

CIS Assessor: Local Cisco Switch Extraction Guide Tip Sheet

CIS-CAT Pro Assessor for Cisco Switch

March 2026





Table of content

1. Tool Description.....	3
2. Licensing Requirements.....	3
3. Who Should Use the Document.....	3
4. Requirements & Permissions	3
5. High Level Process Flow	4
6. The Extraction Process	4
7. Open and Review Integration Results on CyMA	9
8. Review Integration Results on CyMA Web.....	12



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 and processing 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 Cisco Switch devices configuration files for the "Cyber Quant CyMA" cyber risk and security assessment.

4. Requirements & Permissions

- Cisco device requirements:
 - Supported Cisco OS devices
 - Cisco NX-OS, Extreme Networks.
 - Cisco IOS XR.
 - Cisco IOS XE 16 & Cisco IOS XE 17.
 - SSH access to the Cisco device.
 - Admin 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

Log in via SSH to the Cisco Switch device desired for the analysis and export the tech-support file into the machine with the CIS CAT Pro Assessor installed.

Import the extracted file into the CIS CAT Pro Assessor tool and generate an XML report.

Import the XML report into "CyMA" and review the results.

6. The Extraction Process

1. Connect via SSH to the desired Cisco Switch device.
2. Execute the following command to create a local configuration file with the device's configuration.

1. For Cisco device:

```
configure terminal
terminal length 0
show running-configuration | redirect flash:/cisco_switch.txt

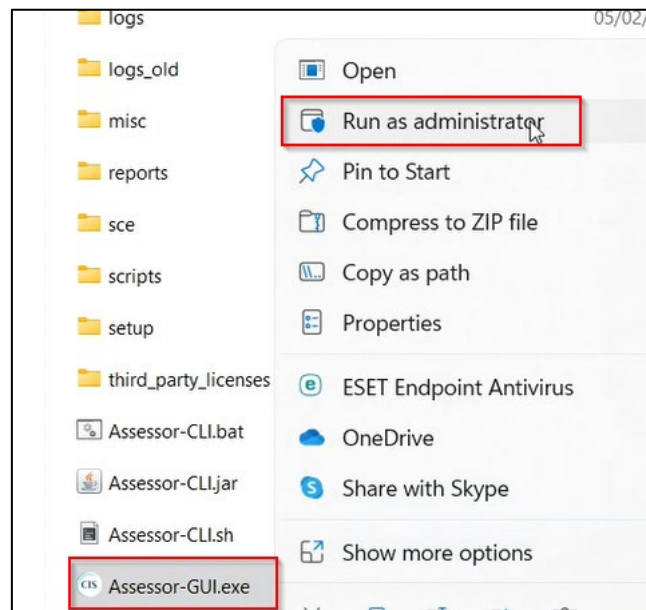
configure terminal
terminal length 24
```

2. For Extreme Networks device:

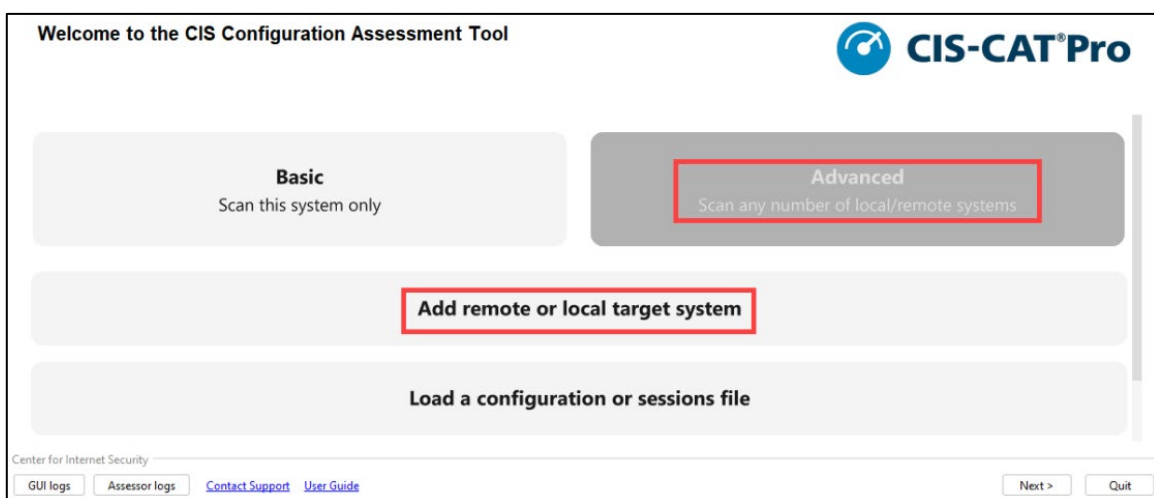
```
Extreme: disable clipaging
copy configuration flash:/extreme_sw.txt
```



3. Transfer the configuration file to a computer with the CIS-CAT Pro Assessor installed.
4. Start the CIS-CAT Pro Assessor as administrator and accept the user account control dialog box (proceed normally if it does not appear); it may require administrative credentials.



