group Data

Field Name	**Value**
Ents. For Groups Query	Query to return resource-action entitlements granted to groups. e.g.: select OwnerName, Resource,Action from entitlement where OwnerType=1
Entitled Group	User Reference ID/Name defined in Generic Column Names
Resource Fully Qualified Name	Resource Fully Qualified Name defined in Generic Column Names.
Action ID/Name	Action ID/Name defined in Generic Column Names.

- Account data

Field Name	**Value**
Ents. For Accounts Query	Query to return resource-action entitlements granted to user accounts. e.g.: select OwnerName, Resource,Action from entitlement where OwnerType=0
Entitled Account	User Reference ID/Name defined in Generic Column Names
Resource Fully Qualified Name	Resource Fully Qualified Name defined in Generic Column Names.
Action ID/Name	Action ID/Name defined in Generic Column Names.

l. Click Next.
m. On the associate a target collector to the Group Name screen, please select the appropriate values from the given drop-down.

Field Name	**Value**
Associated Target Collector	Cyber Ark Account Data Collector
Group Name evaluates to	Name

n. Click Next.
o. On the configure Account evaluation attributes screen.

Field Name	**Value**
Associated account collector	CyberArk Account Data Collector
Associated value evaluates to	Account Name

p. Click finish to save the collector.

4. Creating a new CyberArk Connector (Optional)

The following diagram explains the data flow of the connector.

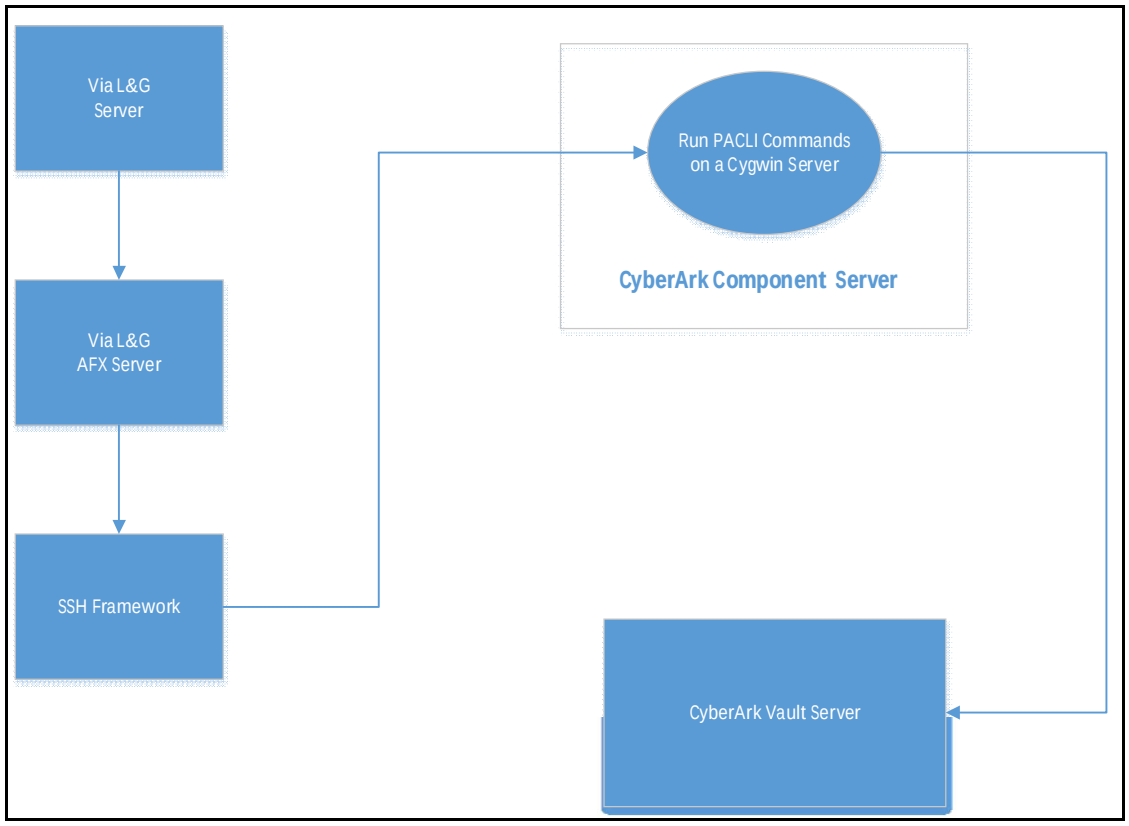


Figure 2: Data flow for connector

Connector Configuration

RSA recommends using the Application Wizard (refereed to Section 2) to get the Application-Connector binding and Account template configurations created; but if you need to update configuration for your existing CyberArk Connector or selectively create a new CyberArk Connector, then refer to the steps below.

