CIS-CAT Pro Assessor: Databases 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

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 database technologies configuration files for the "Cyber Quant CyMA" cyber risk and security assessment.

4. Requirements & Permissions

- Database Access:
  - Network Access to the target Database.
  - Target database user credentials with 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

Open the CIS-CAT Pro Assessor tool with administrative permissions on a Windows machine. The Windows machine must have network access to the network that the target database (Microsoft SQL, PostgreSQL, Oracle SQL, etc.) resides on.

Access the target database technology with the CIS-CAT Pro Assessor tool using its network access option and analyze the technology.

- For MongoDB, download the configuration file of the MongoDB and upload it to the CIS Assessor tool for Analysis.

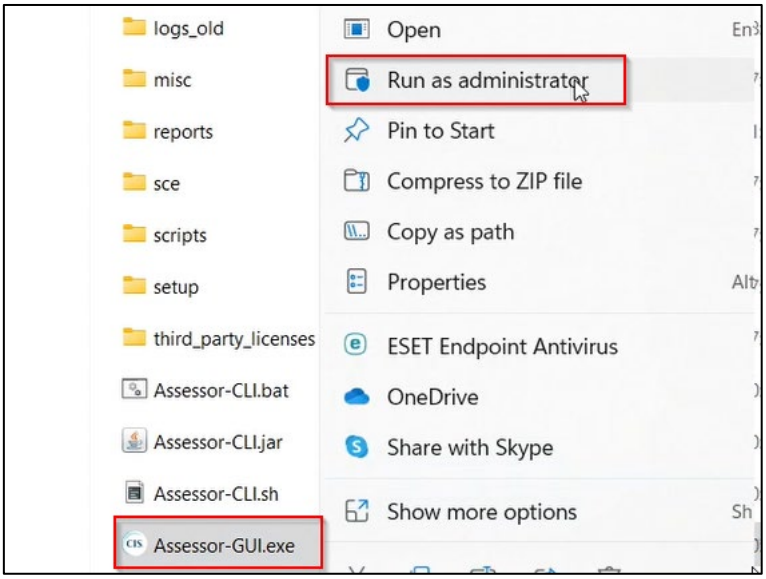
Import the extracted file into the "CIS-CAT Pro Assessor" tool for analysis and to generate an XML report.

6. The Extraction Process (Microsoft SQL, PostgreSQL, Oracle SQL)

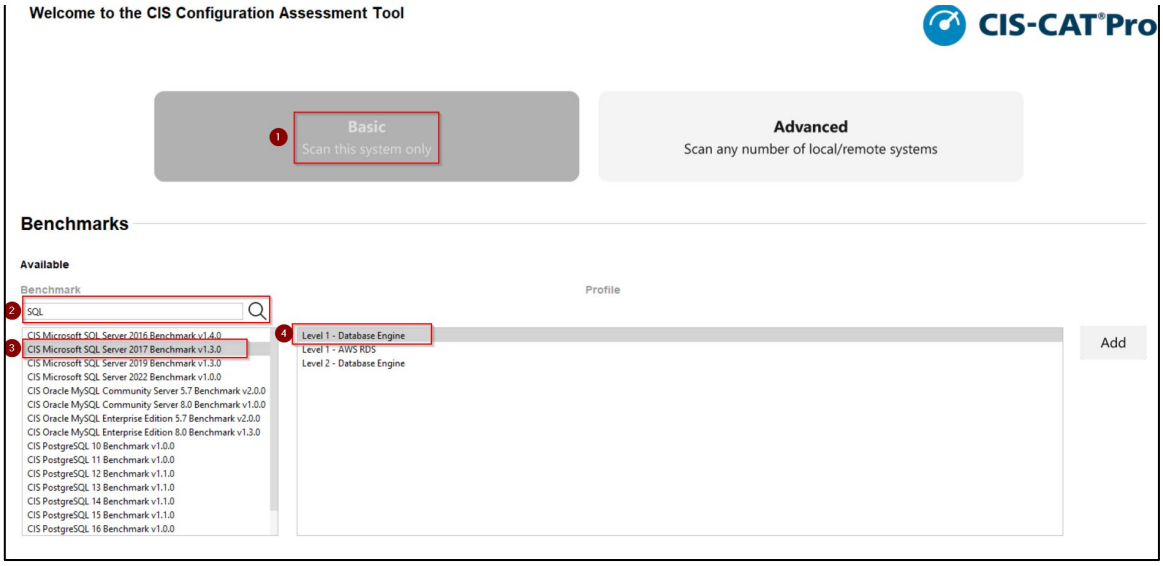
The process described in this part is relevant to the following database technologies:

- Microsoft SQL
- PostgreSQL
- Oracle SQL

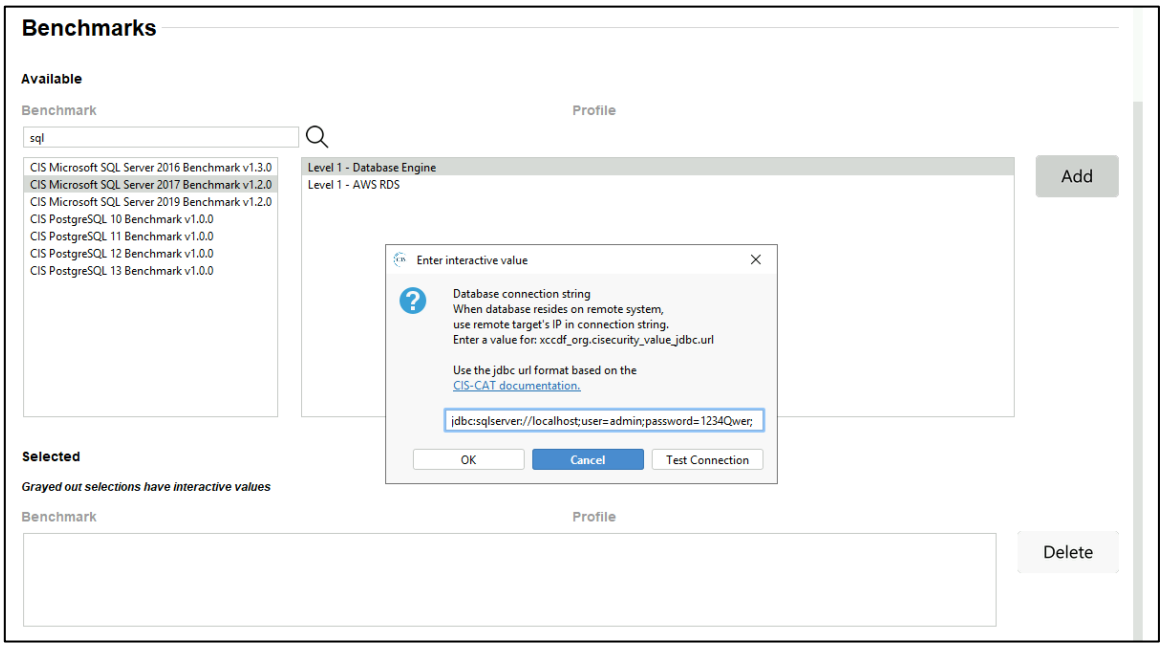
1. Start the "CIS-CAT Pro Assessor" tool as administrator and accept the user account control dialog box (proceed normally if it does not appear), it may require administrative credentials.