5. Click on "Advanced" and then on "Add remote or local target system." Several target systems can be added at the same time; each will require discrete addresses and credentials to retrieve the benchmarks and profiles.





6. Select target System type as "Network Device Txt".

The screenshot shows the 'Add Target System' interface in CIS-CAT Pro. Under the 'Information' section, the 'Target System Name' field is empty. The 'Target System Type' dropdown menu is open, displaying a list of options: 'Select one...', 'Windows', 'Linux', 'Local', 'Network Device XML', and 'Network Device Txt'. The 'Network Device Txt' option is currently selected. There are green question mark icons next to the input fields.

7. Fill in the Target System Name and click on browse to find the Cisco configuration file.

The screenshot shows the 'Add Target System' interface in CIS-CAT Pro. The 'Target System Name' field is now filled with text. The 'Target System Type' dropdown menu is set to 'Network Device Txt'. Below this, the 'Network Device Configuration File (.txt)' field is empty, and a 'Browse...' button is visible next to it. Green question mark icons are present next to the input fields.

8. Once the configuration file is uploaded, the screen will change, then select the desired Cisco Switch version device, the CIS assessment level, and click "Add".



Add Target System

Information

Target System Name *
Cisco_Switch

Target System Type *
Network Device Txt

Network Device Configuration File (.bt) *
C:\Cisco_Switch.txt

Benchmarks

Available

Benchmark	Profile
Cisco	
CIS Cisco IOS XE 16.x Benchmark v2.2.0	Level 1
CIS Cisco IOS XE 17.x Benchmark v2.2.1	Level 2
CIS Cisco IOS XR 7.x v1.0.1	
CIS Cisco NX-OS Benchmark v1.2.0	

Selected

Benchmark	Profile
-----------	---------

Center for Internet Security
GUI logs | Assessor logs | Contact Support | User Guide

Cancel | Save

9. In the "Selected" section, delete any other benchmarks if they exist and keep only the CIS Cisco Switch benchmark. Finally, click on "Save".

Selected

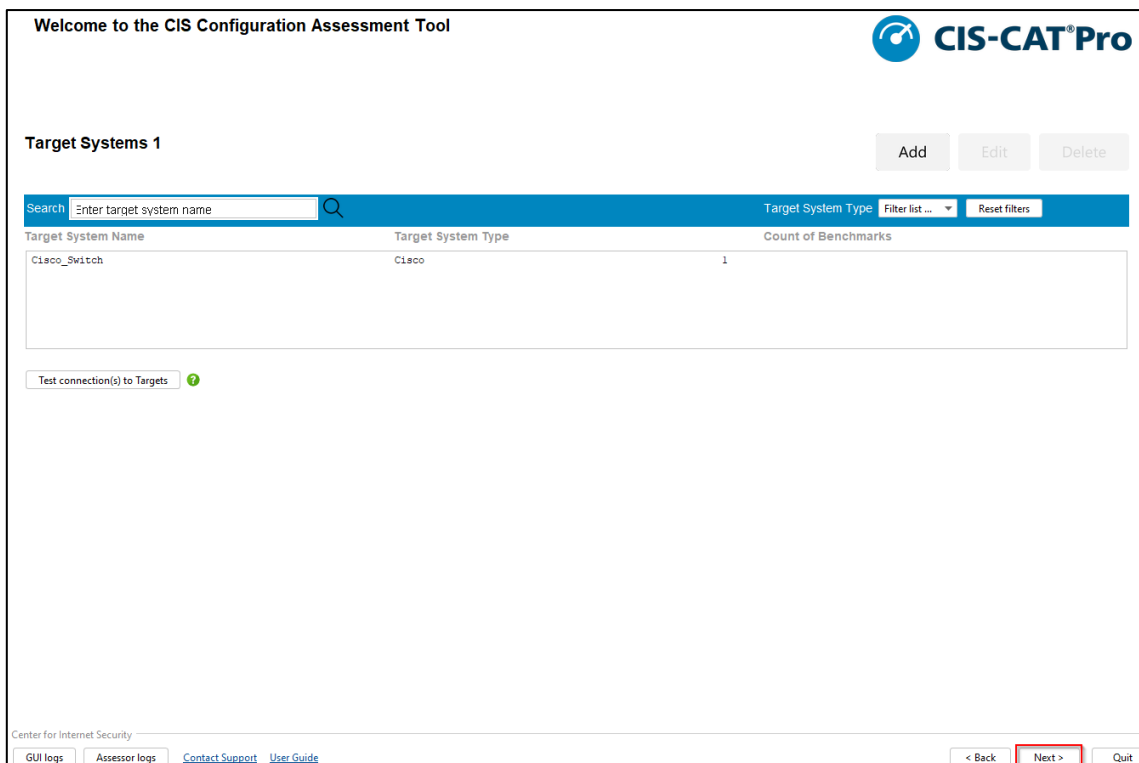
Grayed out selections have interactive values

