

PAS Reporter Quick Start Guide



- PAS Reporter v0.60 -

Contents

1	Using PAS Reporter	2
1.1	Manual mode	2
1.2	Integrated Mode	4
1.3	Automatic Mode.....	7
1.3.1	Example scheduled task configuration.....	8
2	FAQ.....	9

1 Using PAS Reporter

The PAS Reporter can generally be used in three modes; “Manual mode”, “Integrated mode” and “Automatic mode”. In the manual mode, Export Vault Data (EVD) export CSV-files and supported configuration and logfiles can be dragged and dropped into the tool for generating the reports.

In the integrated mode, the EVD exports and the supported configuration files can be retrieved with the EVD and PACLI integrations from the Vault.

The automatic mode is basically the integrated mode, but the exporting and reports generation actions are triggered via command line parameters. This allows running the tool as scheduled task for instance.

1.1 Manual mode

In the manual mode, you can drag and drop supported EVD exports and configuration files in the according sections of the tool. The supported EVD exports and configuration files are described in the FAQ section in this guide.

You can find example scripts in the “evd” folder of the tool for retrieving the EVD exports and configuration files from the Vault. The configuration files can also be retrieved from the Vault using the PrivateArk Client. Please note, that this requires specific permissions on the relevant safes in the Vault. The required permissions are described in the FAQ section in this guide.

Once the EVD exports and configuration files were added, the reports can be generated. Please note, that the tool can provide the most information if all supported EVD exports and all supported configuration files were added.

Add Export Vault Data export files below				
	EVD export file	Export Type	Link to file	Size
▶	LogList.csv	Logs	Open	48.54 MB
	MasterPolicySettings.csv	MasterPolicy	Open	36.22 KB
	ObjectProperties.csv	ObjectProperties	Open	1.12 MB
	OwnersList.csv	Owners	Open	133.97 KB
	SafesList.csv	Safes	Open	11.81 KB
	UsersList.csv	Users	Open	12.62 KB
	FilesList.csv	Files	Open	1011.65 KB
	GroupMembersList.csv	GroupMembers	Open	667 B
	GroupsList.csv	Groups	Open	2.22 KB
EVD export files in list: 9				

Figure 1: EVD export CSV-files are added to the tool

Configuration file	Type	Link to file
DBParm.ini	DBParm config file	Open
Policies.xml	Policies XML file	Open
Policy-AnsibleAWX.ini	Platform policy file	Open
Policy-as400.ini	Platform policy file	Open
Policy-AWS-PSM4C.ini	Platform policy file	Open
Policy-AWS.ini	Platform policy file	Open
Policy-AWSAccessKeys.ini	Platform policy file	Open
Policy-AWSRootAccount.ini	Platform policy file	Open

Configuration files in list: 94

Figure 2: Supported configuration files or logfiles are added to the tool

Once supported files were added, the files can be processed by clicking the “Process Files” button.

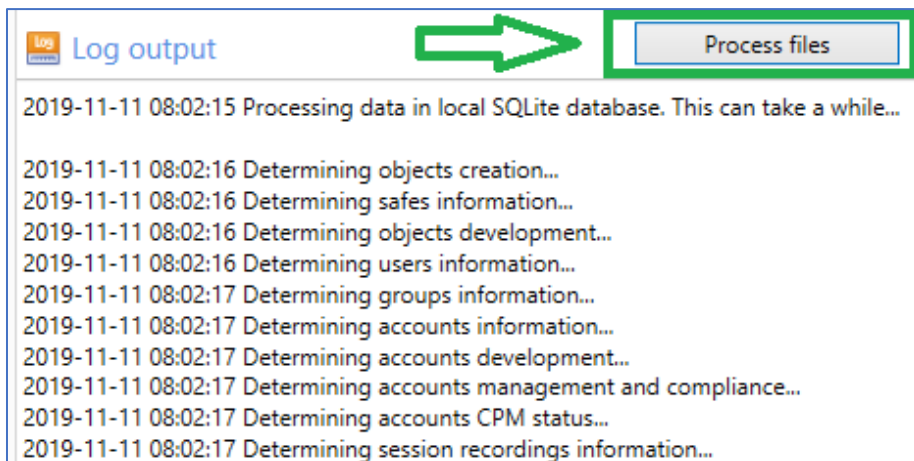


Figure 3: The manually added EVD exports and configurations files are getting processed

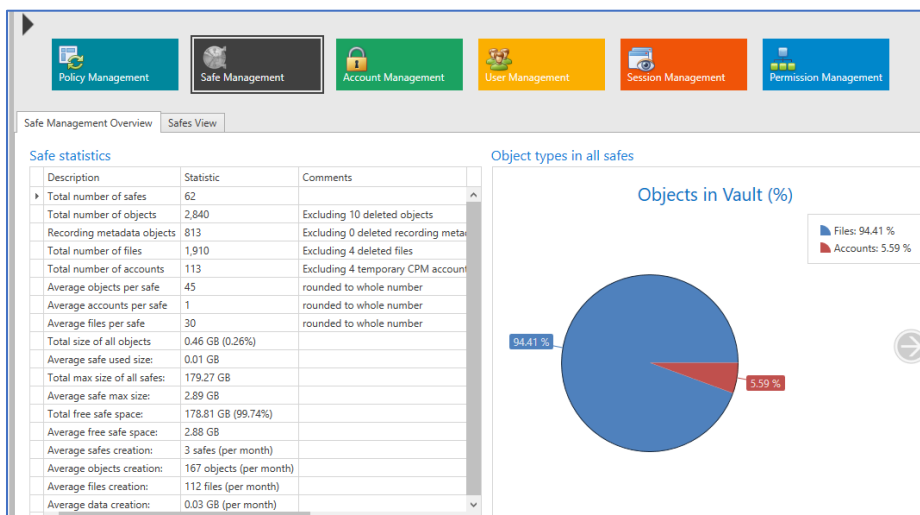


Figure 4: Reports data can be seen if the reports generation as successful

1.2 Integrated Mode

The integrated mode allows retrieving EVD exports as well as supported configuration files from the Vault with the tool's EVD and PACLI integrations.

Therefore, the tool needs to be configured through the settings menu of the tool.