2. Click on "Basic" (1), search the desired database technology product (2), select the product (3), select the relevant benchmark (4), and click on "Add".

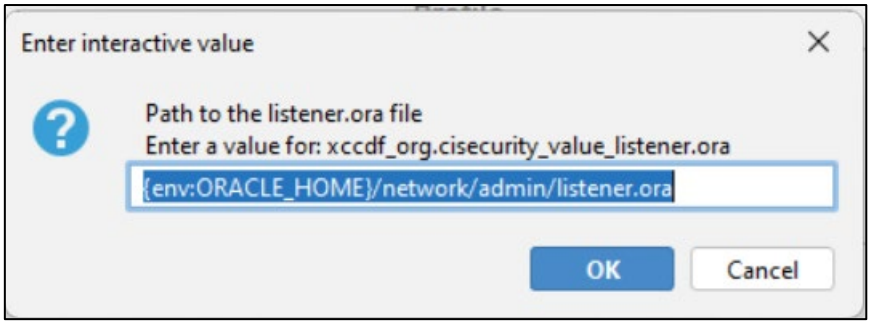


3. Adding the technology to the benchmark list requires inserting the connection string into the desired database. For additional information regarding the connection strings, please refer to "*Appendix A: Connection String Helper*"



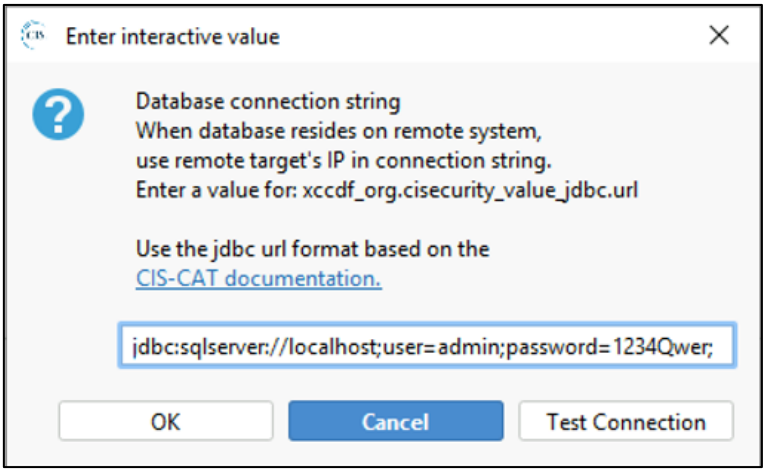
4. This step is **for Oracle databases only**:

a. Following the previous prompt for the connection string, another prompt will be displayed for the path to the "listener.ora" file.
   - The interactive value "listener.ora" is utilized in the assessment process to support recommendations in the section of CIS standard 2.1 of the CIS Oracle Database Benchmarks.
   - The default value is:
     {env:ORACLE_HOME}/network/admin/listener.ora
     In case of a different path, it should be entered instead of the default one.

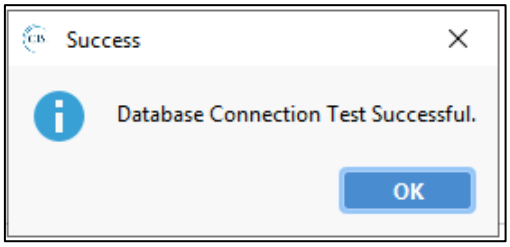


End of "For Oracle databases only" section.