Benchmark	Profile
-----------	---------

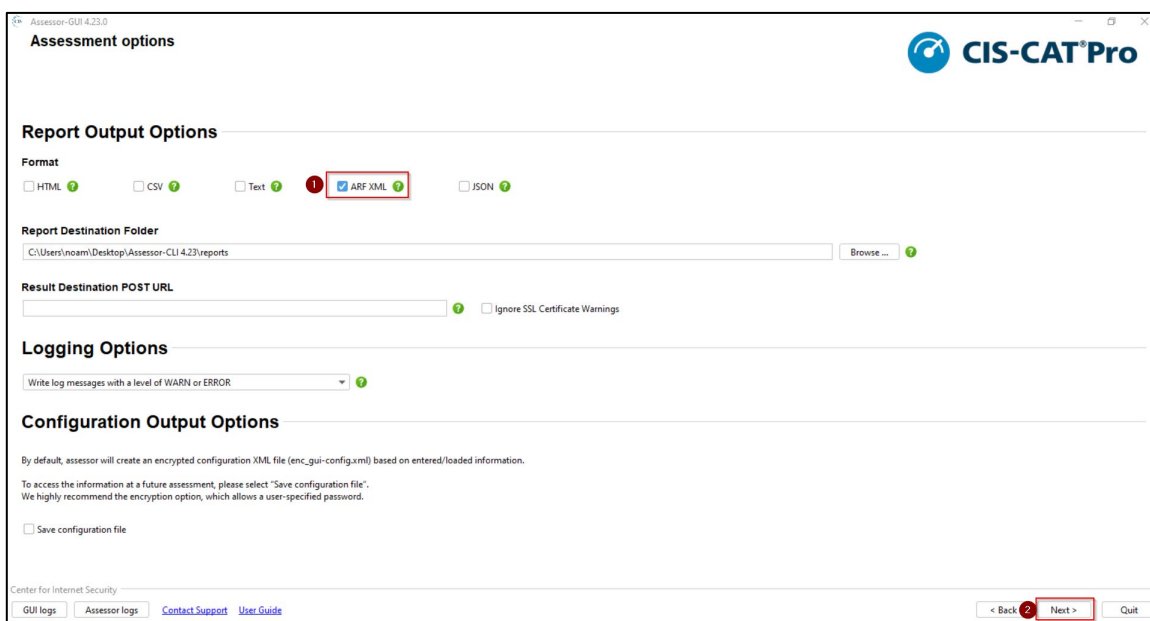
Center for Internet Security
GUI logs | Assessor logs | Contact Support | User Guide

Cancel | Save

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



11. 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".





7. Open and Review Integration Results on CyMA

1. For instructions on how to download CyMA, please refer to the "CyMA Installation" tip sheet.
2. After Installation, execute the "Cyber Quant CyMA" client and log in.

mastercard

Username:

Password:

[Forgot Password?](#)

Login

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

mastercard

Verification code:

[Resend code](#)

Submit

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

Open Assessment

Company:

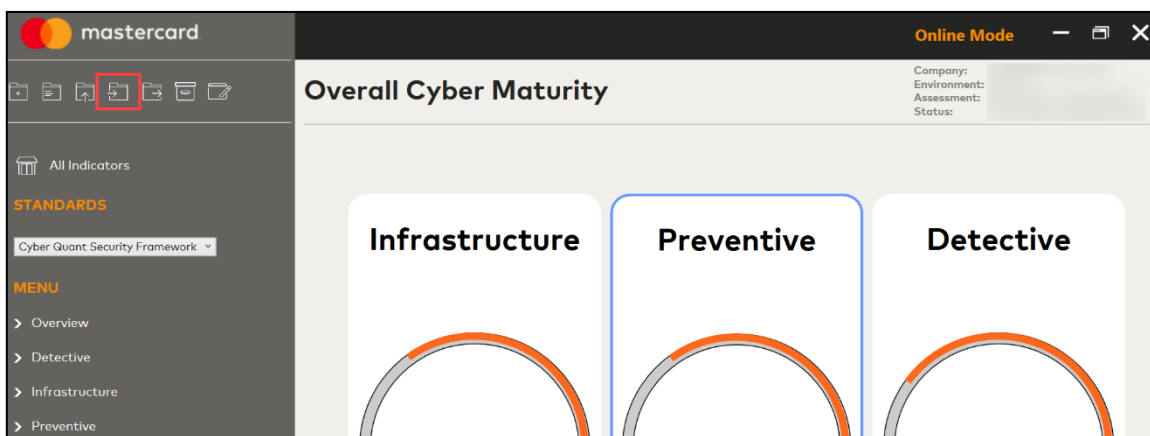
Environment:

Assessment:

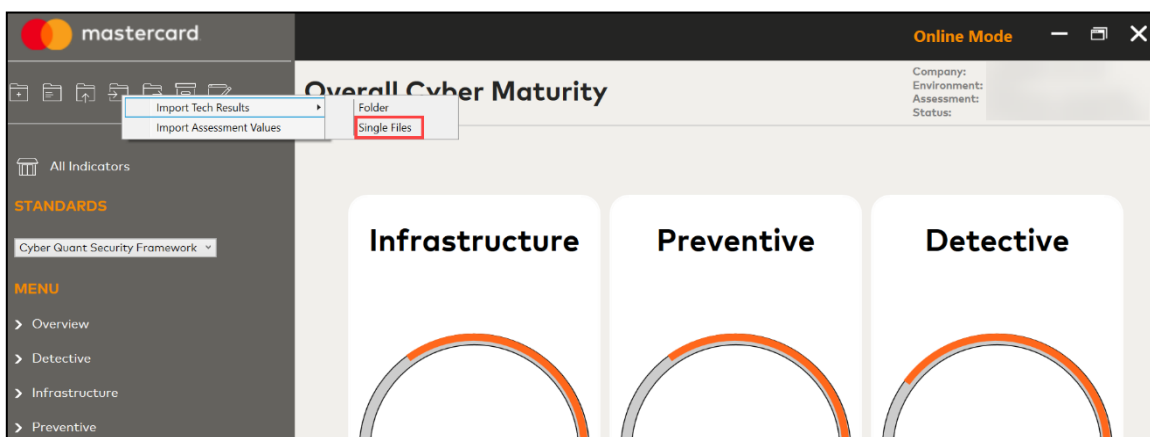
Open



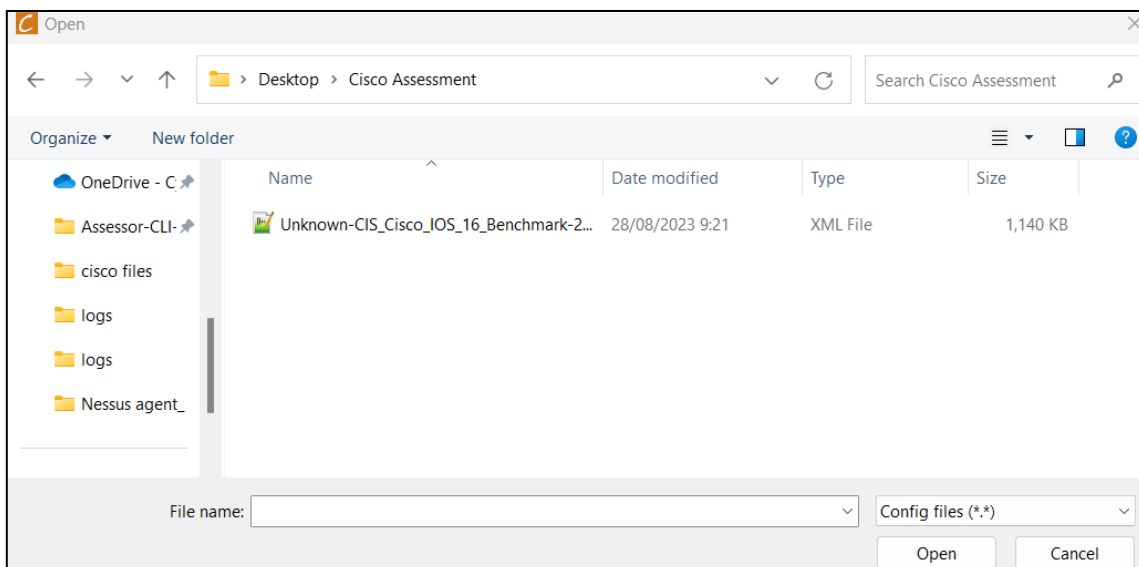
5. Click on the "Import Files" icon on the top left of the screen.



