CIS-CAT Pro Assessor: Palo Alto Extraction Guide Tip Sheet

CIS-CAT Pro Assessor

December 2023

mastercard

Revision history

Revision #	Date	Changes made	Performed by	Authorized by
1.0	Dec 2023	Template Update	Adi Kogan	Adi Kogan
1.1	Jan 2024	Wording Update	Berkay Gur	Juan Carlos Vargas

Table of content

1. Tool Description

CIS-CAT Pro Assessor is a Java-based tool that scans a target system's configuration settings and reports the system's compliance to the corresponding CIS Benchmark. The results generated are only presented in machine-readable format.

2. Licensing Requirements

The CIS-CAT Pro Assessor is available for download through Mastercard's resources. For the complete download and installation guide please refer to the "CIS-CAT Pro Assessor: Extraction Guide Tip Sheet".

The CIS-CAT Pro Assessor tool must be deleted once the configuration files export is completed.

3. Who Should Use the Document

This document is for "Cyber Quant CyMA" users participating in an organizational cyber risk and security assessment using Mastercard's "Cyber Quant Cyber Risk Quantification" platform.
The document is also targeted at experienced IT and cyber professionals who will extract "Palo Alto Next-Generation Firewall" configuration files for the "Cyber Quant CyMA" cyber risk and security assessment.

4. Requirements & permissions

- Palo Alto Next-Generation Firewall device requirements:
    - Web access to the Palo Alto device.
    - Save and export configuration privileges.
- CIS Tool Requirements:
    - Machine Requirements -
        - Windows server or client OS (it cannot be executed on a Linux machine).

- CIS-CAT Pro Assessor requires a Java Runtime Environment (JRE) at or above version 1.8.

- Access Requirements -
  - Administrative permissions to execute the CIS-CAT Pro Assessor.
  - Administrative permissions to connect to the organizational technological assets.

5. High level process flow

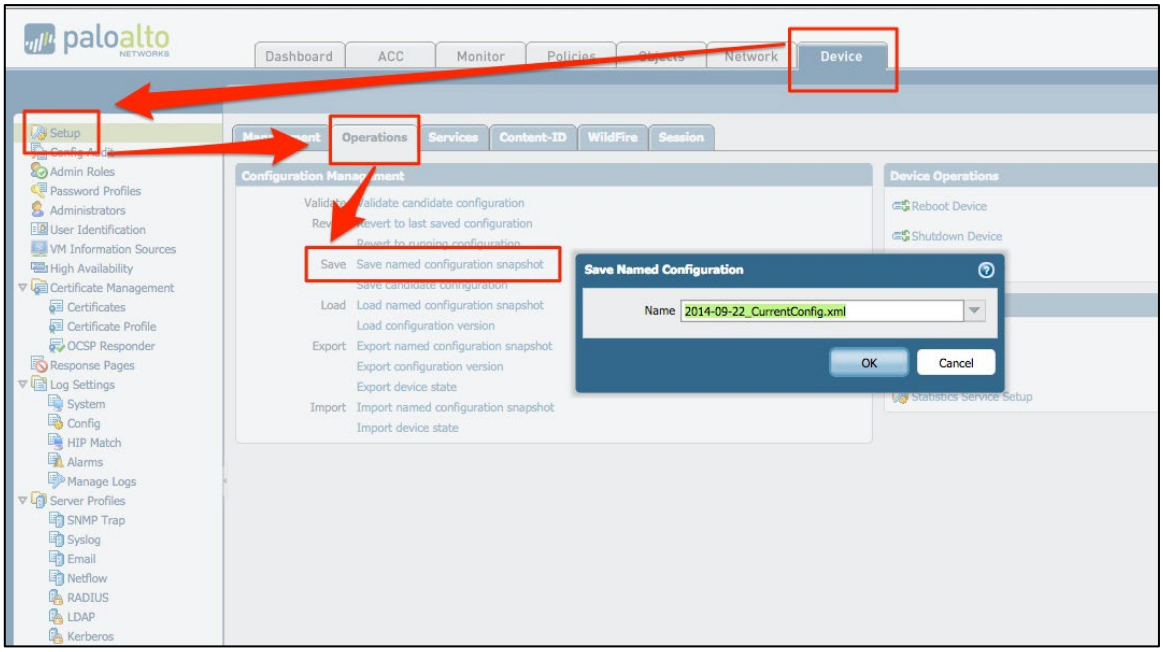
Access the "Palo Alto Next-Generation Firewall" and export the current configuration snapshot file.

Import the extracted file into the "CIS-CAT Pro Assessor" tool for analysis and to generate an XML report.