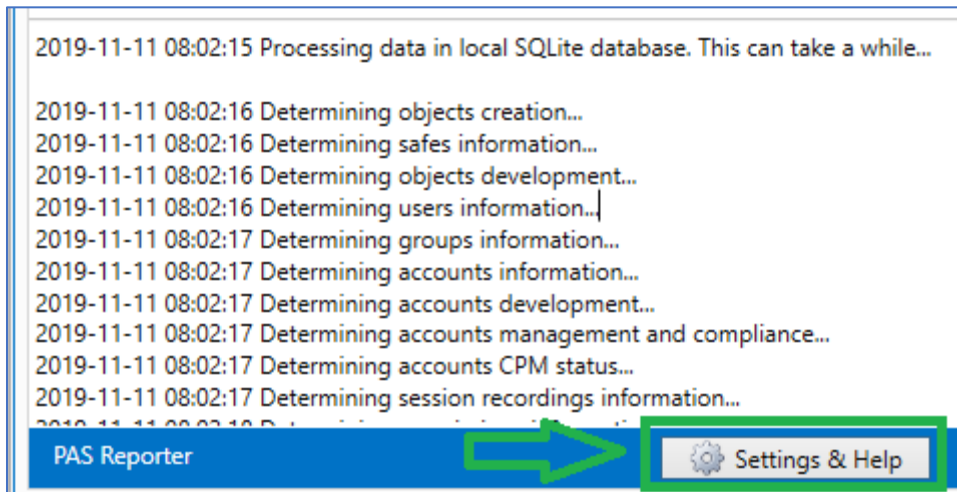


Figure 5: Click on the “Settings & Help” button to open the settings menu

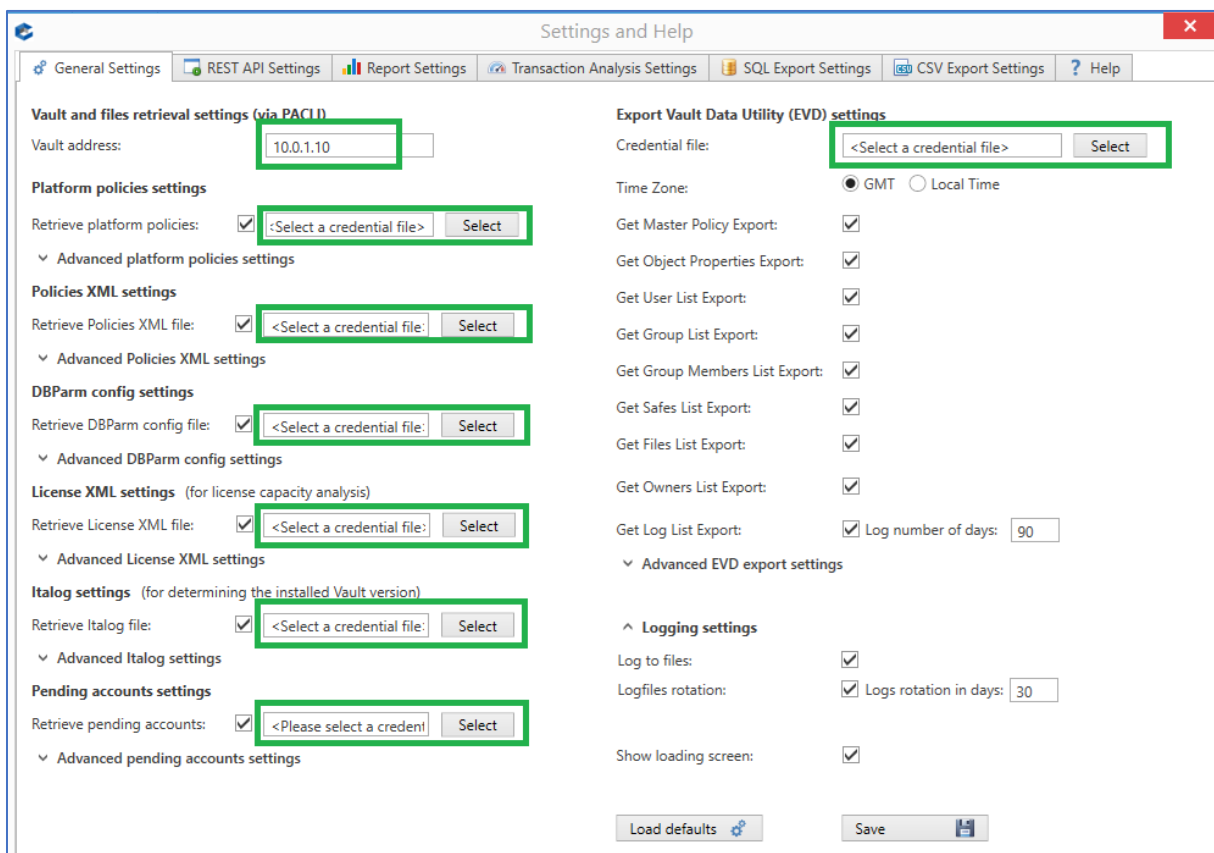


Figure 6: Set the Vault IP, and select credentials files for PACLI and EVD

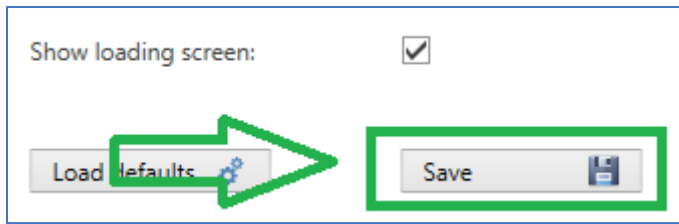


Figure 7: Save the settings by clicking on the “Save” button

Once the settings were applied, the EVD exports and the supported configuration files can be retrieved from the Vault by clicking on the according buttons in the tool.

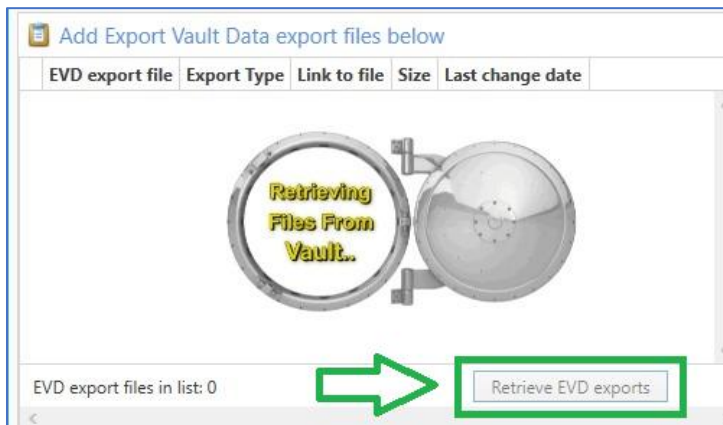


Figure 8: By clicking on “Retrieve EVD exports”, the tool tries retrieving the EVD export from the Vault

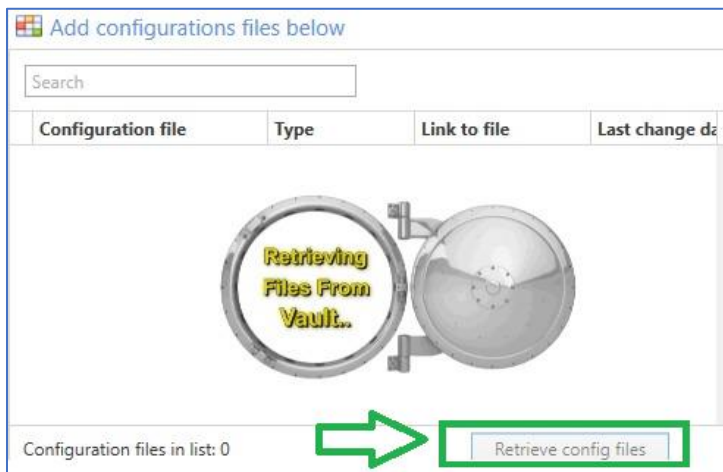


Figure 9: By clicking on “Retrieve config files”, the tools tries retrieving configuration files via PACLI

During the EVD exports and the configuration files retrieval procedures via PACLI, you can check the logs section if the operations are carried out successfully.

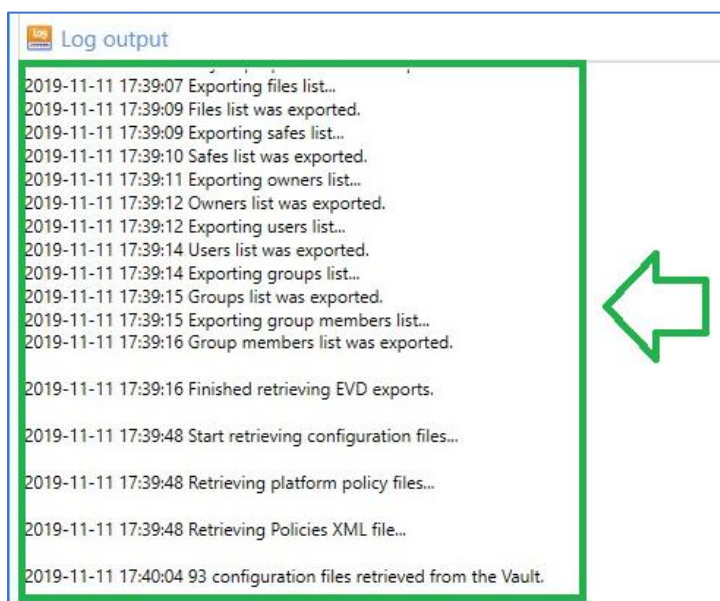


Figure 10: The “Log output” section provides information about the status of the retrieval procedures

Once the EVD exports and configuration files were successfully retrieved, the reports can be generated by clicking on the “Process files” button.