To set up a new instance of the CyberArk connector without using the AppWizard:

1. Login to your RSA Via L&G instance.
2. From the top menu bar, Go to AFX > Connectors.
3. Click “Create Connector”.
4. Use the reference table below to configure the “General” tab.

Field Name	**Value**
Name	CyberArk Connector
Description	CyberArk Connector
Server	AFX Server
Connector Template	CyberArk
State	Test
Export As Template	Yes

5. Reference the table below to configure the “Settings” tab.

Name	**Description**
Host	Hostname or IP address of the CyberArk server.
Port	SSH port number. Default value is 22.

Timeout (milliseconds)	Connection timeout in milliseconds. The default value is 5000.
Login Name	Login Name to login to the server.
Password	Password to login to the server.

6. Configuring capabilities:

Note: The CyberArk Connector template has all the capabilities set as per the standard CyberArk end point. To modify these settings, refer to the mappings for parameters given below.

7. Save the Connector.

To test this connector, please wait till the connector status turns to "Running" and then check any capability using "Test Connector Capability" button.

The following commands are supported by RSA Via Lifecycle and Governance CyberArk Connector:

- Create an Account
- Delete an Account
- Enable an Account
- Disable an Account
- Update an Account
- Rename an Account
- Reset an Account's Password
- Lock an Account
- Unlock an Account
- Create a Group
- Delete a Group
- Add an Account to Group
- Remove an Account from Group
- Update Group

NOTE: Spaces are not allowed in the value of any parameter of all commands.

4.1 Command Input Parameters

1. Create an account.

Field Name	**Value**
Parameter Name	AccountName

Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	${AccountTemplate.AccountName}
Description:	The name of the Account to add to the Vault

Field Name	**Value**
Parameter Name	Password
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	Yes
Display Name	Password
Mapping	${AccountTemplate.Password}
Description:	Password

Field Name	**Value**
Parameter Name	Location
Type	String
Default Value	N/A
Is the parameter required?	Yes

Is the parameter encrypted?	No
Display Name	Location
Mapping	${AccountTemplate.Location}
Description:	Location where Account will reside

Field Name	**Value**
Parameter Name	FirstName
Type	String
Default Value	N/A
Is the parameter required?	No
Is the parameter encrypted?	No
Display Name	First Name
Mapping	${AccountTemplate.FirstName}
Description:	First Name of the Account

Field Name	**Value**
Parameter Name	LastName
Type	String
Default Value	N/A
Is the parameter required?	No
Is the parameter encrypted?	No
Display Name	Last Name
Mapping	${AccountTemplate.LastName}

Description:	Last Name of the Account

Field Name	**Value**
Parameter Name	AdminAccountName
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Admin Account Name
Mapping	${AccountTemplate.AdminAccountName}
Description:	The Account Name of the Account who is logged on i.e. Admin Account name

Field Name	**Value**
Parameter Name	Path
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Path
Mapping	${AccountTemplate.Path}
Description:	Path where CyberArk configuration files are located. e.g. C:\PACLI-part1\PACLI-part1\lib

Command Code

Field Name	**Value**

Shell Command	cd ${Path};./begin.bat;./PACLI ADDUSER DESTUSER="${AccountName}" PASSWORD="${Password}" LOCATION="${Location}" FIRSTNAME="${FirstName}" LASTNAME="${LastName}";
	Note: If a numeric value is to be set to a particular parameter (e.g. Phone Number), that parameter value should be sent using four double quotes (e.g. “””${PhoneNumber}”””) for PowerShell v6 server. e.g. ADDUSER DESTUSER="${AccountName}" PASSWORD="${Password}" LOCATION="${Location}" FIRSTNAME="${FirstName}" LASTNAME="${LastName}" CELLULAR=”””${PhoneNumber}”””;

2. Delete an Account

Field Name	Value
Parameter Name	AccountName
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	${Account.Name}
Description:	The Account Name of the Account to be Deleted

Field Name	**Value**

Parameter Name	AdminAccountName
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Admin Account Name
Mapping	This value may vary as per the CyberArk setup and there is no standard value that can be set as default. Please edit the connector to reflect the actual 'AdminAccountName' being used.
Description:	The Account Name of the Account who is logged on i.e. Admin Account name

Field Name	**Value**
Parameter Name	Path
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Path
Mapping	This value may vary as per the CyberArk setup and there is no standard value that can be set as default. Please edit the connector to reflect the actual 'Path' being used.