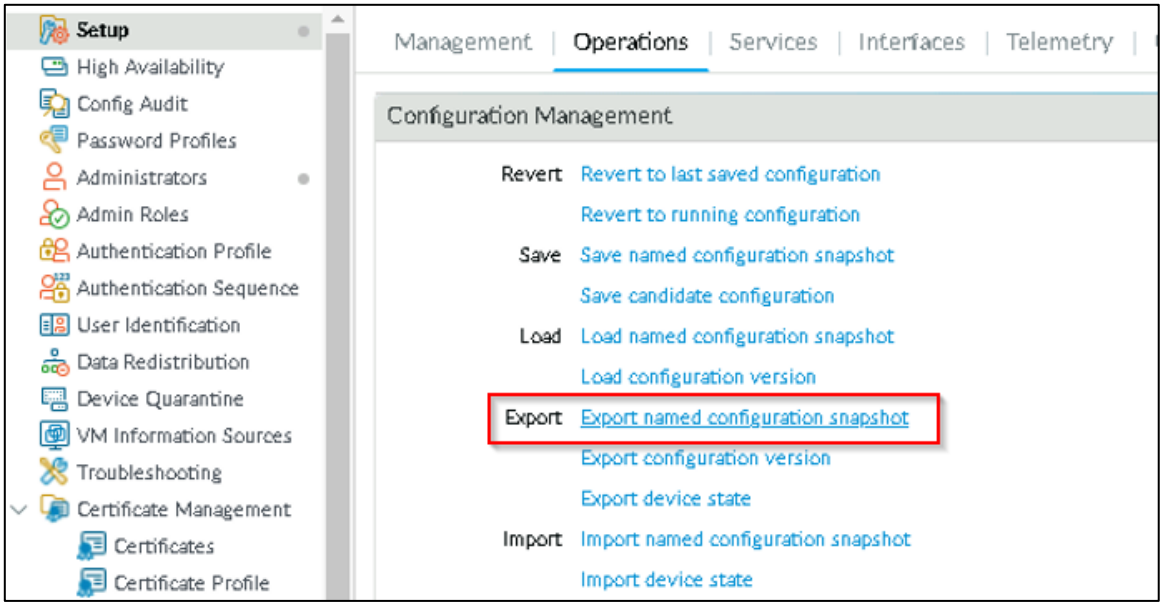
Import the generated XML report into the "CyMA" client for analysis.

6. Export Palo Alto Configuration File

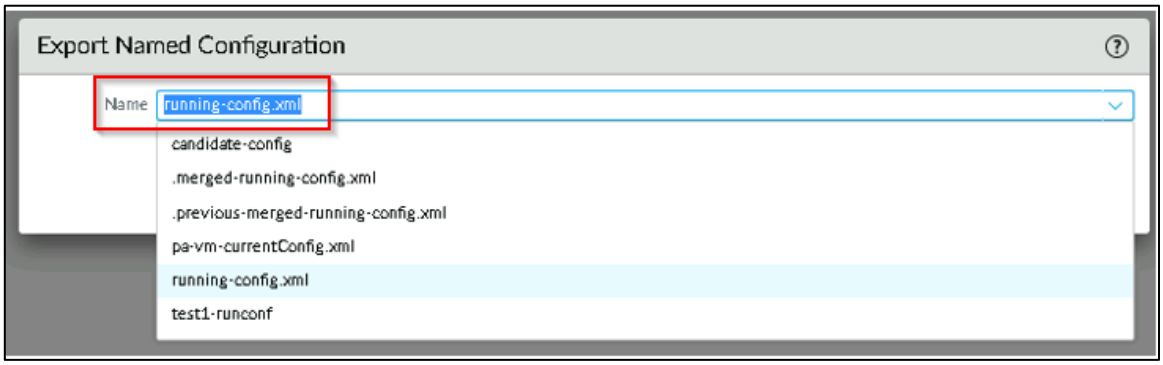
1. Using a web browser, login into the "Palo Alto Next-Generation Firewall" web management portal.
2. Navigate to Device → Setup → Operations and select "Save named configuration snapshot."
3. Name the snapshot with the extension **.xml** and click "OK". It is recommended to use a name with identifiers related to the firewall from which the configuration was exported.