5. After providing the connection string, click "Test Connection" to verify the connection to the database is valid.

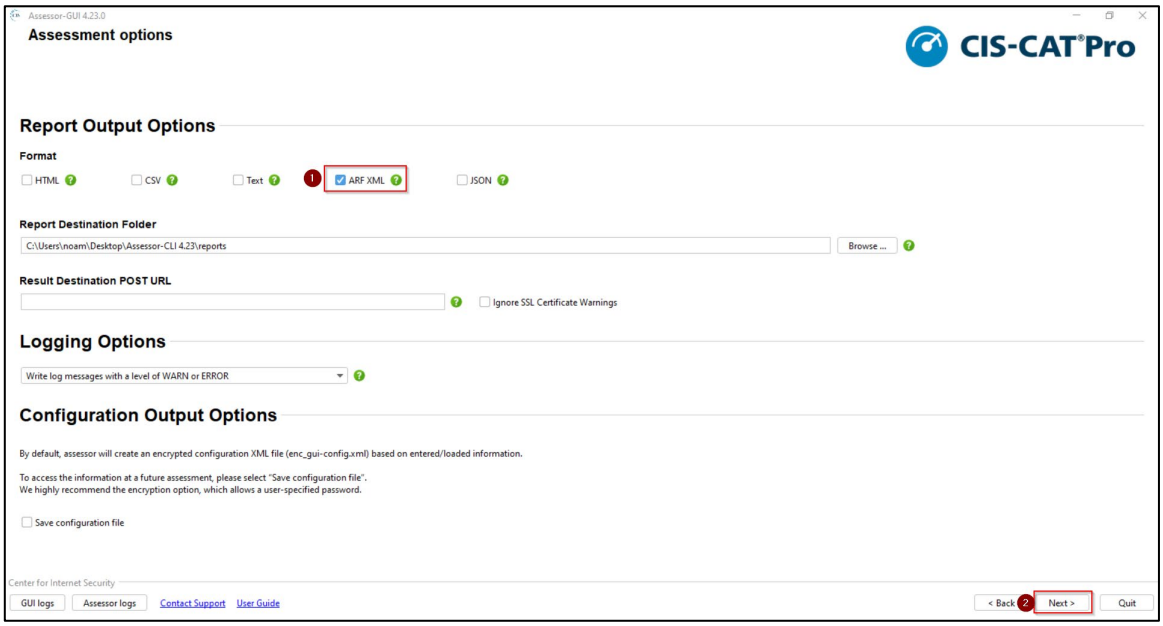


6. Click "OK" and then "Save" to configure the reporting destination and format.

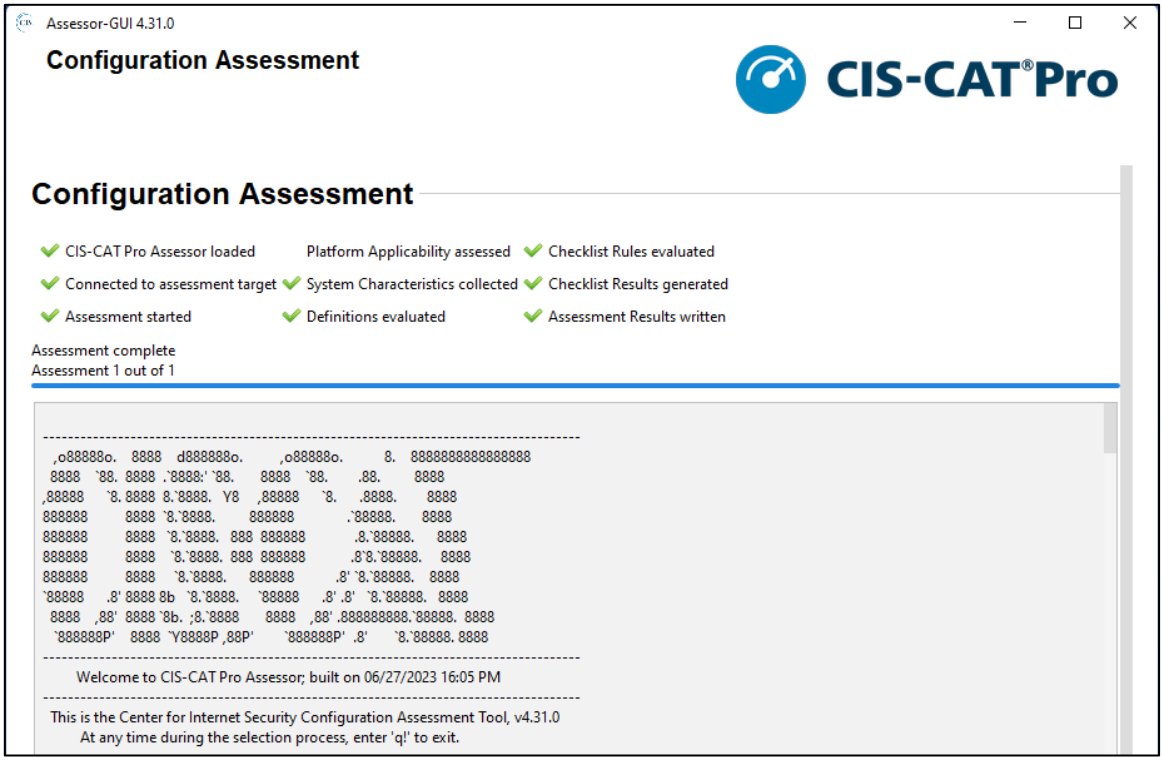


7. Select the "ARF XML" format (this is the only format supported by "CyMA") and the destination to save the report into and click "Next." In addition, an "HTML" format can also be selected to generate a human-friendly report. **It is recommended to store it in the default "C:\Assessor-CLI\reports" to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

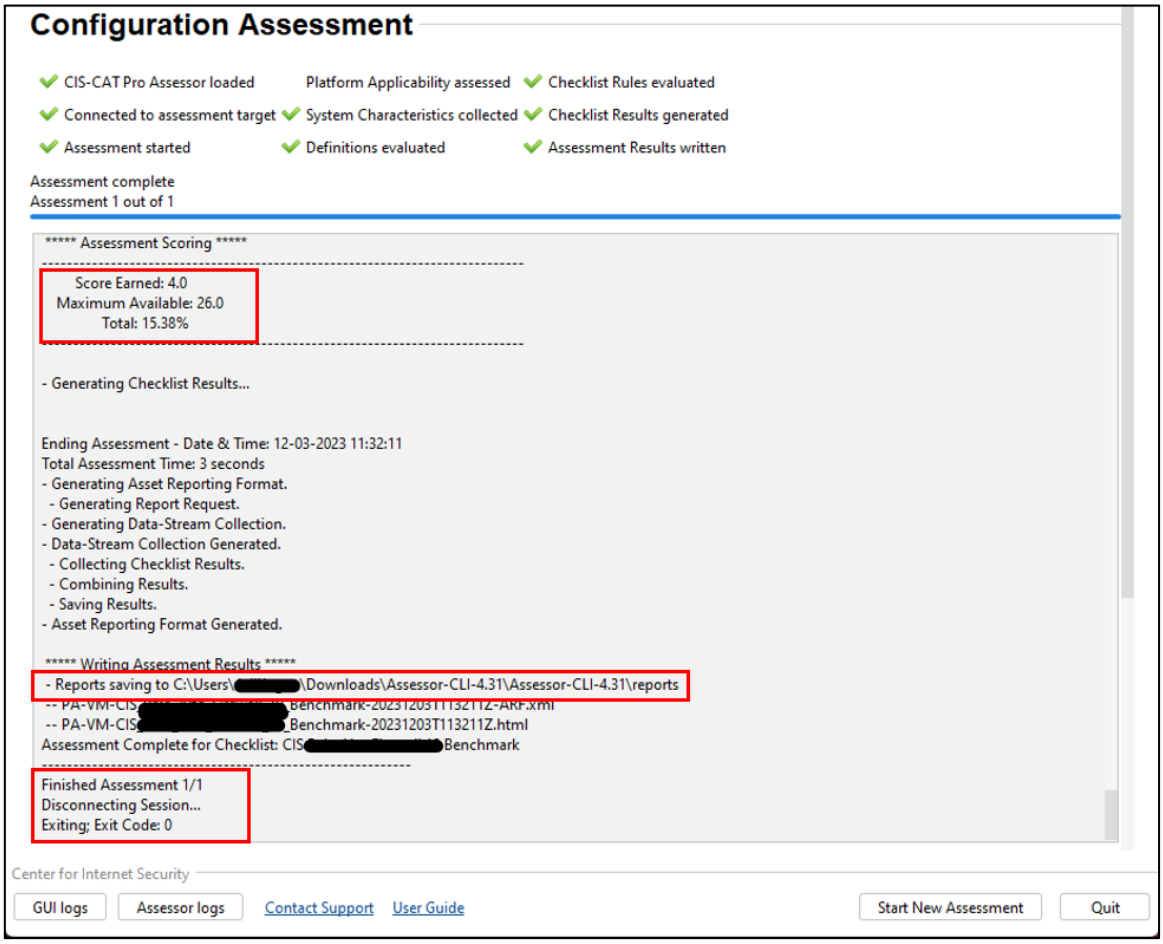
   When the "Confirmation" box appears, click on "Start Assessment".



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



9. 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.