Description:	Path where CyberArk configuration files are located e.g. C:\PACLI-part1\PACLI-part1\lib

Command Code

Field Name	**Value**
Shell Command	cd ${Path};./begin.bat;./PACLI DELETEUSER USER="${AdminAccountName}" DESTUSER="${AccountName}";

3. Enable an Account

Field Name	**Value**
Parameter Name	AccountName
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	${Account.Name}
Description:	The Account Name of the Account to be Enabled

Field Name	**Value**
Parameter Name	AdminAccountName
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No

Display Name	Admin Account Name
Mapping	This value may vary as per the CyberArk setup and there is no standard value that can be set as default. Please edit the connector to reflect the actual 'AdminAccountName' being used.
Description:	The Account Name of the Account who is logged on i.e. Admin Account name

Field Name	**Value**
Parameter Name	Path
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Path
Mapping	This value may vary as per the CyberArk setup and there is no standard value that can be set as default. Please edit the connector to reflect the actual 'Path' being used.
Description:	Path where CyberArk configuration files are located e.g. C:\PACLI-part1\PACLI-part1\lib

Command code

Field Name	**Value**
Shell Command	cd ${Path}; ./begin.bat;./PACLI UPDATEUSER USER="${AdminAccountName}" DESTUSER="${AccountName}" DISABLED=NO;

4. Disable an Account

Field Name	**Value**
Parameter Name	AccountName
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	${Account.Name}
Description:	The Account Name of the Account to be Disabled

Field Name	**Value**
Parameter Name	AdminAccountName
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Admin Account Name
Mapping	This value may vary as per the CyberArk setup and there is no standard value that can be set as default. Please edit the connector to reflect the actual 'AdminAccountName' being used.
Description:	The Account Name of the Account who is logged on i.e. Admin Account name

Field Name	**Value**
Parameter Name	Path

Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Path
Mapping	This value may vary as per the CyberArk setup and there is no standard value that can be set as default. Please edit the connector to reflect the actual 'Path' being used.
Description:	Path where CyberArk configuration files are located e.g. C:\PACLI-part1\PACLI-part1\lib

Field Name	**Value**
Shell Command	cd ${Path}; ./begin.bat;./PACLI UPDATEUSER USER="${AdminAccountName}" DESTUSER="${AccountName}" DISABLED=YES;

5. Update an Account

Field Name	**Value**
Parameter Name	AccountName
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	${Account.Name}
Description:	The Account Name of the Account to be Updated

Field Name	**Value**
Parameter Name	AdminAccountName
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Admin Account Name
Mapping	This value may vary as per the CyberArk setup and there is no standard value that can be set as default. Please edit the connector to reflect the actual 'AdminAccountName' being used.
Description:	The Account Name of the Account who is logged on i.e. Admin Account name

Field Name	**Value**
Parameter Name	Path
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Path
Mapping	This value may vary as per the CyberArk setup and there is no standard value that can be set as default. Please edit the connector to reflect the actual 'Path' being used.
Description:	Path where CyberArk configuration files are located e.g. C:\PACLI-part1\PACLI-part1\lib

Field Name	**Value**
Parameter Name	FirstName
Type	String
Default Value	N/A
Is the parameter required?	No
Is the parameter encrypted?	No
Display Name	First Name
Mapping	${User.First_Name}
Description:	First Name of the Account

Field Name	**Value**
Parameter Name	LastName
Type	String
Default Value	N/A
Is the parameter required?	No
Is the parameter encrypted?	No
Display Name	Last Name
Mapping	${User.Last_Name}
Description:	Last Name of the Account