4. To export the created snapshot, click on “Export named configuration snapshot".

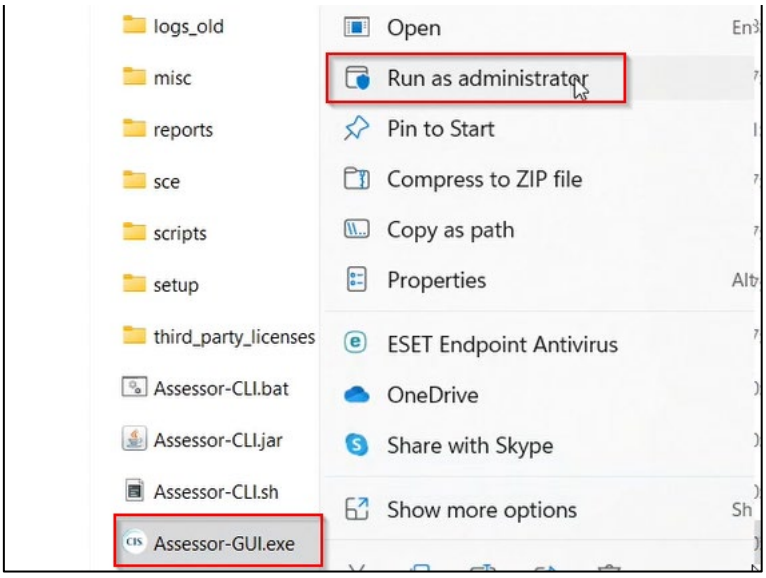


5. Select the snapshot name from step 3 and click “OK” to download it.

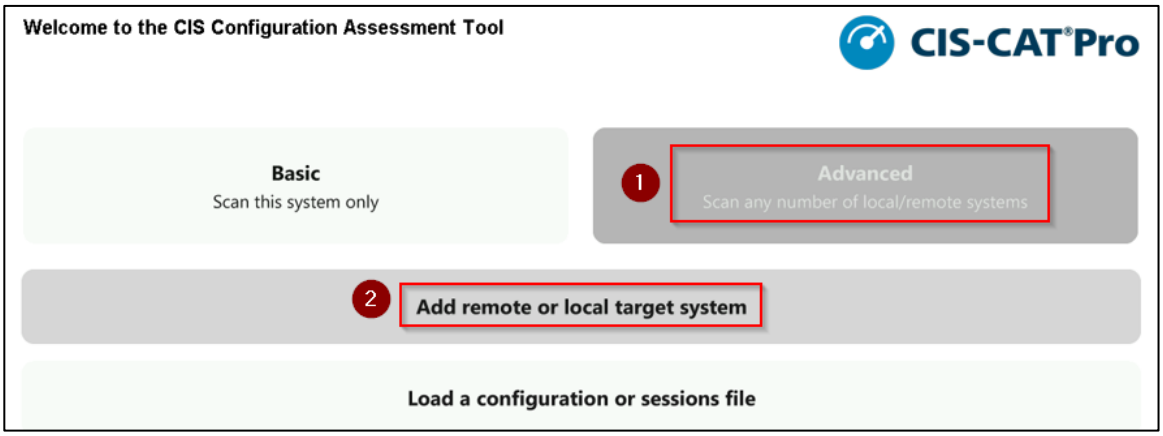


7. Configuration File Analysis

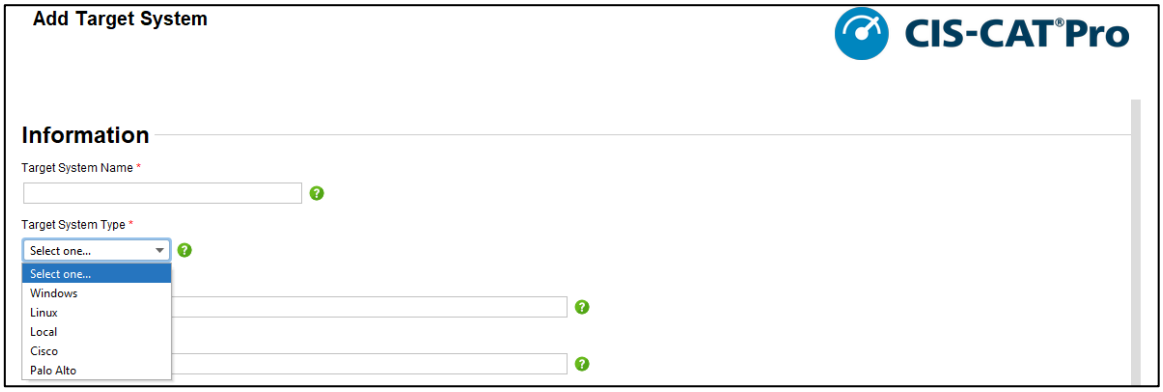
1. Start the "CIS-CAT Pro Assessor" tool as administrator and accept the user account control dialog box (proceed normally if it does not appear), it may require administrative credentials.



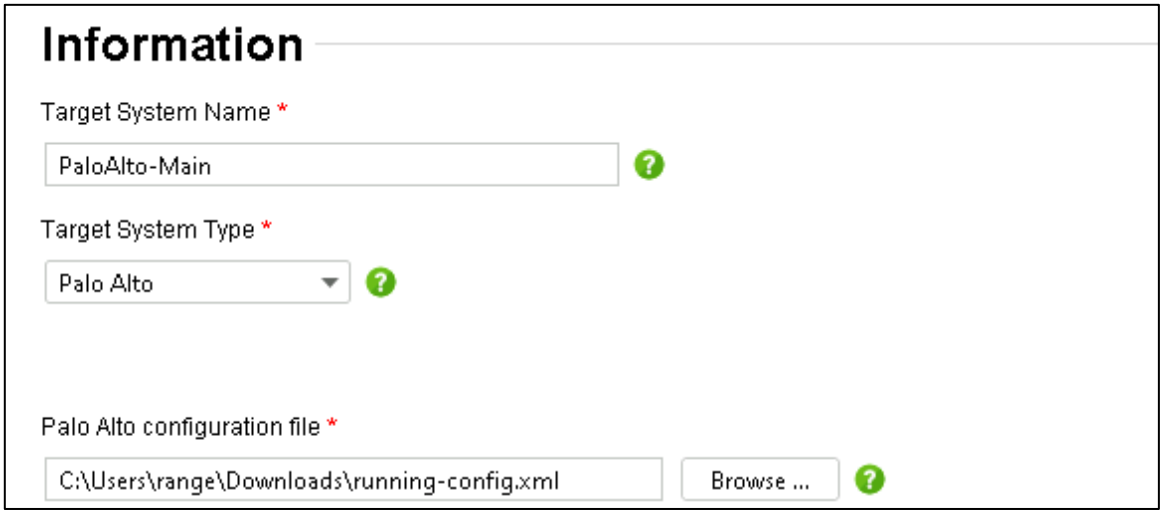
2. Click on "Advanced" and then on "Add remote or local target system." Several target systems can be added at the same time, each one requires discrete addresses and credentials to retrieve the benchmarks and profiles.