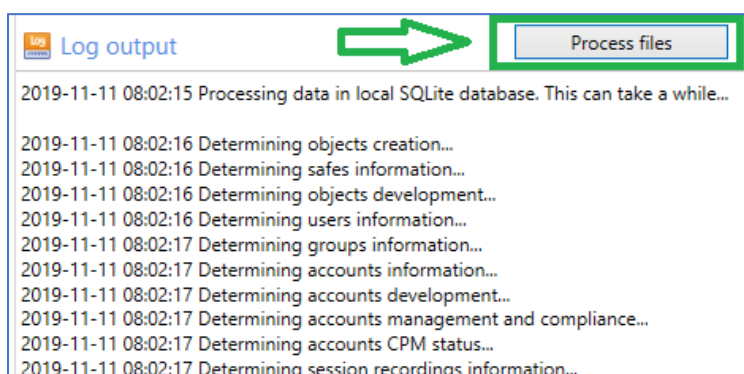


Figure 11: The EVD exports and configurations files are getting processed

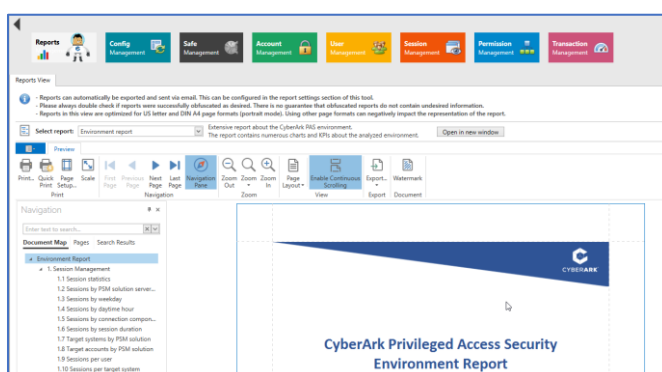


Figure 12: Once the files were successfully processed, reports can be seen in the according report sections

1.3 Automatic Mode

The automatic mode is basically the integrated mode, but the exporting and reports generation actions are triggered automatically via command line parameters. This allows running the tool as scheduled task for instance.

Please note, that EVD exports are creating load on the Vault. Therefore, it can be an idea to run the tool only once per day outside of business hours for instance.

In order to run the tool in automatic mode, it needs to be configured as described in the *Integrated Mode* section in this guide.

You can then run the PAS Reporter.exe with the “/?” parameter in order to see the automatic mode parameter options as well as according examples.