Command code

Field Name	**Value**
Shell Command	cd ${Path}; ./begin.bat;./PACLI UPDATEUSER USER="${AdminAccountName}" DESTUSER="${AccountName}" FIRSTNAME ="${FirstName}" LASTNAME="${LastName}";

	Note: If a numeric value is to be set to a particular parameter (e.g. Phone Number), that parameter value should be sent using four double quotes (e.g. “”””${PhoneNumber}”””””) for PowerShell v6 server. e.g. UPDATEUSER USER="${AdminAccountName}" DESTUSER="${AccountName}" FIRSTNAME="${FirstName}" LASTNAME="${LastName}" CELLULAR=”””””${PhoneNumber}”””””;

6. Rename an Account

Field Name	**Value**
Parameter Name	AccountName
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	${Account.Name}
Description:	The Account Name of the Account to be Updated

Field Name	**Value**
Parameter Name	AdminAccountName
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Admin Account Name
Mapping	This value may vary as per the CyberArk setup and

	there is no standard value that can be set as default. Please edit the connector to reflect the actual 'AdminAccountName' being used.
Description:	The Account Name of the Account who is logged on i.e. Admin Account name

Field Name	**Value**
Parameter Name	Path
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Path
Mapping	This value may vary as per the CyberArk setup and there is no standard value that can be set as default. Please edit the connector to reflect the actual 'Path' being used.
Description:	Path where CyberArk configuration files are located e.g. C:\PACLI-part1\PACLI-part1\lib

Field Name	**Value**
Parameter Name	NewName
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	New Name
Mapping	-

Description:	New Name to be Updated

Command code

Field Name	**Value**
Shell Command	cd ${Path}; ./begin.bat;./PACLI RENAMEUSER USER="${AdminAccountName}" DESTUSER="${AccountName}" NEWNAME = "${NewName}";

7. Reset an Account's Password

Field Name	**Value**
Parameter Name	AccountName
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	${Account.Name}
Description:	The Account Name of the Account for which password will be reset

Field Name	**Value**
Parameter Name	OldPassword
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	Yes

Display Name	Account's Current Password
Mapping	-
Description:	Account's Current Password

Field Name	**Value**
Parameter Name	NewPassword
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	Yes
Display Name	Account's New Password
Mapping	-
Description:	Account's New Password

Field Name	**Value**
Parameter Name	Path
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Path
Mapping	This value may vary as per the CyberArk setup and there is no standard value that can be set as default. Please edit the connector to reflect the actual 'Path' being used.
Description:	Path where CyberArk configuration files are located

	e.g. C:\PACLI-part1\PACLI-part1\lib

Command Code

Field Name	**Value**
Shell Command	cd ${Path}; ./begin.bat;./PACLI LOGON USER="${AccountName}" PASSWORD="${OldPassword}";./PACLI SETPASSWORD USER="${AccountName}" PASSWORD="${OldPassword}" NEWPASSWORD="${NewPassword}";./PACLI LOGOFF USER="${AccountName}";

8. Create a Group

Field Name	**Value**
Parameter Name	GroupName
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Group Name
Mapping	-
Description:	Group to be Created

Field Name	**Value**
Parameter Name	AdminAccountName
Type	String
Default Value	N/A
Is the parameter required?	Yes

Is the parameter encrypted?	No
Display Name	Admin Account Name
Mapping	This value may vary as per the CyberArk setup and there is no standard value that can be set as default. Please edit the connector to reflect the actual 'AdminAccountName' being used.
Description:	The Account Name of the Account who is logged on i.e. Admin Account name

Field Name	**Value**
Parameter Name	Path
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Path
Mapping	This value may vary as per the CyberArk setup and there is no standard value that can be set as default. Please edit the connector to reflect the actual 'Path' being used.
Description:	Path where CyberArk configuration files are located e.g. C:\PACLI-part1\PACLI-part1\lib

Field Name	**Value**
Parameter Name	Location
Type	String
Default Value	N/A
Is the parameter required?	Yes

Is the parameter encrypted?	No
Display Name	Location
Mapping	-
Description:	Location where Account will reside

Command code

Field Name	**Value**
Shell Command	cd ${Path}; ./begin.bat;./PACLI ADDGROUP USER ="${AdminAccountName}" GROUP="${GroupName}" LOCATION="${Location}";

9. Delete a Group

Field Name	**Value**
Parameter Name	GroupName
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Group Name
Mapping	${Group.Name}
Description:	Group to be Created