3. Select the system type "Palo Alto".

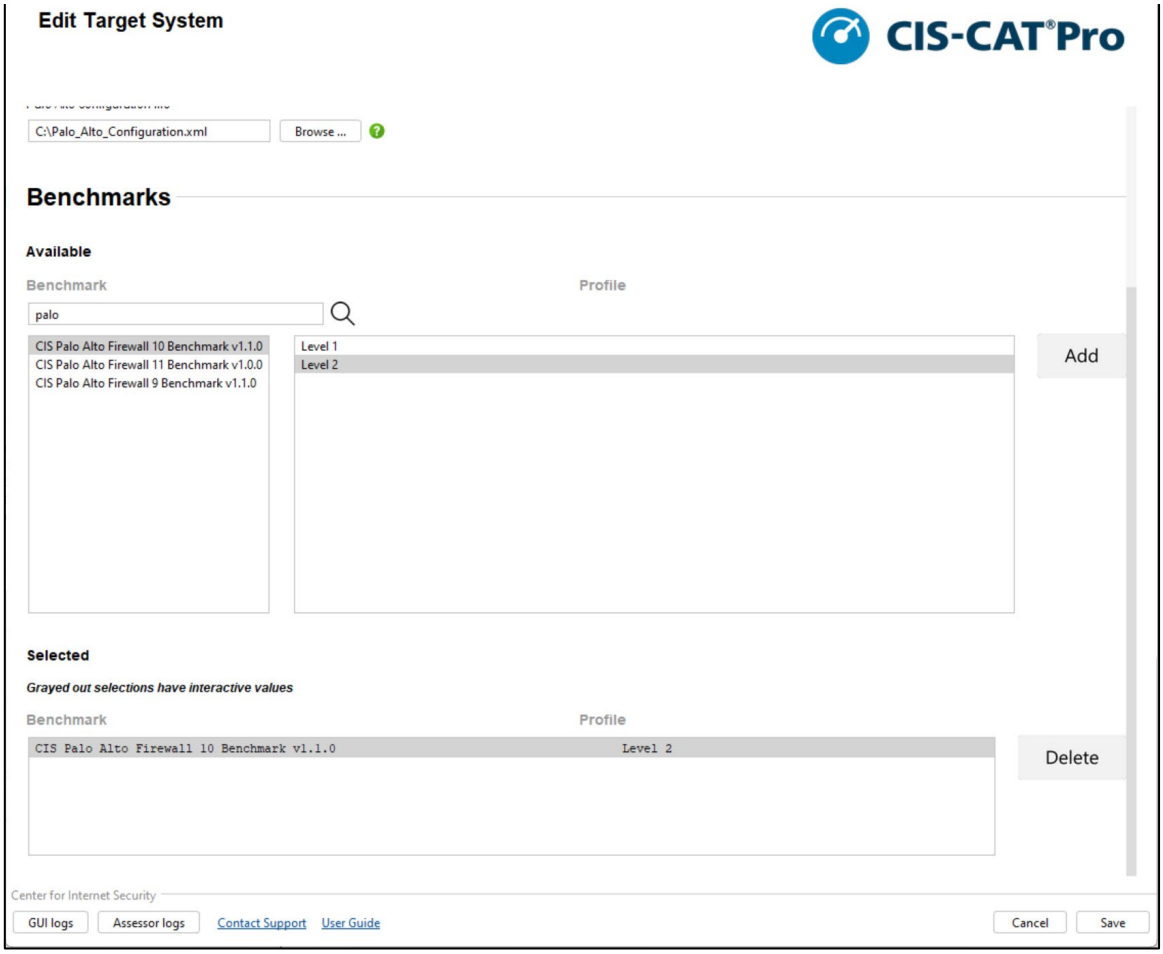


4. Fill in the Target System Name and click on browse to find the Palo Alto configuration file.

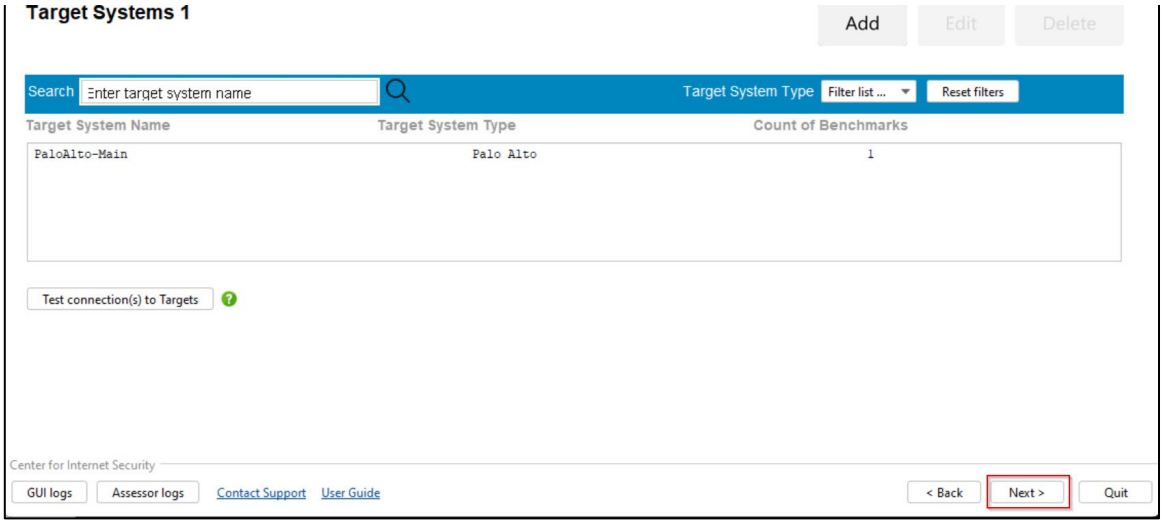


5. Select the desired "Palo Alto Next-Generation Firewall" version device, the CIS assessment level, and click "Add".

6. In the "Selected" section, delete any other benchmarks if exist and keep only the "CIS Palo Alto Firewall" benchmark, click on "Save".