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\PAS Reporter v0.40>"PAS Reporter.exe" /?
```

Figure 13: Run PAS Reporter with the /? parameter to open the automation help window

PAS Reporter - Automation Help

Argument	Required/Optional	Description
/full XOR /evdOnly XOR /pacliOnly	Required	/full = Retrieve EVD exports as well as supported configuration files via PACLI (recommended) /evdOnly = Retrieve EVD exports only /pacliOnly = Retrieve configuration files only
/silent	Optional	/silent = Runs PAS Reporter silently (without UI) and closes the PAS Reporter automatically once the export and processing procedures are completed. Recommended when running PAS Reporter as scheduled task for instance.
/force	Optional	/force = Closes running PAS Reporter instance. Only one instance of a PAS Reporter executable can be run at the same time. The /force argument will close a running PAS Reporter instance automatically which can be useful when running the PAS Reporter as scheduled task for instance. If this argument is not being used and the PAS Reporter instance is already running, the automation procedure will be aborted and according information will be logged in the PAS Reporter automation log file.
/close	Optional	/close = Only relevant when NOT using the /silent argument. Closes the PAS Reporter UI once the export and processing procedures are completed.
/minimized	Optional	/minimized = Only relevant when NOT using the /silent argument. Starts the PAS Reporter UI in a minimized window.
/continueOnError	Optional	/continueOnError = Only relevant when using the /full export argument. This setting will try retrieving configuration files if EVD exports failed (instead of aborting the entire automation procedure).

Hints

- All arguments are case insensitive
- Automation logs can be found in the logs folder



PAS Reporter Automation

Example	Copy	Run	Description
"PAS Reporter.exe" /full /force			Runs PAS Reporter and retrieves both, EVD exports and supported configuration files (/full). Closes running PAS Reporter instance (/force).
"PAS Reporter.exe" /full /silent /force			Runs PAS Reporter in silent mode (/silent). Retrieves both, EVD exports and supported configuration files (/full). Closes running PAS Reporter instance (/force).
"PAS Reporter.exe" /full /close /force			Runs PAS Reporter and closes UI when procedures are finished (/close). Closes running PAS Reporter instance (/force). Retrieves both, EVD exports and supported configuration files (/full).
"PAS Reporter.exe" /full /continueOnError /force			Runs PAS Reporter and retrieves both, EVD exports and configuration files (/full). Will try to retrieve supported configuration files if EVD exports failed (/continueOnError). Closes running PAS Reporter instances (/force).
"PAS Reporter.exe" /evdOnly /minimized /force			Runs PAS Reporter in minimized windows (/minimized). Retrieves EVD exports only (/evdOnly). Closes running PAS Reporter instance (/force).
"PAS Reporter.exe" /pacliOnly /force			Runs PAS Reporter and retrieves supported configuration files only (/pacliOnly). Closes running PAS Reporter instance (/force).

Figure 14: See available automation parameters and examples in the automation help window

1.3.1 Example scheduled task configuration

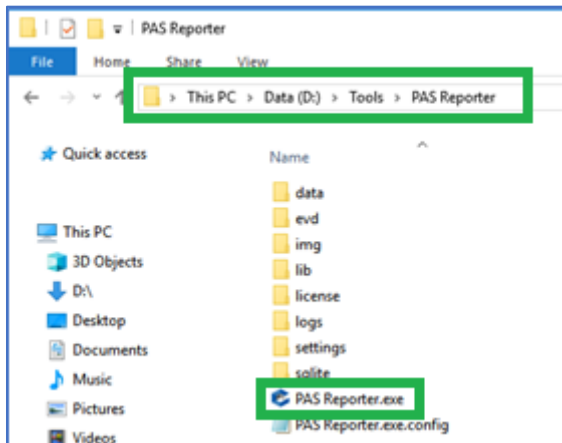


Figure 15: PAS Reporter folder

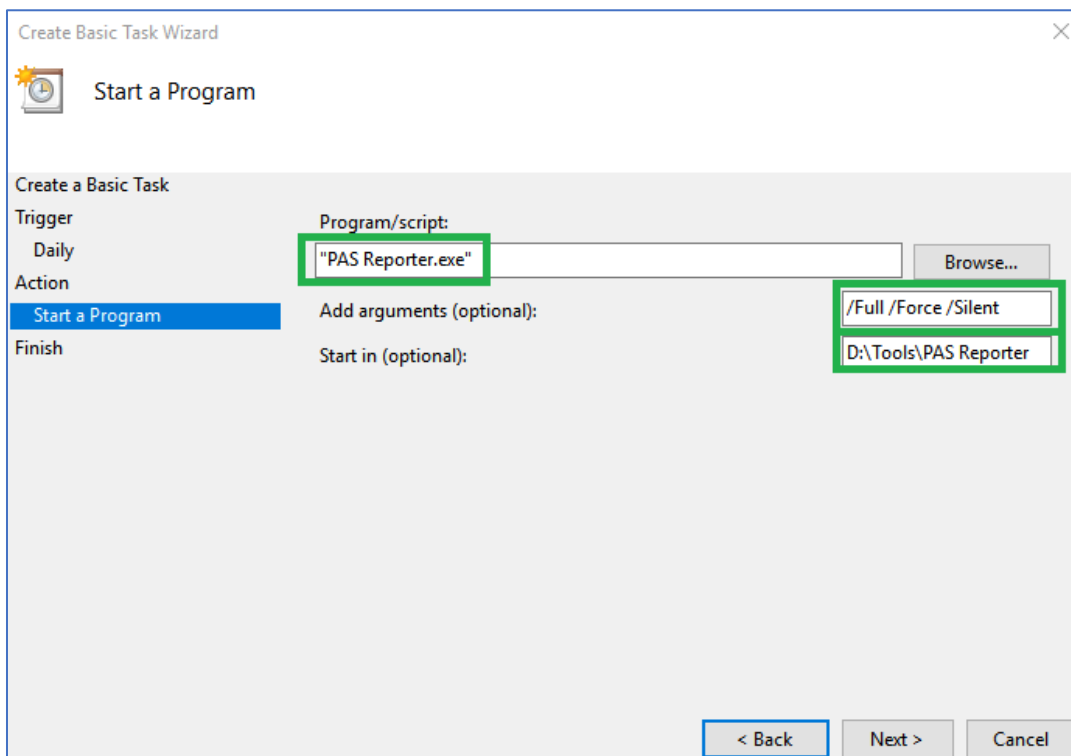


Figure 16: Scheduled task configuration

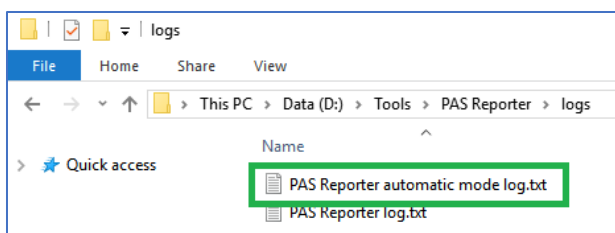


Figure 17: Check the PAS Reporter automatic mode log

2 FAQ

Is this tool supported or maintained by CyberArk?

This is a community tool which does not come with any support or maintenance. Please refer to the "CyberArk Marketplace Terms of Use" for further information.

If you want to support the idea of PAS Reporter becoming a supported tool, you might want to take a look at the following enhancement request: <https://cyberark-customers.force.com/s/enhancement-request-detail?id=0872J000000kCluQAE>

Can I open a support case at CyberArk with regards to this tool (e. g. when I have an issue or a question about the tool)?

CyberArk support cases with regards to this tool will not be handled since this is a non-supported community tool. Questions, feedback, or other matters regarding this tool can be discussed in the CyberArk Customer Community for instance.

Will this tool experience further development?

This tool will not experience further development. We recommend the officially supported CyberArk Telemetry tool for reporting and keeping track of your project's success and outcomes.

Is the information which the tool generates accurate?

The tool was developed with the ambition to provide accurate and helpful information and insights. However, there is no guarantee that the information which the tool generates is accurate.

On which data sources does the tool rely on?

The tool analyzes Export Vault Data (EVD) exports as well as various configuration files, Vault trace logs, and information retrieved via REST API.

How can I use this tool?

Generally, there are three options:

- 1) Retrieve EVD export CSV files as well as supported configuration files from the Vault and add them to the tool. This can be achieved via dragging and dropping the EVD export CSV files as well as the supported configuration files to the according sections of the tool.
- 2) Retrieval of the EVD exports and supported configuration files through the EVD and PACLI integrations of the tool. The authentication for EVD and PACLI needs to happen via credential files for the according EPV users.
- 3) Run the tool in automatic mode (e. g. as scheduled task)

What are the system requirements for this tool?

The tool requires a Windows 64-Bit OS with .NET Framework 4.5.2 or higher.

The recommended hardware specifications are:

- Dual-Core CPU @2.0 GHz
- 16 GB of RAM
- 300 MB disk space for the tool itself + additional disk space depending on the amount of retrieved and generated data
- Screen with Full HD resolution (1.920 x 1.080) or higher
 - Users with high resolution screens (e. g. 4K or Ultrawide resolutions) will benefit since charts will scale in accordance to the screen resolutions
 - Particularly users with screen resolutions lower than Full HD resolution (1.920 x 1.080) might need to open charts in a new window sometimes to see all details

Where does the tool store the generated data?

The tool stores the generated data in the tool's SQLite database files (PASReporter.db & VaultTraces.db) in the data folder of the tool.

Which permissions or authorization are required to retrieve the desired information from the Vault?