Field Name	**Value**
Parameter Name	AdminAccountName
Type	String

Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Admin Account Name
Mapping	This value may vary as per the CyberArk setup and there is no standard value that can be set as default. Please edit the connector to reflect the actual 'AdminAccountName' being used.
Description:	The Account Name of the Account who is logged on i.e. Admin Account name
Field Name	**Value**
Parameter Name	Path
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Path
Mapping	This value may vary as per the CyberArk setup and there is no standard value that can be set as default. Please edit the connector to reflect the actual 'Path' being used.
Description:	Path where CyberArk configuration files are located e.g. C:\PACLI-part1\PACLI-part1\lib

Command code

Field Name	**Value**
Shell Command	cd ${Path}; ./begin.bat;./PACLI DELETEGROUP USER ="${AdminAccountName}" GROUP="${GroupName}";

10. Add an Account to Group

Field Name	**Value**
Parameter Name	AccountName
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	${Account.Name}
Description:	Name of the account that will be added to the group

Field Name	**Value**
Parameter Name	GroupName
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Group Name
Mapping	${Group.Name}
Description:	The name of the group

Field Name	**Value**
Parameter Name	AdminAccountName
Type	String
Default Value	N/A

Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Admin Account Name
Mapping	This value may vary as per the CyberArk setup and there is no standard value that can be set as default. Please edit the connector to reflect the actual 'AdminAccountName' being used.
Description:	The AccountName of the Account that is carrying out the command

Field Name	**Value**
Parameter Name	Path
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Path
Mapping	This value may vary as per the CyberArk setup and there is no standard value that can be set as default. Please edit the connector to reflect the actual 'Path' being used.
Description:	Path where CyberArk configuration files are located e.g. C:\PACLI-part1\PACLI-part1\lib

Command code

Field Name	**Value**
Shell Command	cd ${Path}; ./begin.bat;./PACLI ADDGROUPMEMBER USER="${AdminAccountName}" GROUP="${GroupName}"

	MEMBER="${AccountName}";

11. Remove an Account from Group

Field Name	**Value**
Parameter Name	AccountName
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	${Account.Name}
Description:	Name of the account that will be removed from the group

Field Name	**Value**
Parameter Name	GroupName
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Group Name
Mapping	${Group.Name}
Description:	The name of the group

Field Name	**Value**

Parameter Name	AdminAccountName
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Admin Account Name
Mapping	This value may vary as per the CyberArk setup and there is no standard value that can be set as default. Please edit the connector to reflect the actual 'AdminAccountName' being used.
Description:	The AccountName of the Account that is carrying out the command

Field Name	**Value**
Parameter Name	Path
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Path
Mapping	This value may vary as per the CyberArk setup and there is no standard value that can be set as default. Please edit the connector to reflect the actual 'Path' being used.
Description:	Path where CyberArk configuration files are located e.g. C:\PACLI-part1\PACLI-part1\lib

Command code:

Field Name	**Value**
Shell Command	cd ${Path}; ./begin.bat;./PACLI DELETEGROUPMEMBER USER="${AdminAccountName}" GROUP="${GroupName}" MEMBER="${AccountName}";

12. Update Group

Field Name	**Value**
Parameter Name	GroupName
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Group Name
Mapping	${Group.Name}
Description:	Name of Group that will be updated

Field Name	**Value**
Parameter Name	AdminAccountName
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Admin Account Name
Mapping	This value may vary as per the CyberArk setup and there is no standard value that can be set as default. Please edit the connector to reflect the actual 'AdminAccountName' being used.
Description:	The AccountName of the Account that is carrying out the command

Field Name	**Value**

Parameter Name	Location
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Location
Mapping	“”
Description:	Location where group resides. Note: Add a backslash \ before the name of the location

Field Name	**Value**
Parameter Name	Path
Type	String
Default Value	N/A
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Path
Mapping	This value may vary as per the CyberArk setup and there is no standard value that can be set as default. Please edit the connector to reflect the actual ‘Path’ being used.
Description:	Path where CyberArk configuration files are located e.g. C:\PACLI-part1\PACLI-part1\lib

Command code:

Field Name	**Value**

Shell Command	cd ${Path}; ./begin.bat;./PACLI DELETEGROUPMEMBER USER="${AdminAccountName}" GROUP="${GroupName}" MEMBER="${AccountName}";