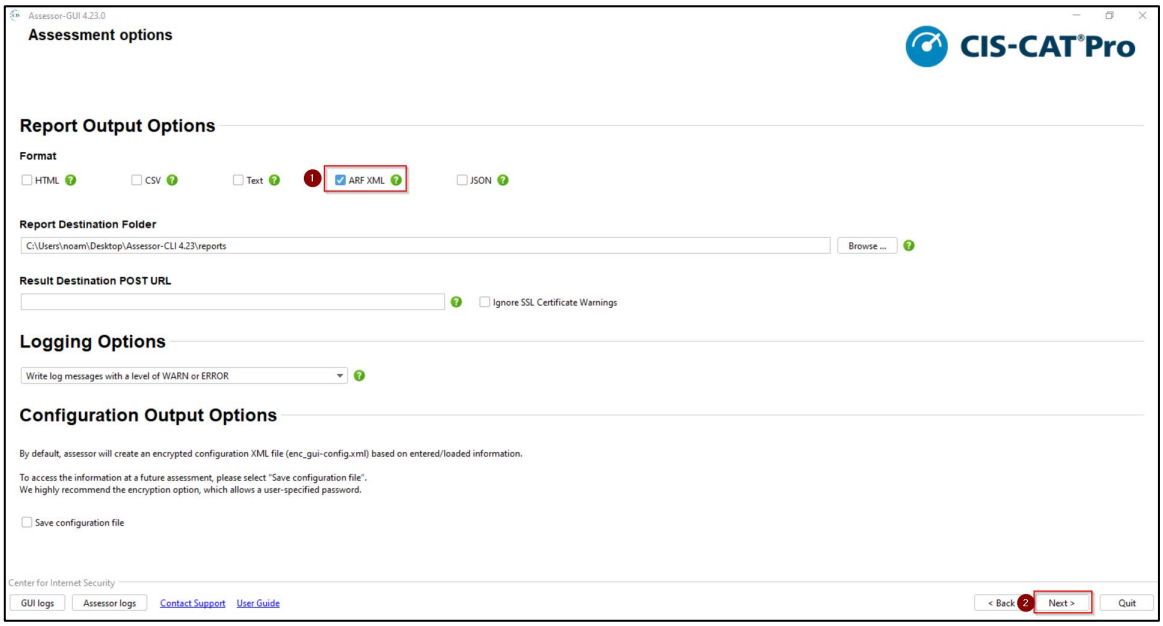


7. Click on "Next" on the test connection page.

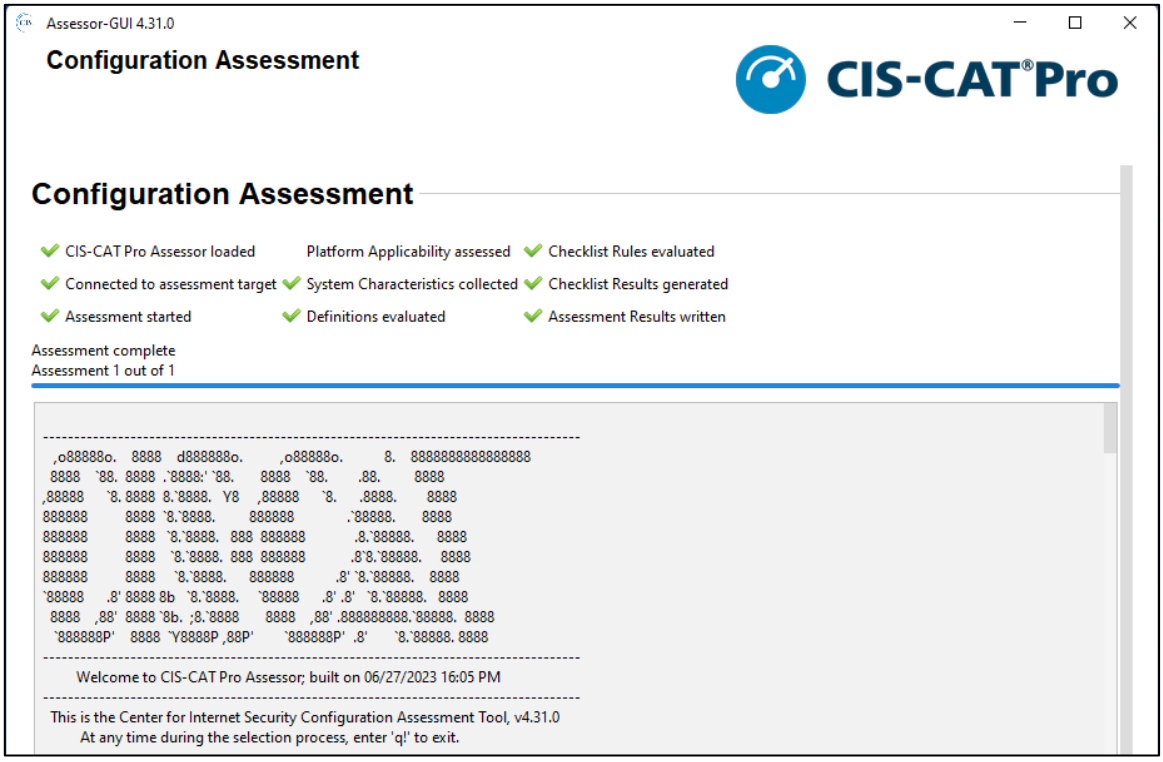


8. Select the "ARF XML" format (this is the only format supported by "CyMA") and the destination to save the report into and click "Next." In addition, an "HTML" format can also be selected to generate a human-friendly report. **It is recommended to store it in the default "C:\Assessor-CLI\reports" to avoid long paths that may cause errors.**