For the retrieval of supported configuration files via PACLI, the user which is used for the retrieval needs sufficient permissions on the according safes. By default, those safes usually are:

Safe	Permissions	Comments
PasswordManagerShared	• List Files • Retrieve Files	Contains the platform policy files
PVWAConfig	• List Files • Retrieve Files	Contains the Policies.xml file
PasswordManager_Pending	• List Files	Contains the pending accounts
System	• List Files • Retrieve Files • Update/Store Files*	Contains the DBParm.ini file, the License.xml file, and the Italog.log file

* Please note: Depending on the PAS version and other possible factors, it can be that the "Update/Store Files" permissions will be required in addition to the "List Files" and "Retrieve Files" permissions on the System safe.

In order to retrieve all EVD exports that are supported from this tool, an EPV user requires the "Audit Users" Vault authorization. Furthermore, the EVD export user can be added to the built-in CyberArk "Auditors" group which usually has sufficient permissions on the relevant safes. However, this might differ depending various factors such as the CyberArk PAS version, configurations in your environment, and other possible factors.

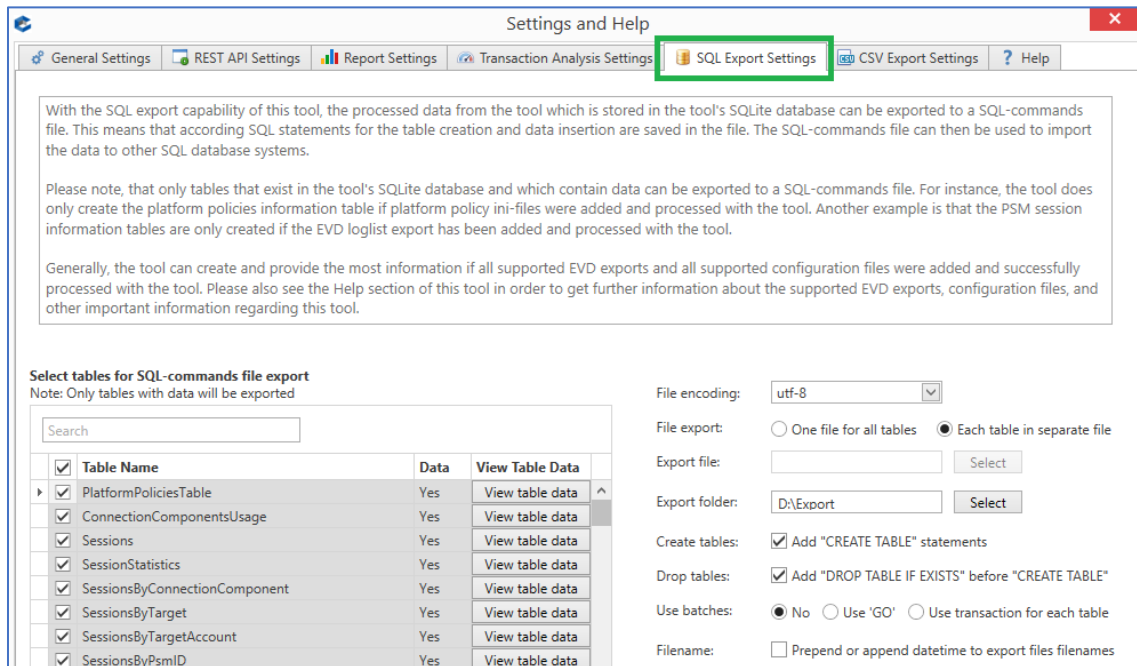
Furthermore, please always check the official CyberArk EVD documentation in order to ensure, that the EVD export user is configured with least privileges.

Please note, that Vault trace files cannot be retrieved via EVD or PACLI. Please see the *"Where can I find the Vault trace files which can be processed with this tool?"* in the FAQ section.

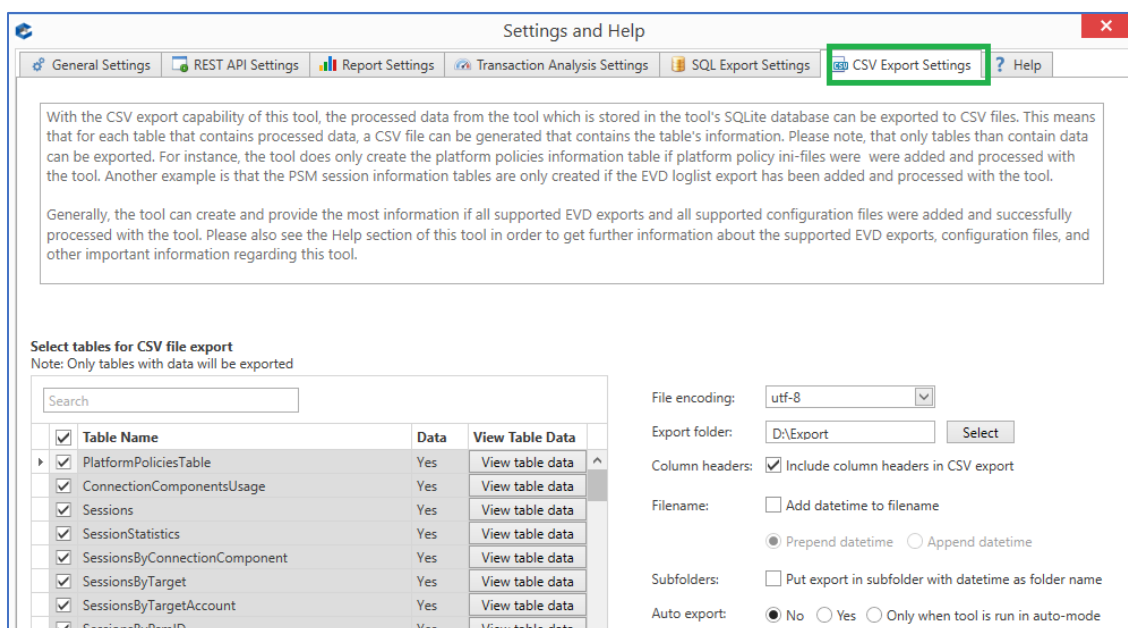
Can I export data from this tool?

Yes, please make a right click on any data grid or chart that you would like to export. There will appear a context menu with according exporting options (e. g. export to Excel, CSV, or PNG).

Furthermore, you can export the generated data from this tool to a SQL-commands file. This can allow you to import data from this tool into other SQL database system. This can be configured in the “SQL Export Settings” of the tool.



Additionally, the PAS Reporter data can also be bulk-exported to CSV files. This can be configured in the “CSV Export Settings” of the tool.



Furthermore, there are summary reports available that allow exporting numerous charts and KPIs in a structured document (PDF, DOCX, XLSX, HTML).

The summary reports can be found in the “Reports” section of the tool.

The screenshot displays the 'Reports View' section of the CyberArk Privileged Access Security tool. The top navigation bar includes 'Reports' (highlighted), 'Config Management', 'Safe Management', 'Account Management', 'User Management', 'Session Management', 'Permission Management', and 'Trans Mana'. Below the navigation bar, a 'Reports View' header contains informational text and a 'Select report:' dropdown menu set to 'Environment report'. A 'Preview' tab is active, showing a toolbar with options like 'Print...', 'Quick Print', 'Page Setup...', 'Scale', 'Navigation', 'Zoom Out', 'Zoom In', 'Page Layout', 'Enable Continuous Scrolling', 'Export...', and 'Watermark'. The left sidebar, titled 'Navigation', shows a 'Document Map' with a tree structure: 'Environment Report' (expanded), '1. Installed Product Versions', '2. License Capacity', '3. Account Management' (expanded), '4. Safe Management', and '5. Session Management'. The main content area displays the 'CyberArk Privileged Access Security Environment Report' for 'Version v11.5'. It features the CyberArk logo, a cartoon character, and the text 'CyberArk Example Environment'. The date and time 'Sunday, July 12, 2020 - 07:27 PM' are shown at the bottom.

The reports can also be automatically sent via email. Please also see “How can I automatically send reports via email?” in this guide.

Some of the reports also offer an automated obfuscation of the data. This can be useful if there is sensitive information in the reports which is not supposed to be shared.

Can I run several instances of the tool?

You can run several instances of the tool. Therefore, you can make copies of the entire tool (not only the executable of the tool) and run copies of the tool simultaneously.

It is not possible to run several instances of the same PAS Reporter executable (let's say for example on "D:\PAS Reporter\PAS Reporter.exe"). The reason is that running several instances of the same PAS Reporter executable can cause issues with e. g. simultaneous write access operations to the tool's SQLite database.

You can run for example "D:\PAS Reporter\PAS Reporter.exe" and "F:\PAS Reporter\PAS Reporter.exe" simultaneously since both copies of the tool will have their dedicated SQLite databases and run dedicated processes.

Do I need to use the tool in order to retrieve the EVD exports and the configuration files from the Vault?

No, you do not need to use this tool to retrieve the EVD exports or the configuration files. You can also retrieve the configuration files manually from the according safes in the Vault.

You can also find script examples in the "evd" folder of this tool for retrieving the EVD exports and the configuration from the Vault. Once the files were retrieved, you can drag and drop them into the tool.

How does the tool import EVD exports and configuration files into its SQLite database?

If the files and information are retrieved via the built-in EVD and PACLI integrations of the tool, the EVD exports are retrieved as CSV files from the Vault in a subfolder of the "data" folder of the tool. The configurations files are also retrieved on a subfolder of the "data" folder of the tool.

Once the EVD export CSV files were retrieved, they are automatically imported into the tool's SQLite database by using "sqlite3.exe" utility for further processing.

The configuration files are getting processed during the data processing procedure of the tool and the processed information is then stored in the tool's SQLite database.

How can I see which information the tool has stored and analyzed?

The information which the tool has generated is stored in the tool's SQLite database files. The generated information is automatically loaded from the database and illustrated in the tool's user interface when the tool was started. There are also tools available that allow you opening and exploring the tool's SQLite database.