10. Click on "Quit" after a successful assessment to close the too.

7. The Extraction Process (MongoDB)

1. Download the MongoDB configuration file from the target server and copy it to the CIS-Assessor machine.

   Note:

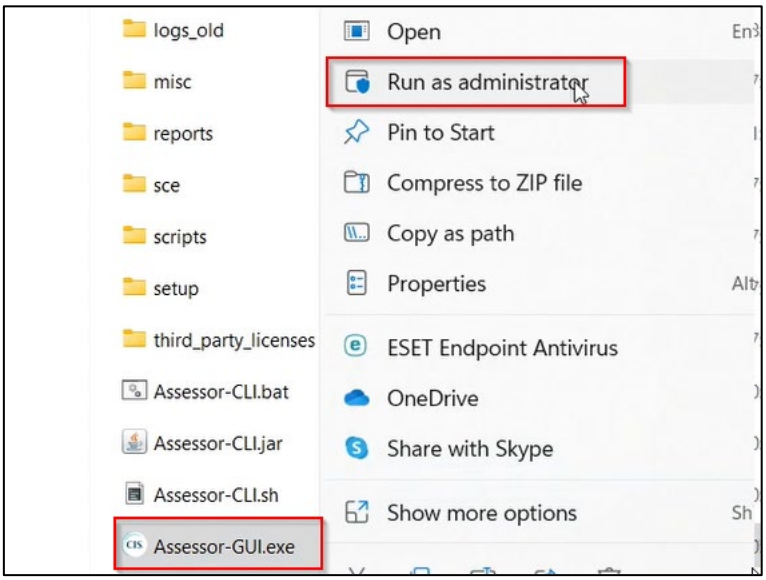
   If you can't find the MongoDB configuration file in the default location, connect to the Mongo DB instance using the MongoDB Client with a valid username and password and execute the following command:

   db.runCommand({ getCmdLineOpts: 1 })

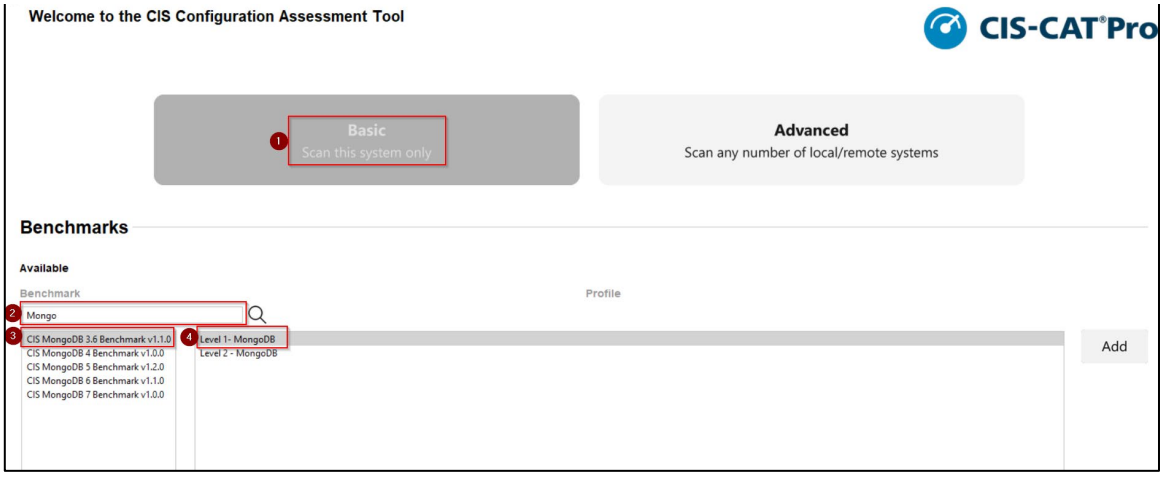
   The output of the command will include the MongoDB running configuration file location. For example:

   "config" : "/user/data/mongod.conf",

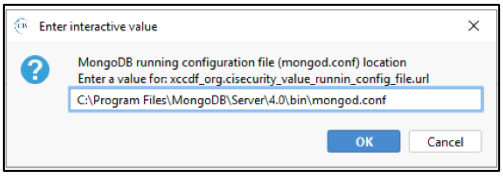
2. Start the "CIS-CAT Pro Assessor" tool as administrator and accept the user account control dialog box (proceed normally if it does not appear), it may require administrative credentials.



3. Click on "Basic" (1), search the desired database technology product (2), select the product (3), select the relevant benchmark (4), and click on "Add".



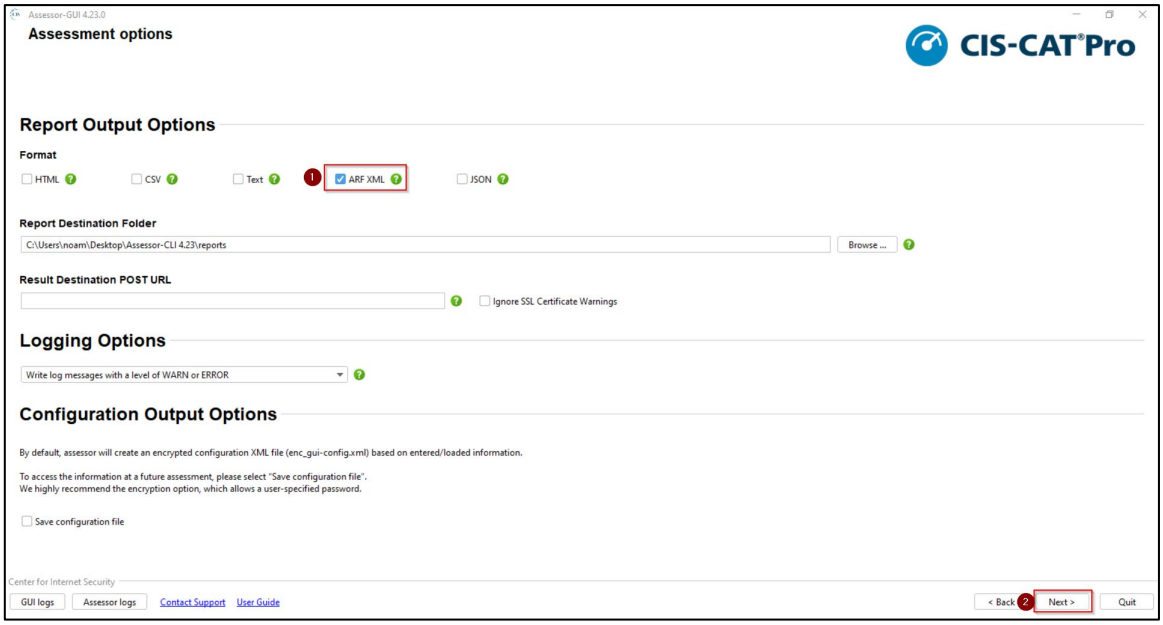
4. In the interactive value window, enter the path of the configuration file location. The default download location of the configuration file is "/etc/mongod.conf"