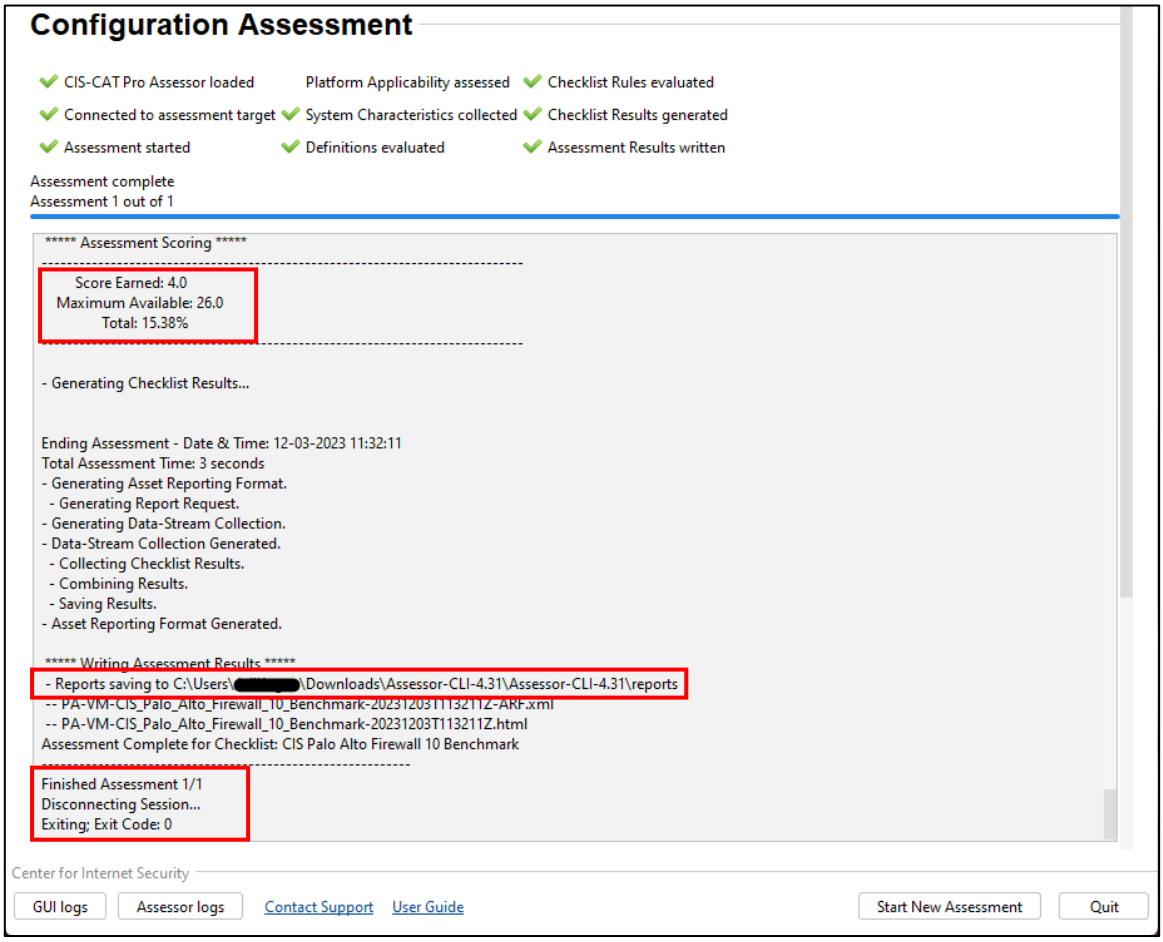
   When the "Confirmation" box appears, click on "Start Assessment".



9. The assessment may take several minutes to execute while displaying its progress.



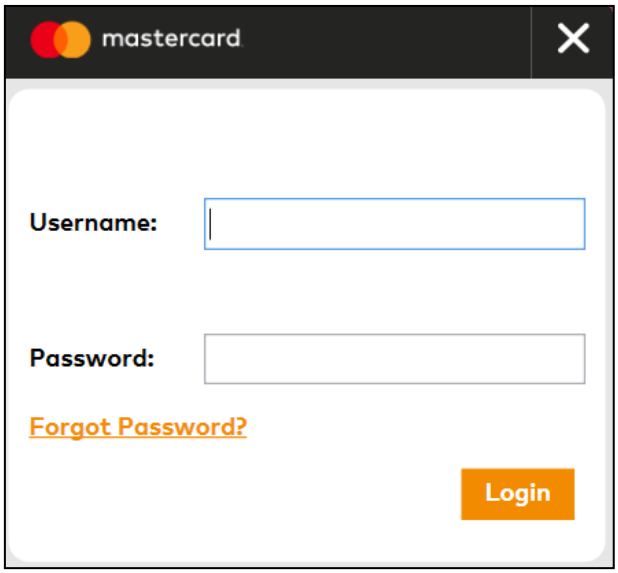
10. Once the assessment finishes, it displays information such as a score, the location of the generated reports, and whether it was successful or not. An exit code of 0 indicates a successful execution, while 1 indicates an error.



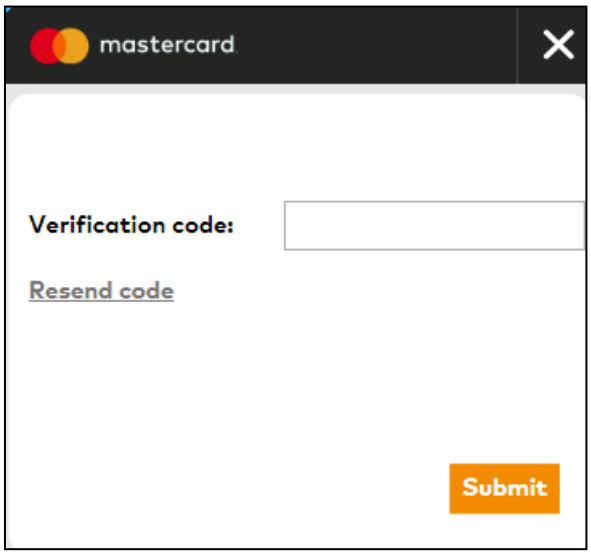
11. Click on “Quit” after a successful assessment to close the too.

8. Open and Review Integration Results

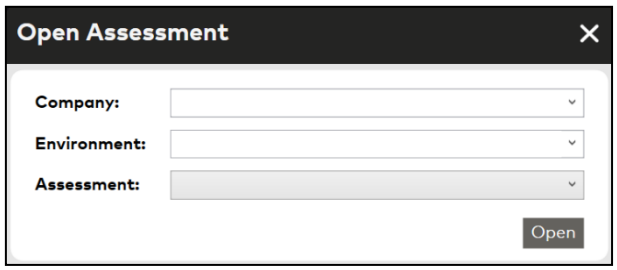
1. Execute the "Cyber Quant CyMA" client and log in.