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

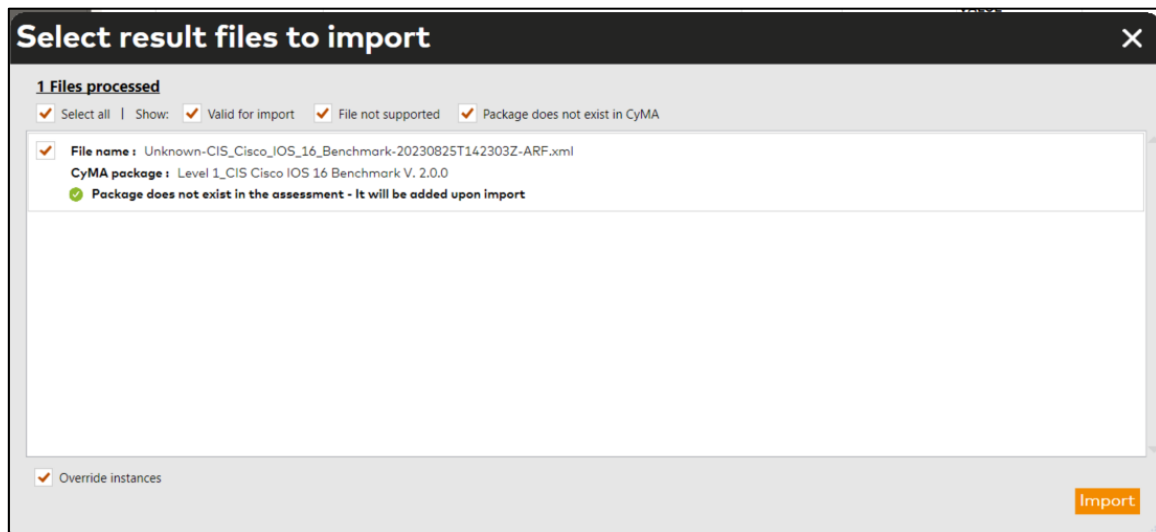


7. Browse to the dedicated folder where the configuration files are stored:

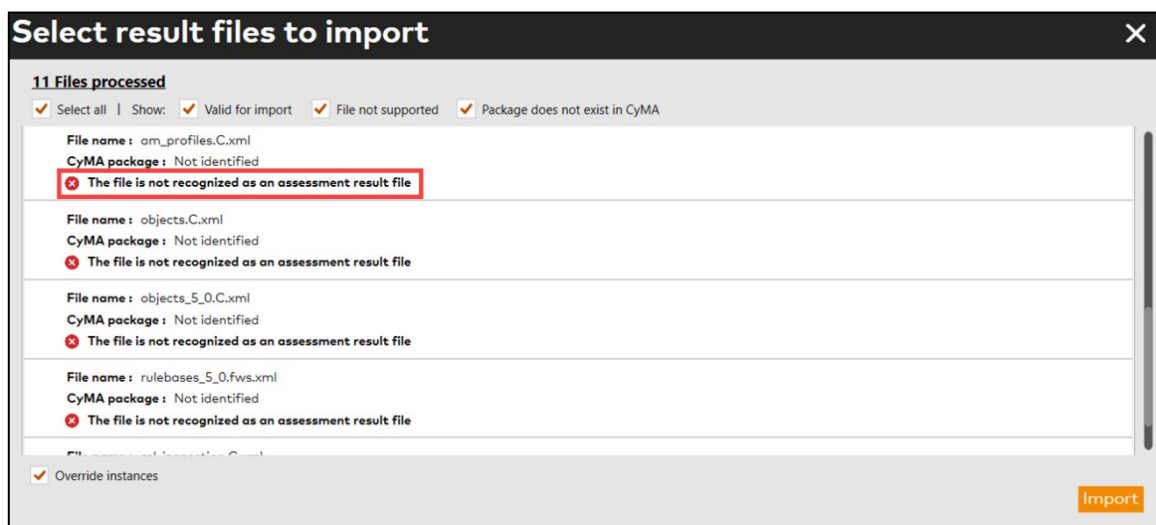




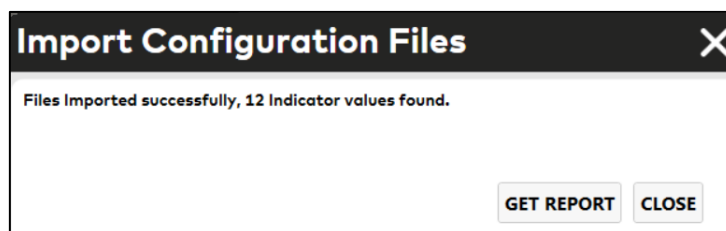
- Once the report is open, select the file and click "Import". The following screen displays