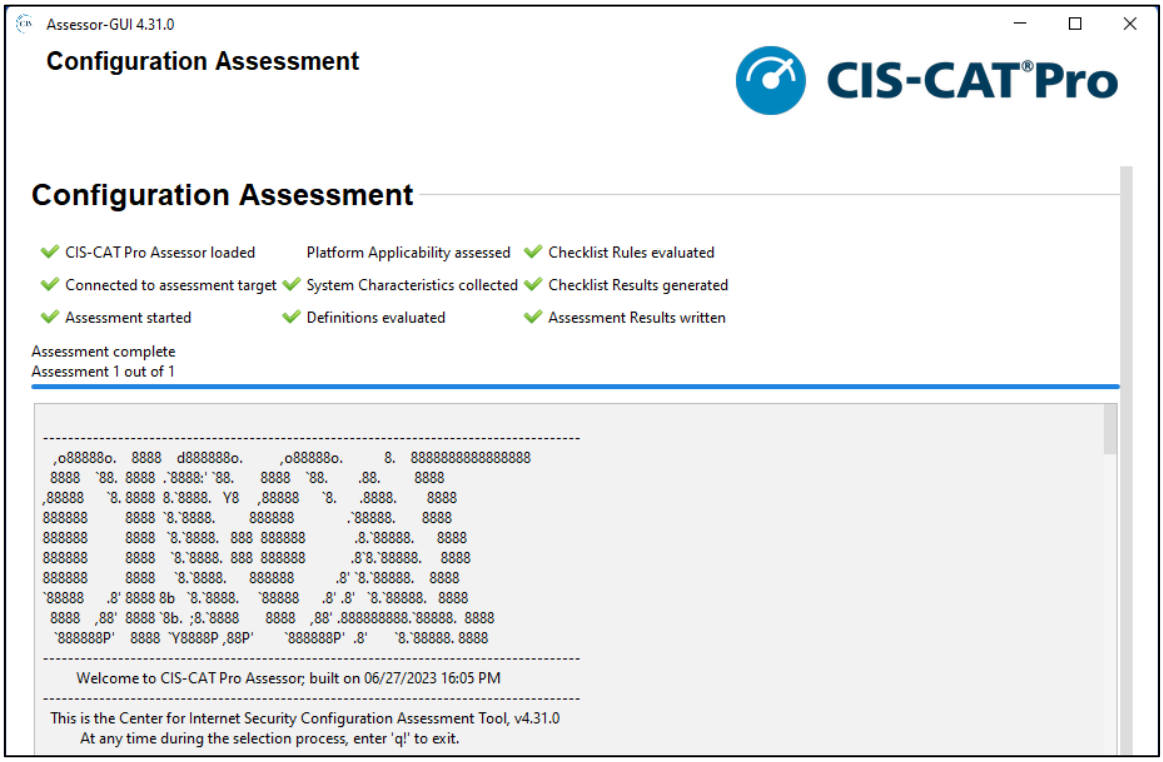
5. Click "OK" and then "Save" to configure the reporting destination and format.

6. 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.**

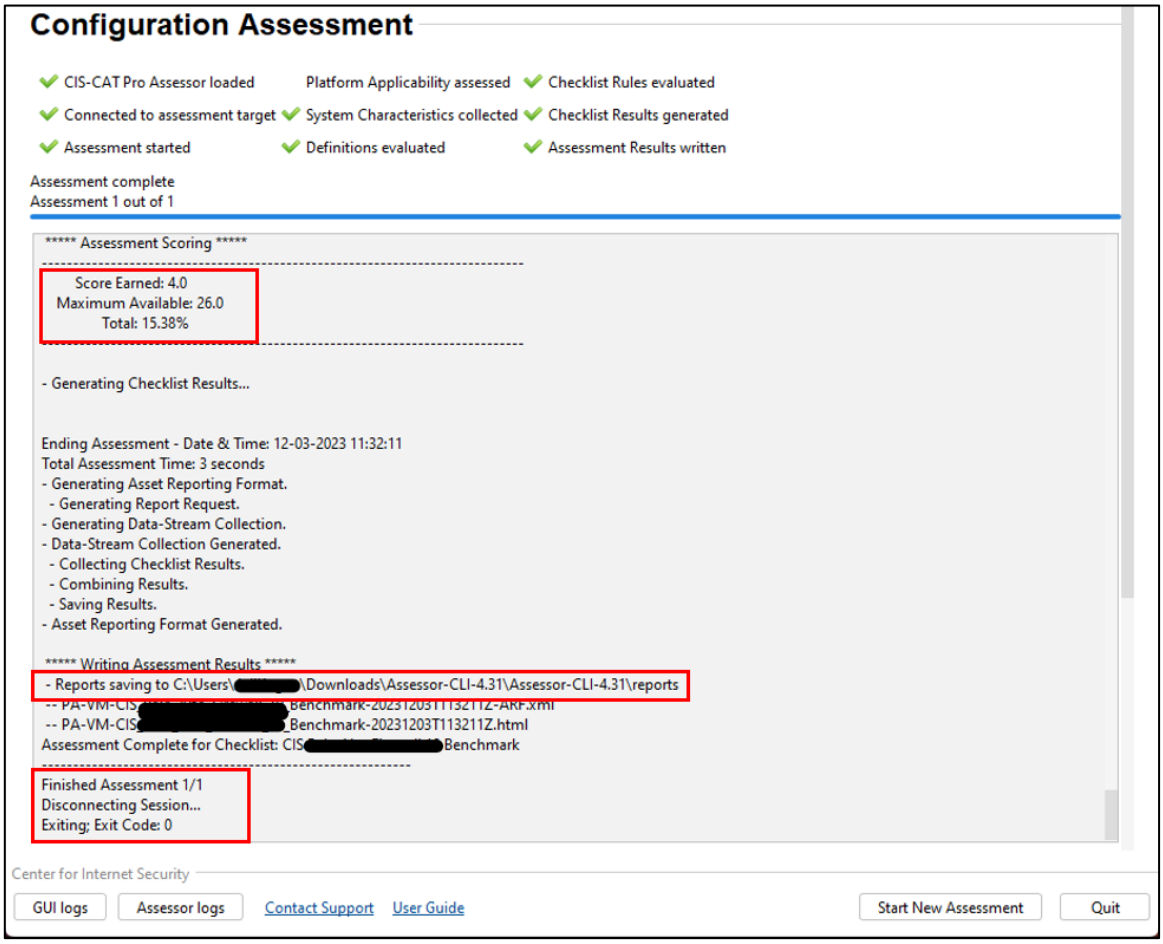
   When the "Confirmation" box appears, click on "Start Assessment".