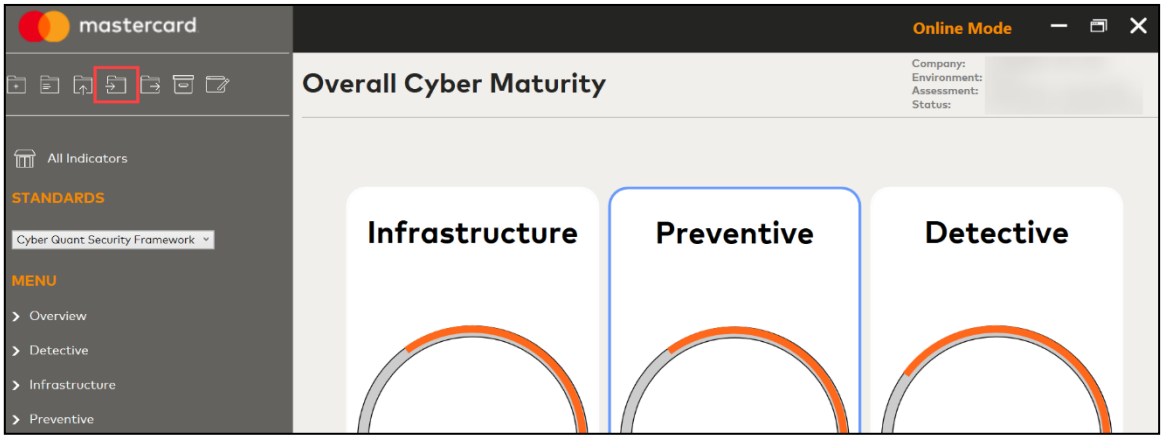
2. Enter the verification code sent to the account's email address.



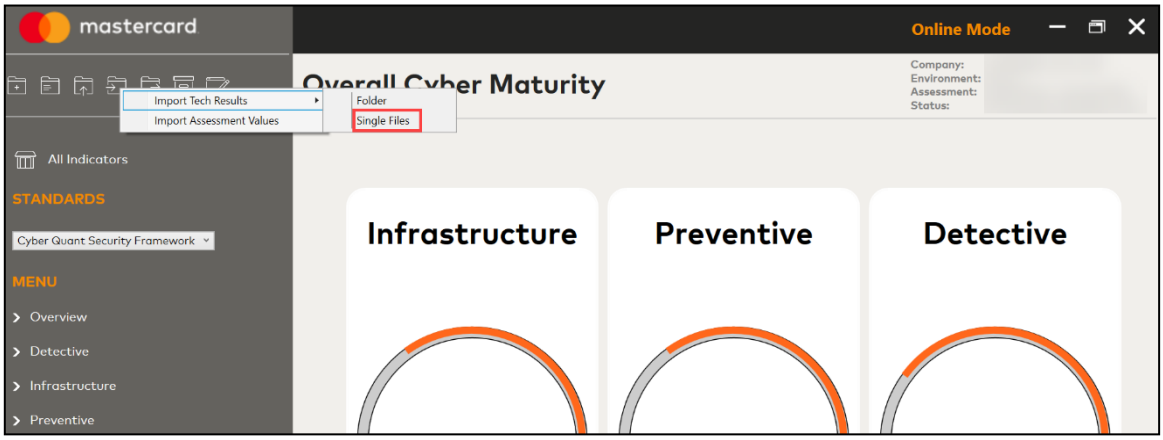
3. Select the desired company, environment, and assessment to import the report.



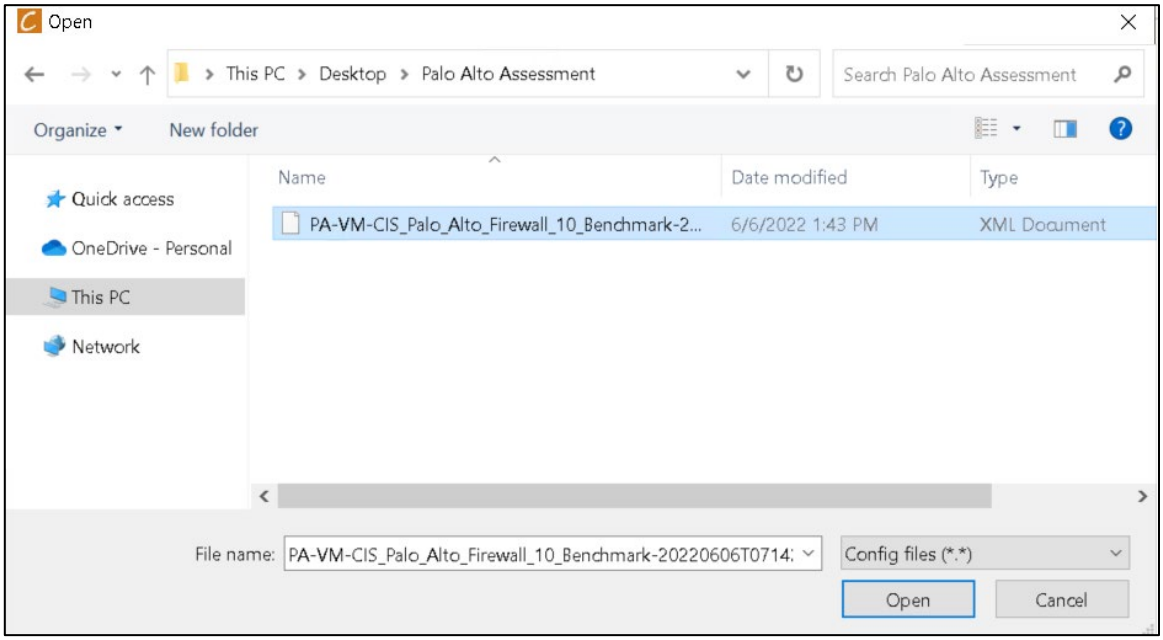
4. Click on the "Import Files" icon on the top left of the screen.