information regarding import errors and packages associated with the imported files.



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

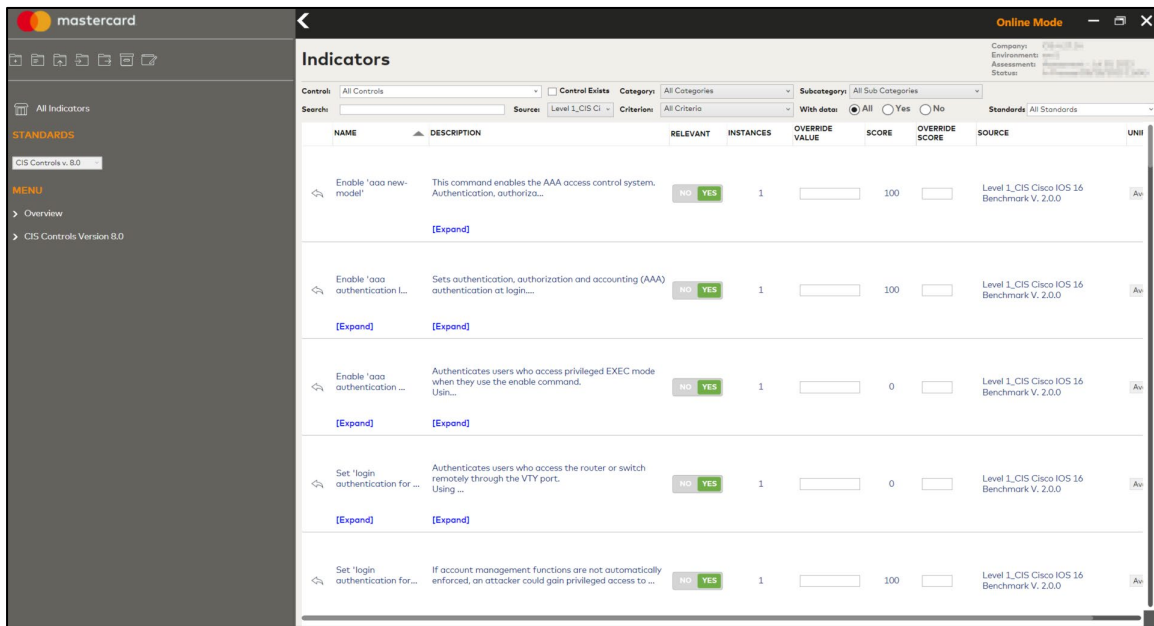


- Upon successful import, a confirmation notice is displayed, click "CLOSE". Please note that the number of indicators may vary based on the input configuration files.