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



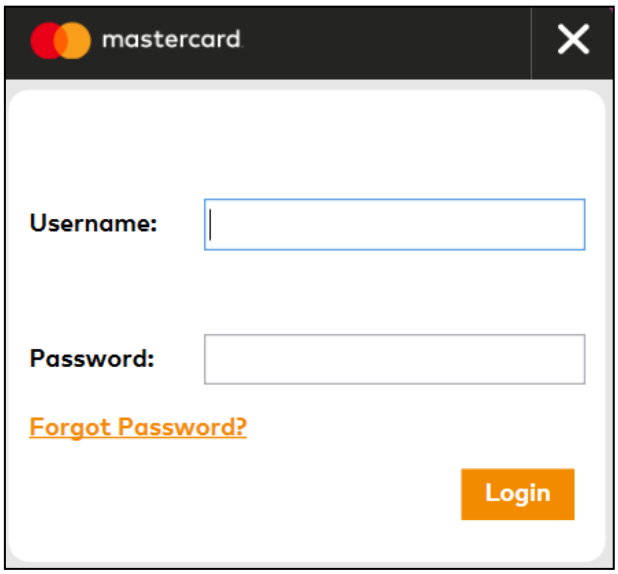
8. Once the assessment finishes, it displays information such as a score, the location of the generated reports, and whether it was successful or not. An exit code of 0 indicates a successful execution, while 1 indicates an error.



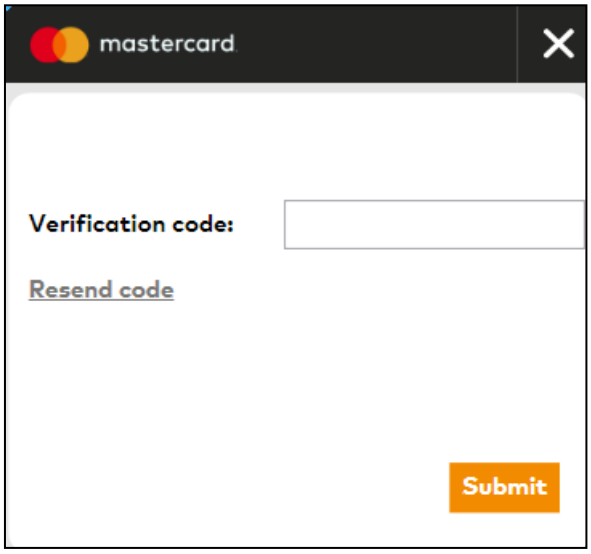
9. Click on "Quit" after a successful assessment to close the too.

10. Open and Review Integration Results

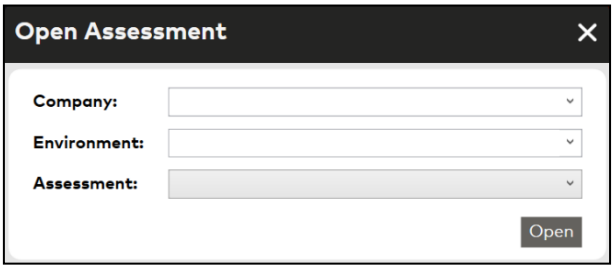
1. For instructions on how to download CyMA, please refer to the "CyMA Installation" tip sheet.
2. Execute the "Cyber Quant CyMA" client and log in.



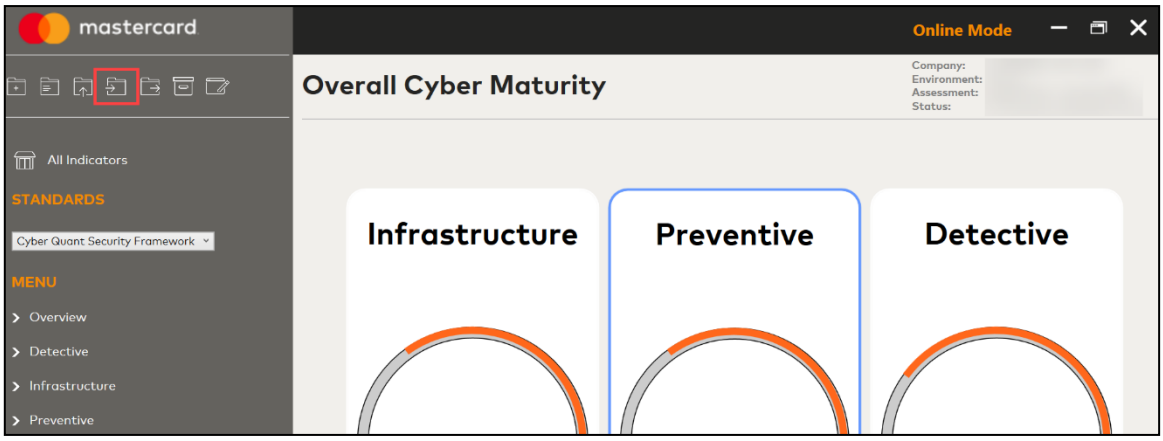
3. Enter the verification code sent to the account's email address.



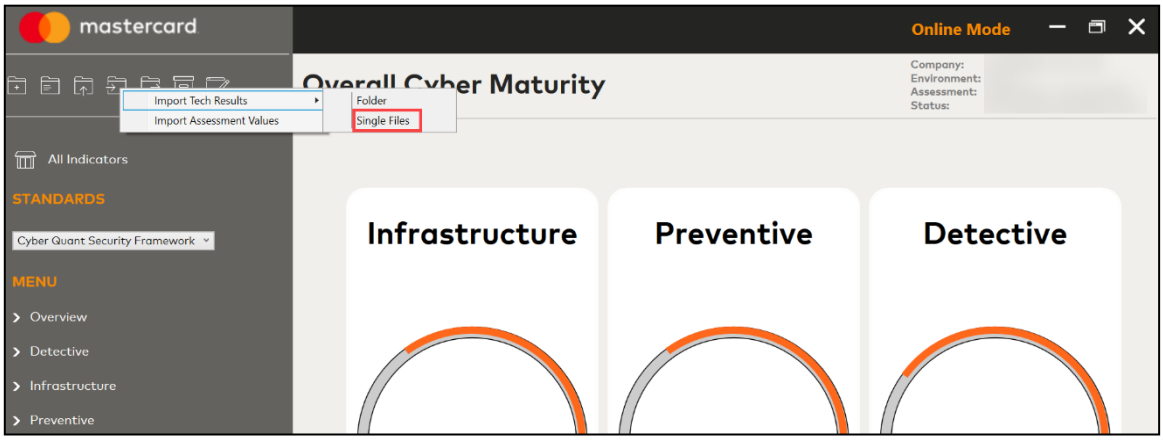
4. Select the desired company, environment, and assessment to import the report.