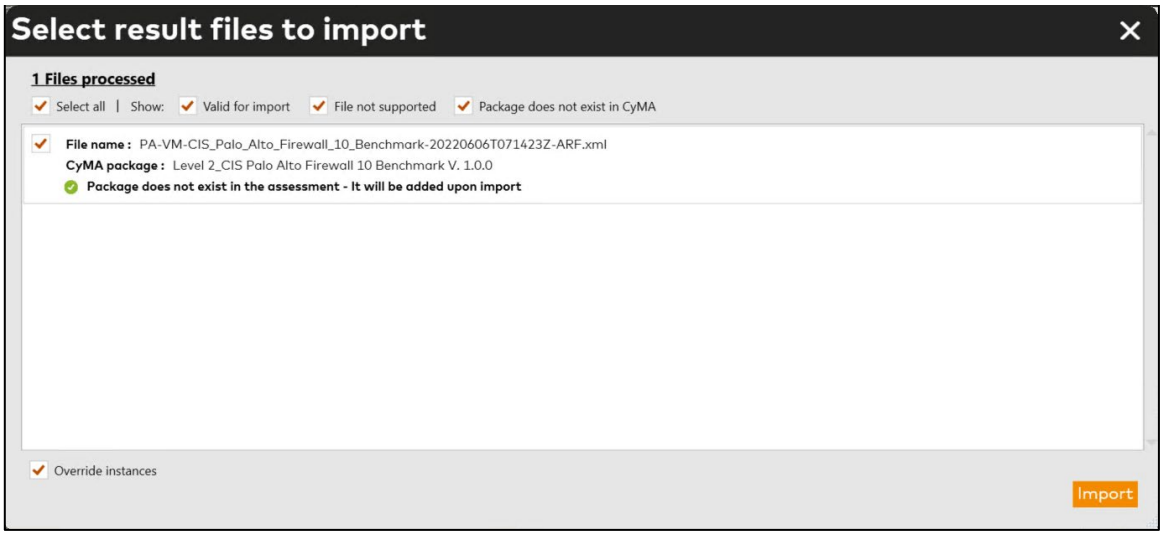
5. Hover over "Import Tech Results", click "Choose Single File".



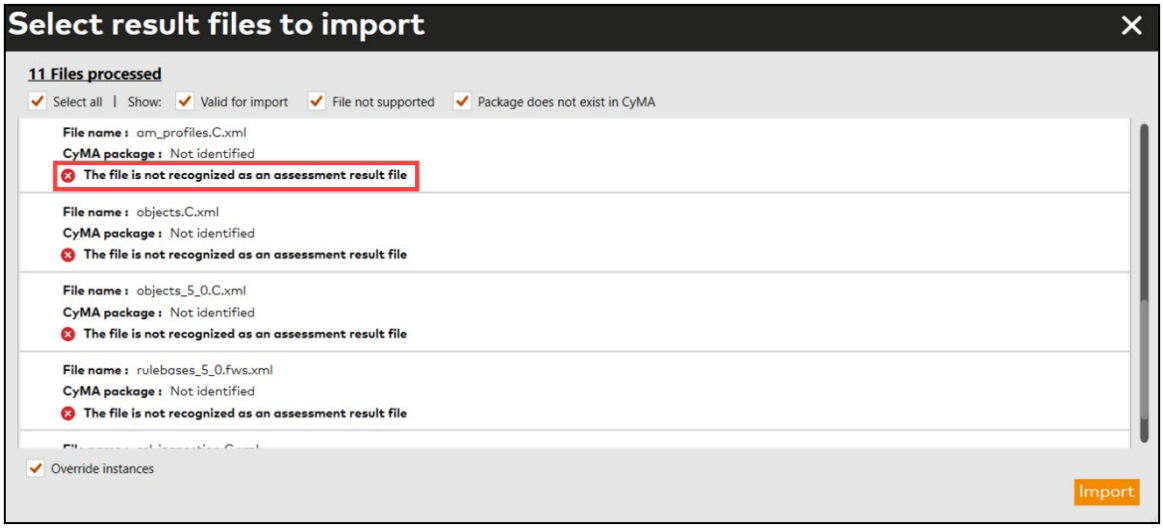
6. Browse to the dedicated folder where the configuration files are stored:



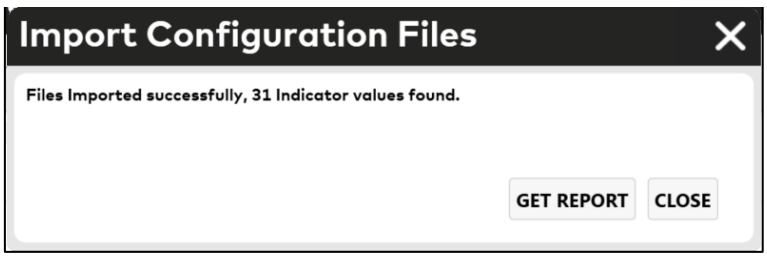
7. Once the report is open, select the file and click "Import". The following screen displays information regarding import errors and packages associated with the imported files.



A red mark is displayed below the package in case of an error.



8. Upon successful import, a confirmation notice is displayed, click "CLOSE". **Please note that the number of indicators may vary based on the input configuration files**.



9. The assessment results are now available for review.