The EVD export CSV files and the configuration files which were retrieved through this tool, are stored in according subfolders of the "data" folder of this tool. Furthermore, you can see table data information from the tool's local SQLite database in the SQL export settings section and the transaction management section of this tool.

Which EVD exports can be analyzed with the tool?

The tool supports the following 9 EVD exports:

- Master Policy export
- Files list export
- Safes list export
- Object properties export
- User list export
- Group list export
- Group members export
- Owner list export
- Log activities export

The tool will show according messages if un-supported EVD exports are added.

Which configuration files and logfiles can be analyzed with the tool?

The tool currently supports the following files:

- Platform policy ini-files
- The Policies.xml file.
- The License.xml file
- The DBParm.ini files
- Vault trace logfiles
- Vault Italog logfile

Additionally, the following information can be retrieved via REST API through the tool's REST API integrations:

- Additional platform policies information (e. g. whether or not a platform is active)
- Installed component versions
- OPM policy rules

Which EVD exports cannot be analyzed individually?

The following EVD exports are dependent on each other for the data processing procedure of the tool and can only be analyzed together:

- Files list export
- Safes list export
- Object properties export
- User list export
- Group list export
- Group members export
- Owner list export

The tool will show according messages if dependent reports are missing.

Which EVD exports can be analyzed individually?

The following EVD exports can be analyzed individually:

- Master Policy export
- Log activities export

How can I get the maximum information from the tool?

The tool can generate the most information if all supported EVD exports and all supported configuration files and logfiles were added and analyzed. Furthermore, the REST API integration of the tool should be used so that information can be retrieved that is (exclusively) available via the REST API.

How can I create credential files for EVD and PACLI?

Please refer to the official CyberArk documentation: <https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/CreateCredFile-Utility.htm>

Should I use separate credential files with individual EPV users to retrieve information from the Vault?

It is recommended to use separate credential files with individual EPV users that have the least privileges for retrieving the desired information.

Do I need to run this tool with administrative privileges (e. g. local Administrator on Windows)?

Generally, this tool was designed to run without administrative privileges. However, this might differ depending on your system, its configuration, and other factors.

Where can I find the logs from the tool?

You can find the logs from the tool in the "logs" folder. Logfiles will be automatically created if logging to files was enabled in the tool's settings.

Why does the tool sometimes need to convert EVD exports?

The tool uses a SQLite database. This database only supports the ISO 8601 DateTime format. EVD exports that were generated on a system which does not have this DateTime format set, need to be converted so that the data can be imported in the SQLite database of this tool.

EVD exports that are generated through this tool do not need to be converted since the exports will automatically be generated with the ISO 8601 DateTime format.

How does the integrated EVD from this tool generate exports with the ISO 8601 DateTime format?

The EVD executable (ExportVaultData.exe) is run in a so-called culture context that uses the ISO 8601 format as DateTime pattern. As a result, the EVD exports are generated with the ISO 8601 DateTime format.

How can I delete the generated data from the tool?

The tool stores the generated data in the tool's SQLite database files in the data folder. You can delete the database files (PASReporter.db & VaultTraces.db) or delete the entire data folder for instance.

On some charts I cannot see the labels or the legend. What can I do?

The labels or legends from charts can "disappear" if your screen resolution is low (e. g. smaller than 1.920 x 1.080) or if the labels or legends contain long strings. In those cases, you can make a right click on the chart and select the "Open in new window" option. This will open the chart in a new window which can also be resized as desired.

What can I do to improve the performance of the tool?

Please make sure that there is enough free memory available for the tool. For data writing procedures (e. g. importing data in the tool's SQLite database), fast disk drives (e. g. SSDs) can improve the performance. It has also been observed, that the tool runs in many cases faster on physical hardware - compared to virtual machines with similar specifications.

Why are the executables of this tool not signed by CyberArk?

The executables of this tool are not signed by CyberArk because this tool is a non-supported community tool.

Which information is needed in order to create the license capacity report?

In order to create the license capacity report, the License.xml file as well as the "Users" EVD export and its dependent EVD exports need to be added and processed.

Please note, that the accuracy of the license capacity report highly depends on having complete EVD exports. For instance, if the "Users" EVD export is not complete (e. g. users are missing in the export), the accuracy of the license capacity report is negatively impacted. In any case, the accuracy of the license capacity report from this tool cannot be guaranteed and the report should not be considered as an adequate "equivalent" for the native license capacity report.

Where can I find the Vault trace files which can be processed with this tool?

The Vault traces files can usually be found in the “Logs” folder of the CyberArk Vault installation.
For instance: “<Drive>:\Program Files (x86)\PrivateArk\Server\Logs”

The trace files usually have the following filenames:

- Trace.d0
- Trace.d1
- Trace.d2
- Trace.d3
- Trace.d4
- Arc-<DateTimeStamp> (for archived trace files)

Archived Vault traces files can be found in the “Archive” folder (a subfolder of the “Logs” folder).
Example archived trace filename: Arc-20191216-085206.log.

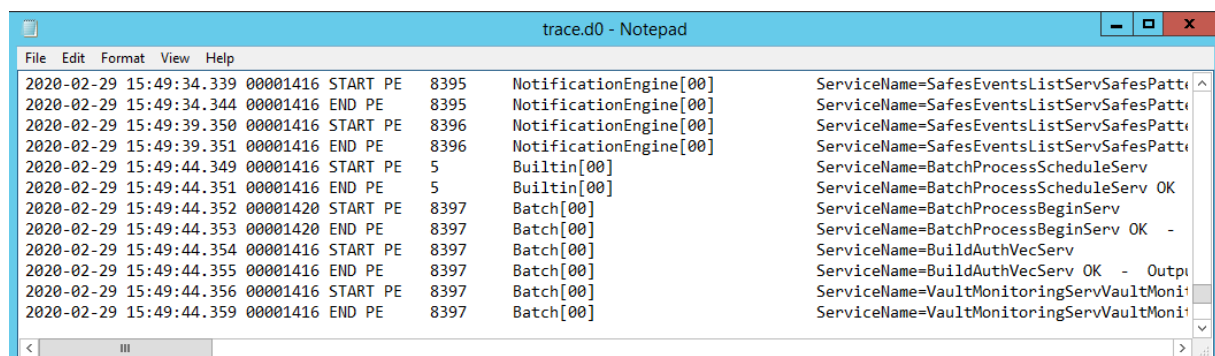
Logic container trace files are not supported and usually end with (“.LC.log”) in their filename.

I have added Vault trace files to the tool but they are not getting recognized, what can I do?

Please check if the trace files have been generated with a Vault debug setting that includes

PE(1),PERF(1,2)