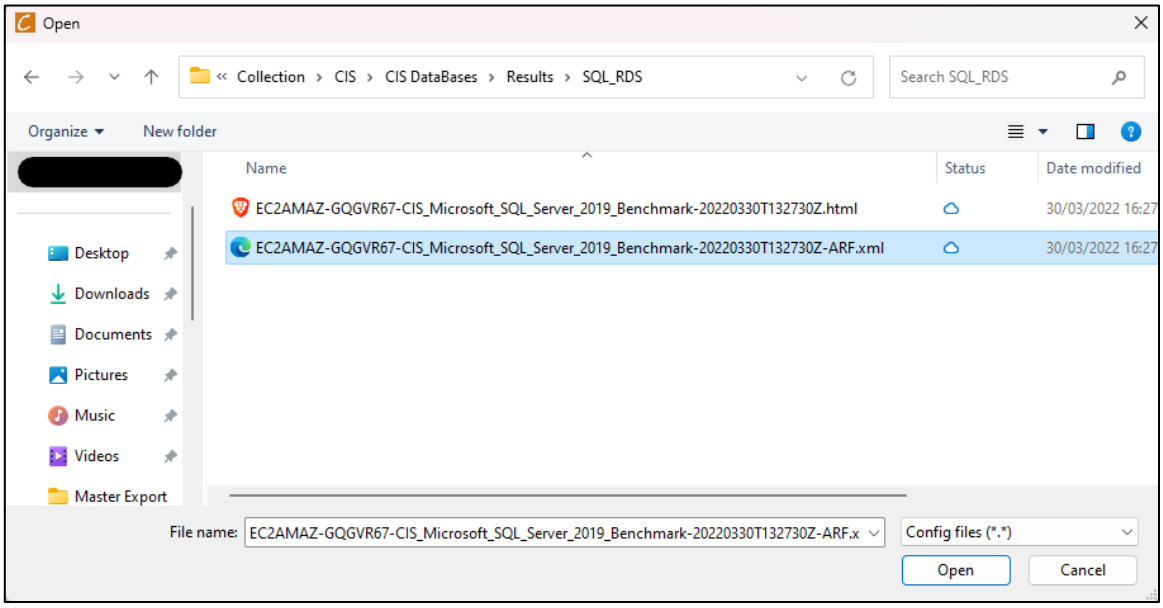
5. Click on the “Import Files” icon on the top left of the screen.



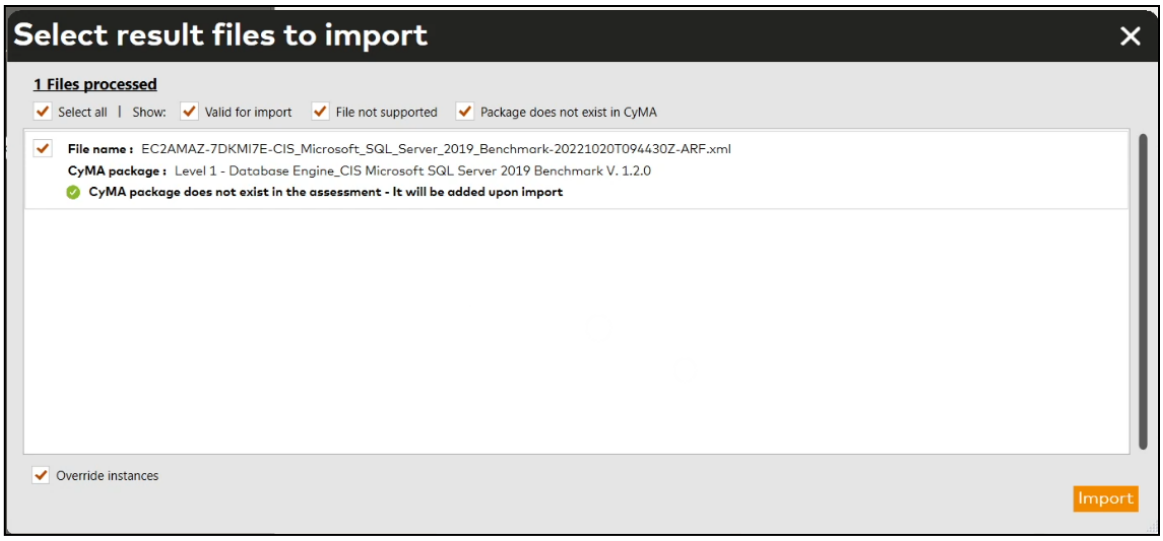
6. Hover over “Import Tech Results”, click “Choose Single File”.



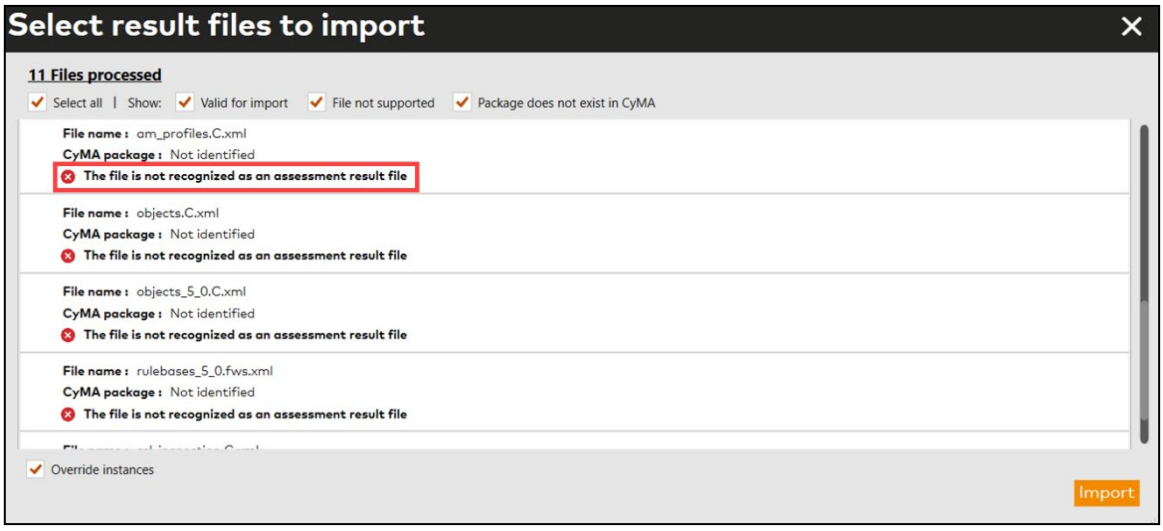
7. Browse to the dedicated folder where the report files are stored:



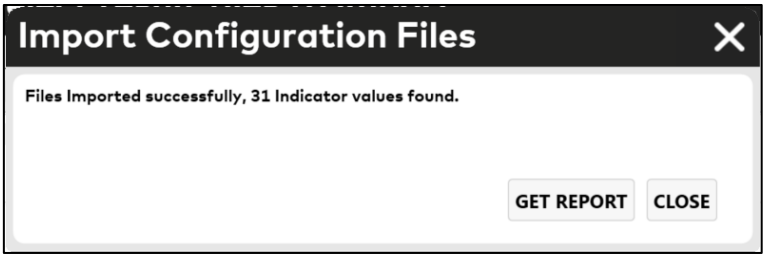
8. Once the report is open, select the file and click "Import". The following screen displays information regarding import errors and packages associated with the imported files.



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



9. 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.