5. Tips and Troubleshooting

1. By default, when the CyberArk collector is created through RSA Via L&G, it has table names. For example, userlist_mod is the default for user list.
   If you modify the names of the output CSV files while running the 'csvtransformer.jar', , do not forget to edit the collector to reflect that change.
2. In ExportVaultData utility, for more details on error Check log.txt
   - **Error: ITACM012S Timeout has expired** then check Vault.ini. It should contain the correct address of the vault machine.
   - **Error: ITATS006E Station is suspended for User,** please follow CyberArk's solution #00000031.
     - Using CyberArk's PrivateArk Client tool, connect as an administrator user and do the following:
       - Go to Tools | Administrative Tools | Users & Groups.
       - Highlight the relevant User and click the "Trusted Net Areas" button.
       - Highlight the suspended Area and click the "Activate" button.
       - Highlight the relevant User and click the "Update" button.
       - Go to "Authentication" tab and enter the new password (twice).
     - Re-create the credential file as described previously in this document
   - If generated CSV files are empty, then check user has at least auditor access. For creating a new user with the desired access, user PrivateArk client

3. In case the wrong CSV file URL/path is provided , the collector can show the error "Could not get account data".
4. If the files generated after running the CSVTransformer are empty, make sure that the input file path in config.properties is correct.
5. For troubleshooting, refer the connector logs from the location AFX/esb/logs.
6. It is always a good practice to enable the SSH server logs so that each activity related to the SSH server will be logged in the log file and used for the troubleshooting.
7. For troubleshooting, enable the debug SSH logs, using following steps.

   Go to AFX/esb/apps/<ConnectorName>/connector-flow.xml and change the "logger level" value from "DEBUG" to "INFO" in two places.

```
    </otherwise>
</choice>

<!-- send back response -->
<flow-ref name="AFX_OUT"/>

<logger level="DEBUG" message="SSH payload with out params: #[payload]"/>
```

```
<!-- endpoint processing -->
<flow name="SSH_Conn" processingStrategy="synchronous">

    <!-- read in a JMS message from queue -->
    <jms:inbound-endpoint queue="AFX.JMS.EP.SSH_Conn" connector-ref="jmsConnector"/>
    <logger level="DEBUG" message="XML Payload from JMS: #[payload]"/>
```

Appendix

A. Data Mapping between CyberArk and RSA Via L&G Collector

A. Account Data Collector

I. Accounts

We collect the following attributes from userlist_mod.csv

Attribute	Data type
Userid	String
Username	String
Firstname	String
Lastname	String
Business email	String
Disabled	Integer
ExpirationDate	Date
Internal/External	Integer (1 = internal, 2 = external)
LDAPfullDN	String
LastLoginDate	Date
CreationDate	Date
UserTypeID	String

II. Groups

We collect the following attributes from groupslist_mod.csv

Attribute	Data type
GroupID	String
GroupName	String
Description	String
ExternalGroupName	String
Internal	String
LDAPFullDN	String

III. Account Membership

We determine the account membership by cross referencing userlist_mod.csv, groupslist_mod.csv and groupmemberslist_mod.csv.

B. Entitlement Collector

We collect the following attributes to define the EDC as OwnerName with Resource: Action

Attribute	**Data type**
OwnerName	String
OwnerType	String
Resource	String
Action	String

Note:

I. The "Resource" string is collected by referencing to the ownerslist and objectproperty CSV's (generated as 'entitlement.csv' after running CyberArk's ExportVaultData utility and then running the data transformer utility) in the format of Safename=<SafeName>,username=<UserName>yyy,policyid=<PolicyID>,address=<Address>

II. Modified CSV are generated as follows:
ExportVaultData Utility -> unmodified.csv ->Data Transformer Utility -> modified.csv

Custom Attributes for an account:

1. Internal/External
2. Business email
3. LDAPfullDN
4. CreationDate
5. UserTypeID
6. ExpirationDate

Note: Make sure to add the additional attributes through the Admin > Attributes > Account Ta **Custom Attributes for a group:**

1. LDAPfullDN
2. ExternalGroupName
3. Internal/External

Note: Make sure to add the additional attributes through the Admin > Attributes > Group Tab

COPYRIGHTS

TRADEMARKS