Supported trace files are structured like in the following example:

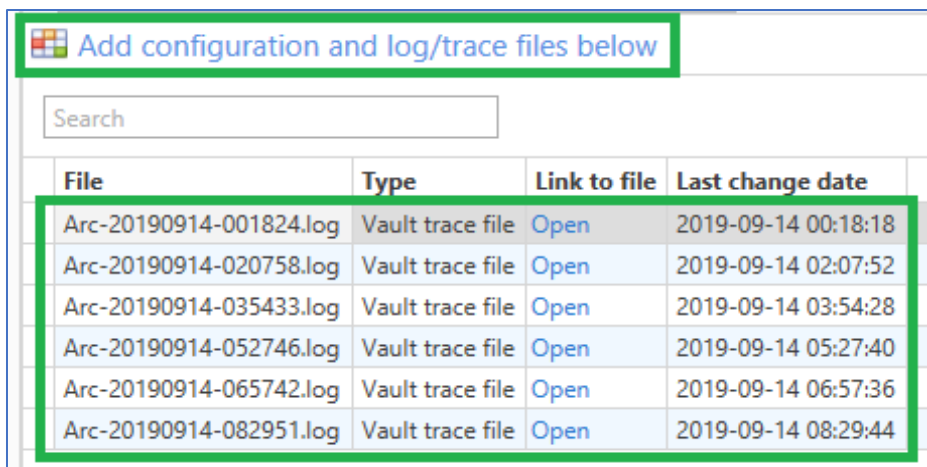


Can I retrieve Vault trace files via PACLI or EVD?

There is no out-of-the box capability for retrieving Vault trace files via PACLI or EVD from the Vault.
Please also see “Where can I find the Vault trace files which can be processed with this tool?” for further information.

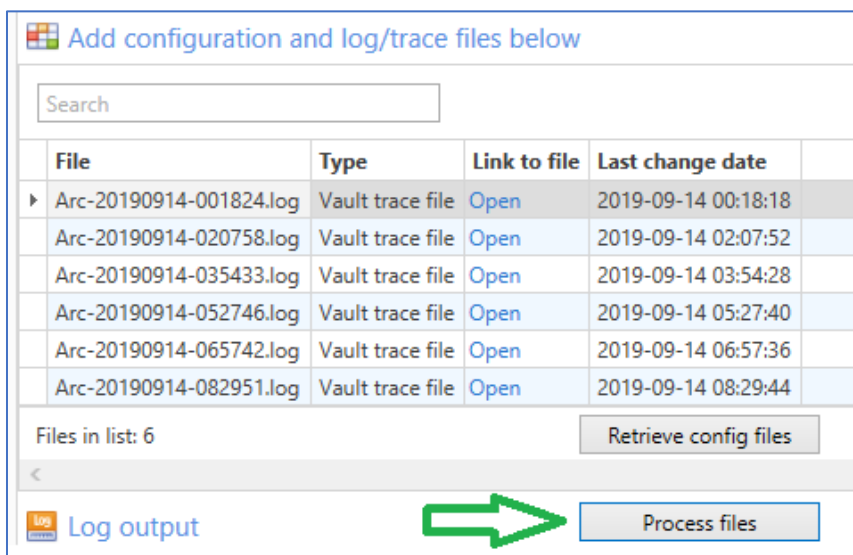
Where can I add Vault trace files to the tool?

The Vault trace file can be added to the grid to which configuration and log files can be added:



File	Type	Link to file	Last change date
Arc-20190914-001824.log	Vault trace file	Open	2019-09-14 00:18:18
Arc-20190914-020758.log	Vault trace file	Open	2019-09-14 02:07:52
Arc-20190914-035433.log	Vault trace file	Open	2019-09-14 03:54:28
Arc-20190914-052746.log	Vault trace file	Open	2019-09-14 05:27:40
Arc-20190914-065742.log	Vault trace file	Open	2019-09-14 06:57:36
Arc-20190914-082951.log	Vault trace file	Open	2019-09-14 08:29:44

Once valid trace files were added, the files can be processed by clicking on “Process Files”:



Search

File	Type	Link to file	Last change date
▶ Arc-20190914-001824.log	Vault trace file	Open	2019-09-14 00:18:18
Arc-20190914-020758.log	Vault trace file	Open	2019-09-14 02:07:52
Arc-20190914-035433.log	Vault trace file	Open	2019-09-14 03:54:28
Arc-20190914-052746.log	Vault trace file	Open	2019-09-14 05:27:40
Arc-20190914-065742.log	Vault trace file	Open	2019-09-14 06:57:36
Arc-20190914-082951.log	Vault trace file	Open	2019-09-14 08:29:44

Files in list: 6 [Retrieve config files](#)

 Log output [Process files](#)

Where is the data from the “Transaction Management” section stored?

The data from the Transaction Management section is stored in the SQLite database file “VaultTraces.db” in the data folder of the tool.

Why is the data from “Transaction Management” section stored in a separate SQLite database file?

This is mainly due to technical reasons, in particular because of performance considerations. There can be millions of Vault transactions and storing those in a dedicated database file comes with some benefits that improve the performance and UI responsiveness.

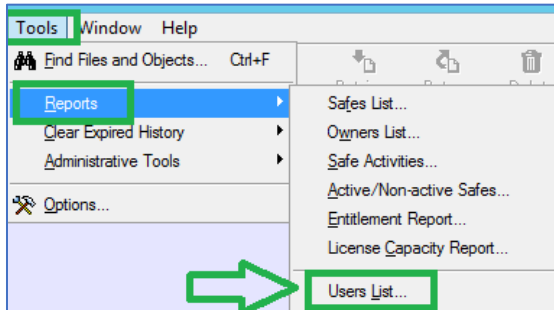
How can I delete the data from the “Transaction Management” section?

You can simply delete the “VaultTraces.db” SQLite database file in the data folder of the tool.

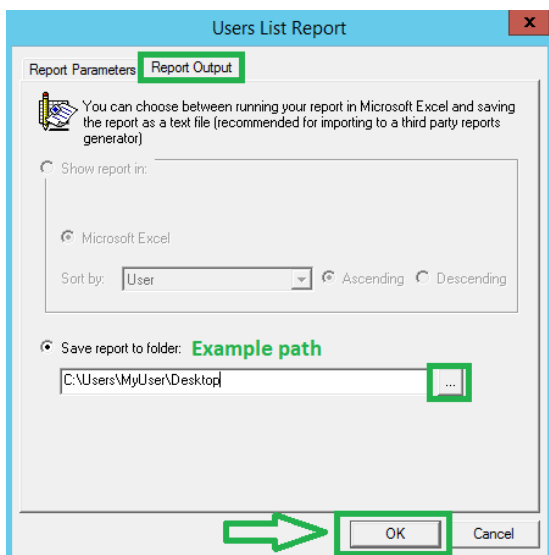
How can I get the user list export (non-EVD) which I can use as an option for the user type determination for Vault transactions (transaction management section)?

You can create the user list export (non-EVD) using the PrivateArk Client.

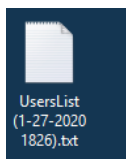
➔ Select “Users List”



➔ Select “Report Output” tab and choose an export folder



Created users list output file (example):



Add the file to the tool along with Vault trace files:

Add configuration and log files below			
Search			
File	Type	Link to file	Last change date
UsersList (1-27-2020 1826).txt	User list (non-EVD)	Open	2020-01-27 03:33:39
Arc-20200113-042728.log	Vault trace file	Open	2020-01-13 04:27:22
Arc-20200113-055039.log	Vault trace file	Open	2020-01-13 05:50:32
Arc-20200113-070630.log	Vault trace file	Open	2020-01-13 07:06:24
Arc-20200113-080418.log	Vault trace file	Open	2020-01-13 08:04:12

How are the user types determined in the Vault transaction section?

The user types in the Vault transaction management section are determined based on the user type detection regex settings that can be configuration in the tool.

If the EVD users export or the non-EVD user list (from the PrivateArk client) have been processed with the tool, the user types will be determined from the EVD users export or the non-EVD user list data in the first step and in the second step through the regular expression settings if the user type could not be determined from the EVD users export or user list data.

If both, the EVD users export as well as the non-EVD user list (from the PrivateArk client) were added to the tool, the non-EVD user list takes precedence over the EVD users export.

Can I use the users list export (non-EVD) for generating the license capacity report?

The license capacity report in the tool cannot be generated with the non-EVD users list export from the PrivateArk client.

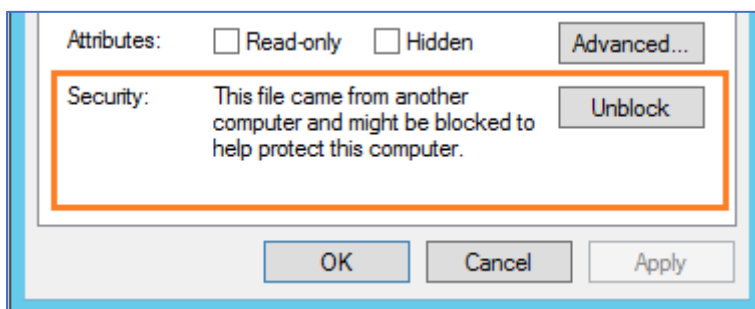
The main reason is that the non-EVD users list export from the PrivateArk client does not contain the user type IDs of the users. These user type IDs are matched against the user type IDs in the License.xml file which is a more accurate approach for determining the license consumption.

The user type IDs are included in the **EVD users list export** but not in the non-EVD users list export from the PrivateArk client.

Please also see “Which information is needed in order to create the license capacity report?” for further information.

After downloading or copying the tool I cannot start the “PAS Reporter.exe” file. I have double-clicked the executable but nothing appears to happen. In the Windows event logs, I am seeing errors such as “[...] App failed with error: This app can't be activated by the Built-in Administrator. See the Microsoft-Windows-TWinUI/Operational log for additional information [...]”. What can I do about that?

You can check if the “PAS Reporter.exe” is blocked.



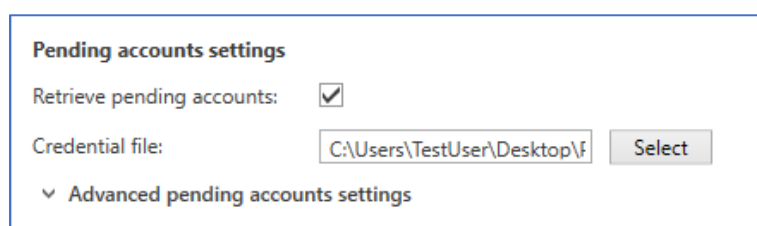
Please always make sure that downloaded and copied files are scanned with an AV solution and reach out to your administrator and security team regarding security matters.

When trying to retrieve files via PACLI from the System safe, the following error occurs: “Error: ITATS044E You are unauthorized to store object in Safe System.” What can I do?

Depending on the CyberArk PAS version and other possible factors, it can be that the “Update Files” permission will be required in addition to the “List Files” and “Retrieve Files” permissions in order to retrieve files from the System safe.

How does the tool generate the pending accounts report?

Since the pending accounts information is not in the EVD data, the tool retrieves the pending accounts information via PACLI. You can configure the tool to retrieve the pending accounts information in the settings.



Pending accounts settings

Retrieve pending accounts: ☒

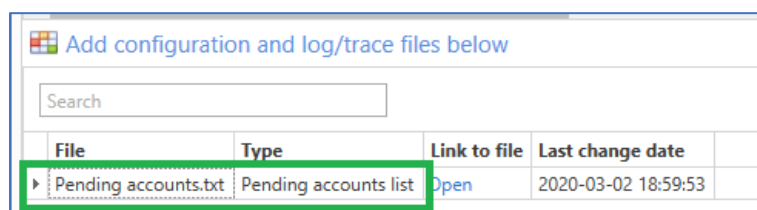
Credential file:

▼ Advanced pending accounts settings

Do I need to run the tool using the integrated mode to generate the pending accounts report?