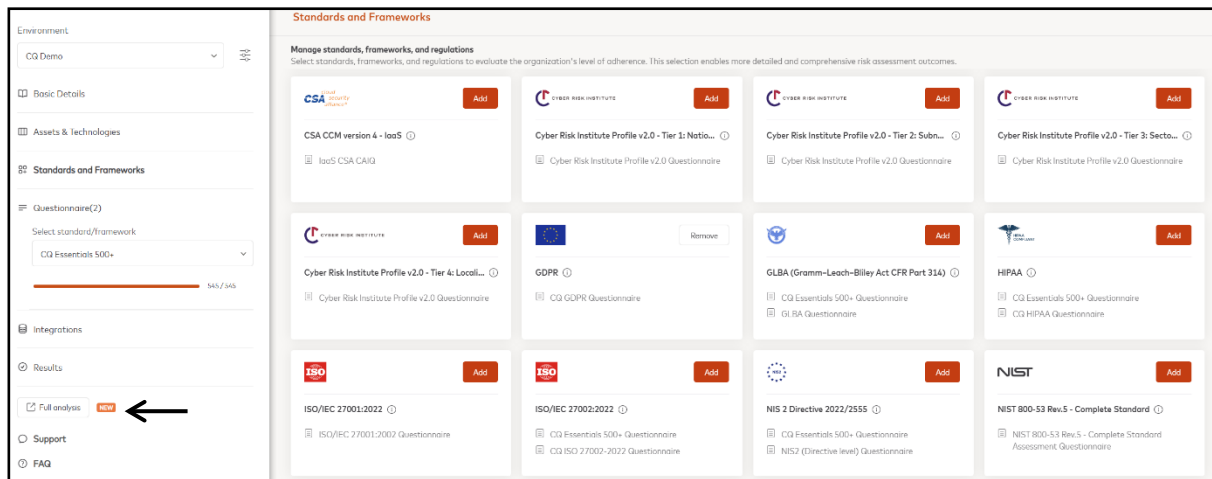


10. The assessment results are now available for review.

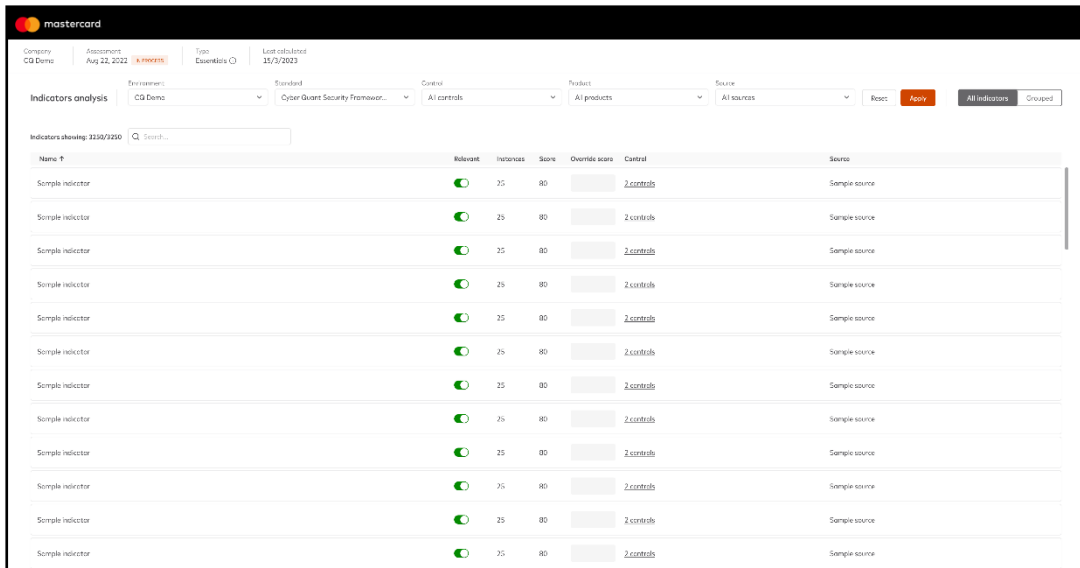


8. Review Integration Results on CyMA Web

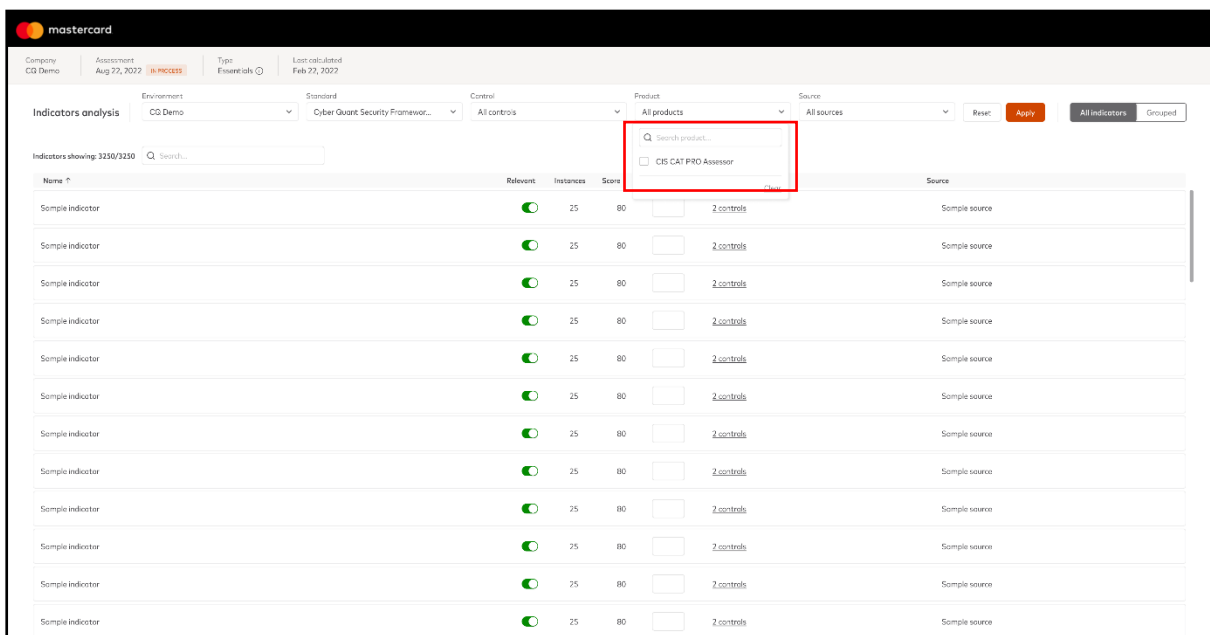
1. Go to the Assessment Portal, open the relevant company and click on "Full analysis" option.



2. After selection, you will be redirected to the page containing the CyMA or "Full Analysis" information.



3. Here you can filter the indicator based on the relevant product integration.



4. The product selection will be made with "CIS CAT Pro" and then select the Apply option.



The screenshot shows the Mastercard CIS Assessor interface. At the top, there are filters for Environment (CQ Demo), Standard (Cyber Quant Security Framework...), Control (All controls), Product (All products), and Source (All sources). A red box highlights the 'Apply' button. Below the filters, a table lists indicators. A dropdown menu is open over the 'Product' filter, showing 'CIS CAT PRO Assessor' selected. The table has columns for Name, Relevance, Instances, Score, and Source.

Name	Relevant	Instances	Score	Source
Sample indicator	<input checked="" type="checkbox"/>	25	80	2 controls
Sample indicator	<input checked="" type="checkbox"/>	25	80	2 controls
Sample indicator	<input checked="" type="checkbox"/>	25	80	2 controls
Sample indicator	<input checked="" type="checkbox"/>	25	80	2 controls
Sample indicator	<input checked="" type="checkbox"/>	25	80	2 controls
Sample indicator	<input checked="" type="checkbox"/>	25	80	2 controls
Sample indicator	<input checked="" type="checkbox"/>	25	80	2 controls
Sample indicator	<input checked="" type="checkbox"/>	25	80	2 controls
Sample indicator	<input checked="" type="checkbox"/>	25	80	2 controls