The pending accounts report can be generated via the integrated mode as well as via the manual mode. For the manual mode, you can run a script to generate the pending accounts list. You can then drag and drop the retrieved pending accounts list into the tool and process the data to generate the pending accounts report.

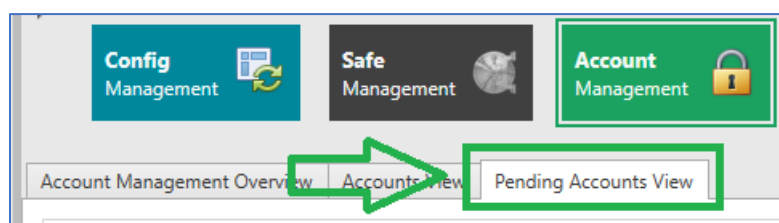
You can find a script to retrieve then pending accounts list in the “evd” folder of the tool (script name: “02 Retrieve configuration files.cmd”).



File	Type	Link to file	Last change date
▶ Pending accounts.txt	Pending accounts list	Open	2020-03-02 18:59:53

Where can I find the pending accounts report in the tool?

The pending accounts report can be found in the “Account Management” section in the “Pending Accounts View” tab:



How can I use the REST API integration of the tool?

In order to use the REST API, the URL of the PVWA or load balancer URL can be configured in the “REST API Settings” section of the tool.

The screenshot shows the 'Settings and Help' window with the 'REST API Settings' tab selected. The 'Connection settings' section includes a text box for 'PVWA address' containing 'https://PVWAorLoadBalancerAddress'. The 'Authentication settings' section includes a dropdown for 'Authentication method' set to 'CyberArk', a 'Save & test CyberArk authentication (automated)' button, and options for 'Concurrent connection' (1), 'Skip SSL certificate check' (No), and 'Use client certificate' (Specify thumbprint). The 'Automate authentication' checkbox is checked. Below these are fields for 'EPV / LDAP user' (ReportingUser), 'Credentials retrieval' (Use CP), 'Folder name' (Root), 'Safe name' (VaultUser), 'Object name' (UserAccount), 'Retrieval reason' (PAS Reporter automation), and 'Application ID' (PAS_Reporter). A 'Test credentials retrieval via CP' button is at the bottom. On the right, a text box explains the REST API integration, and a list of checkboxes for component versions and policies are all checked. At the bottom right, there are 'Load defaults' and 'Save' buttons.

All authentication methods that are currently available via REST API can be used.

If the PAS Reporter is run automatically (e. g. via a scheduled task), it can be an idea to automate the authentication via REST API through retrieving the user’s credentials via AAM or PACLI.

Please note, that for some authentication methods (e. g. RADIUS), non-interactive authentication is not possible. These authentication methods are not supported for the automated mode.

If interactive authentication is required, the tool will automatically show an according authentication dialog.

The screenshot shows a dialog box titled 'RADIUS authentication (REST API)'. It contains a text box for the username 'ReportingUser' and a password field with a masked password (dots) and a toggle icon. At the bottom, there are 'Cancel' and 'Sign in' buttons.

Figure 18: REST API authentication dialog

How can I automatically send reports via email?

In order to automatically send reports via email, the SMTP settings can be configured in the “Report Settings” section of the tool.

Settings and Help

General Settings | REST API Settings | **Report Settings** | Transaction Analysis Settings | SQL Export Settings | CSV Export Settings | Help

Report cover page settings

Add company name: ☒ CyberArk

Add environment name: ☒ Example environment

Add logo to cover: ☒ Default ☐ Custom ☐ No logo

Obfuscation settings:

Email SMTP settings

SMTP server address:

SMTP server port: Enable TLS: ☒ Check certificate: ☐

Sender email address:

Sender display name:

SMTP authentication: ☒ Yes ☐ No

SMTP username:

Credentials retrieval: ☒ Use CP ☐ Use CCP ☐ Use PACLI

Folder name:

Safe name:

Object name:

Retrieval reason:

Application ID:

Email report settings

Send reports via email: ☒ No ☐ Yes ☐ Only when tool is run in auto-mode

Detailed logging: ☒

ID	Email job name	Format	Edit / Process
0	Test	DOCX	Edit / Process

Report export settings

Auto export reports: ☒ No ☐ Yes ☐ Only when tool is run in auto-mode

Export report filename: ☐ Add report creation-datetime to export filename

☒ Prepend datetime ☐ Append datetime

Use subfolders: ☐ Export report to folder with report name as folder name

ID	Export folder	Format	Edit / Process
No report export jobs are defined. Please use the "Add export job" button for adding report export jobs.			

If SMTP authentication is required, the authentication can be automated via credentials retrieval via AAM or PACLI.

Furthermore, the sending of emails can be tested via the “Save & send test email” button.

Send test email

To:

Subject:

Dear recipient,

this is a test email for testing the email integration of the PAS Reporter tool.

Thank you very much

Manual authentication is only supported for sending test emails (not for email jobs)

Once the SMTP settings were configured and tested successfully, email jobs can be added via the “Add email job” button.

Email report settings

Send reports via email: ☐ No ☒ Yes ☐ Only when tool is run in auto-mode

Detailed logging: ☒

ID	Email job name	Format	Edit / Process

Please use the "Add email job" button to add a new email job.

Add email report job

- Email jobs are only processed when the tool is running AND new data was processed with the tool. The jobs are then executed at the end of the data processing procedure.
- The processing of an email job can be limited to specific weekdays and to only once per day. For instance if the tool is run via a scheduled task each day but the specified report should only be sent on a specific weekday. Or if the report is generated several times per day but should only be sent once per day.

Job name: Example email job

Report: Environment report

Format: PDF

To: test@myexamplemailserver.com

CC: Specify CC recipients for the email job. Multiple recipients can be separated with semicolon.

BCC: Specify BCC recipients for the email job. Multiple recipients can be separated with semicolon.

Weekdays: ☒ Mon ☒ Tues ☒ Wed ☒ Thurs ☒ Fri ☒ Sat ☒ Sun

☐ Send only once per day

Cancel Add email job

In the email job the report can be chose, the file format (PDF, DOCX, XLSX, HTML), and the desired recipients.

Furthermore, the email job can be configured to be sent only on specific weekdays and only once per day. After the configuration, the report will be added to the email jobs list.

Email report settings

Send reports via email: ☐ No ☒ Yes ☐ Only when tool is run in auto-mode

Detailed logging: ☒

ID	Email job name	Format	Edit / Process
0	Example email job	PDF	Edit / Process

Add email job Remove email job Email template