Sample indicator	<input checked="" type="checkbox"/>	25	80	2 controls
Sample indicator	<input checked="" type="checkbox"/>	25	80	2 controls
Sample indicator	<input checked="" type="checkbox"/>	25	80	2 controls
Sample indicator	<input checked="" type="checkbox"/>	25	80	2 controls
Sample indicator	<input checked="" type="checkbox"/>	25	80	2 controls
Sample indicator	<input checked="" type="checkbox"/>	25	80	2 controls

5. For the selected Product, you can analyze the indicator score, relevance, number of instances, and controls.
6. Clicking on the indicator will open a slider on the right-hand side with an in-depth view.

The screenshot shows the 'Indicator details' view in the Mastercard CIS Assessor. The 'Product' filter is set to 'CIS CAT PRO Assessor'. The table shows one indicator: 'Enable 'aaa new-model''. The details panel on the right provides information about the indicator, including its name, source, and controls.

Name	Relevant	Instances	Score	Override score	Control
Enable 'aaa new-model'	<input checked="" type="checkbox"/>	1	0		Access Control Management

Indicator details

Name
Enable 'aaa new-model'

This command enables the AAA access control system. Authentication, authorization and accounting (AAA) services provide an authoritative source for managing and monitoring access for devices. Centralizing control improves consistency of access control, the services that may be allowed or not authorized and accountability by tracking services accessed. Additionally, centralizing access control simplifies and reduces administrative costs of account provisioning and de-provisioning, especially when managing a large number of devices.

Source
Level_2_CIS Cisco IOS XE 17.3 Benchmark V. 2.2.0

Controls
Access Control Management