11. Appendices

Appendix A: Connection String Helper

1. CIS Oracle Database Connection Strings

- Connection using SID examples:

  jdbc:oracle:thin:[username]/[password]@[hostname]:[port]:[SID]

  jdbc:oracle:thin:admin/pa55w0rd!@servername:1521:ORCL

- Connection using Service Name examples:

  jdbc:oracle:thin:[username]/[password]@//[hostname]:[port]/[service_name]

  jdbc:oracle:thin:sys as sysdba/pa55w0rd!@//servername:1521/SERVICE_NAME

  Property table for Oracle JDBC Connection String:

Property Name	Property Description
username	A valid username that can connect to the database instance. This user should have sufficient privileges to SELECT from the various tables and views indicated in the specific Oracle benchmark or be granted SYSDBA privileges.
password	The credentials for the specified username to connect to the database instance.
hostname	The name of the server (or it's IP address) hosting the database.
port	The port number on which the database is listening. By default, Oracle databases are configured to listen on port **1521**.
SID	The database SID.
Service Name	The database Service Name.

2. Microsoft SQL Server

In the CIS-CAT Pro Assessor, a Microsoft SQL Server database support is implemented using the Microsoft JDBC driver. The format of the Microsoft JDBC URL for Microsoft SQL Server is:

jdbc:sqlserver://[serverName[\instanceName][:portNumber]][;property=value[;property=value]]

- **jdbc:sqlserver:// (Required)** - is known as the subprotocol and is constant.
- **serverName (Optional)** - is the address of the server to connect to. This address can be a DNS or IP address, or it can be localhost or 127.0.0.1 for the local computer. If not specified in the connection URL, the server name must be specified in the properties collection.
- **instanceName (Optional)** - is the instance to connect to serverName. If not specified, a connection to the default instance is made.
- **portNumber (Optional)** - is the port to connect to on serverName. The default is 1433. If you're using the default, you don't have to specify the port, nor it's preceding ':', in the URL.
- **property (Optional)** - is one or more option connection properties.
  For more information, see Setting the connection properties.

Any property from the list can be specified.

Properties can only be delimited by using the semicolon (';'), and they can't be duplicated.

For example, consider a Microsoft SQL Server database instance with the following information:

Property Name	Property Value
Server Name	CIS-SERVER
Database Name	TestDB
Database Port	1433
Windows Domain	WIN-DOMAIN
Windows Domain User/Password	jsmith/qw3rty
SQL Server Database User/Password	db_user/db_pass
Instance Name	TestInstance

Basic Connection

The connection string to connect to the default database on the local computer by using a username/password is as follows:

jdbc:sqlserver://localhost;user=MyUserName;password=Pa$$w0rd;

Windows Authentication

Windows Authentication Mode allows the user to connect to a SQL Server instance through a Microsoft Windows user account. This mode allows domain user account information to be supplied to establish a connection. The following JDBC connection string would be valid for establishing a connection using the above example information:

jdbc:sqlserver://CIS-SERVER:1433;databaseName=TestDB;domain=WIN-DOMAIN;user=jsmith;
password=qw3rty;instanceName=TestInstance;

Windows Authentication Mode may also be used against databases running on machines not joined to a domain (standalone servers). When authenticating Microsoft Windows user accounts to non-domain joined servers, place it as the "domain" name.

For example, if the name of the standalone server is SQLSERVER, the JDBC connection string would look as such:

jdbc:sqlserver://CIS-SERVER:1433;databaseName=TestDB;domain=SQLSERVER;user=jsmith;
password=qw3rty;instanceName=TestInstance;

SQL Server Authentication

SQL Server Authentication provides the ability for connections to a database instance to be made using trusted username and password information, allowing SQL Server to perform the authentication itself by checking to see if a SQL Server login account has been set up and if the password matches one previously recorded for that user.

The following JDBC URLs would be valid for establishing a connection using the above example information:

jdbc:sqlserver://CIS-SERVER:1433;databaseName=TestDB;user=db_user;password=db_pass;
instanceName=TestInstance;
jdbc:sqlserver://CIS-SERVER:1433;databaseName=TestDB;user=jsmith;password=qw3rty;
instanceName=TestInstance;

Integrated Security

The Microsoft SQL Server driver and CIS-CAT Pro Assessor do support the use of integrated security in the connection string. An example connection string could look like below:

jdbc:sqlserver://CIS-SERVER:1433;integratedSecurity=true;

When utilizing integrated security, the Microsoft SQL Server JDBC driver requires at least an additional .dll file to properly function. Additional information regarding the .dll file is located on the official Microsoft website.

CIS-CAT Pro includes the "mssql-jdbc_auth-<version>-<arch>.dll64-bit" file in the misc folder of the CIS-CAT build directories. The .dll files must be placed into the bin directory of the 64-bit Java

Runtime Environment (JRE) utilized to execute CIS-CAT Pro Assessor. CIS-CAT Pro does not support 32-bit Java when assessing a Windows environment.

Dynamic Ports

CIS-CAT Pro supports remote and local assessments when dynamic ports are configured. For the configuration assessment to be successful, the following must be in place:

- CIS-CAT Pro Assessor resides on the database host machine for local assessment.
- The Microsoft SQL Server named instance option is utilized as opposed to the default instance.
- SQL Server Browser enabled
- UDP 1434 (SQL Server Browser) and sqlserver.exe opened on the firewall

Modify the connection string by replacing the Server Name with localhost like the below example when conducting a local assessment:

jdbc:sqlserver://localhost;databaseName=TestDB;user=jsmith;password=qw3rty;
instanceName=TestInstance;

When assessing remote hosts in the cloud, the below additional requirements should be fulfilled:

- The traffic of port 49 and port range 152 to 65,535 should be allowed to initiate a connection to the database. Please ensure that the above is in line with your organizational security policies. Otherwise, utilize a static port.
- UDP port 1434 must be allowed in the security group.

3. PostgreSQL Database

CIS-CAT Pro Assessor has implemented support for assessments against PostgreSQL database instances using the PostgreSQL JDBC driver.

The format for the PostgreSQL JDBC connection string is:

jdbc:postgresql://<host>:<port>/<database>?<key1>=<value1>&<key2>=<value2>...

For example:

jdbc:postgresql://POSTGRESQL:5432/PostgreSQL-DB?user=username&password=password

If CIS-CAT Pro Assessor is connecting to PostgreSQL on the default port (5432), it can be omitted from the connection string:

jdbc:postgresql://CIS-POSTGRESQL/PostgreSQL-DB?user=db_user&password=db_pass

For example, to force the database connection to require SSL, the connection string would look like:

jdbc:postgresql://CIS-POSTGRESQL/PostgreSQL-DB?user=db_user&password=db_pass&ssl=true

Property Name	Property Value
host	The name of the server (or its IP address) hosting the database.
port	The port number on which the database is listening. By default, Oracle databases are configured to listen on port 5432 (the default).
database	The database name
username	A valid username who can connect to the database server.
password	The credentials for the specified username to connect to the database server.
ssl	A Boolean value (true or false), to force the usage of SSL on the connection.
db_user	A valid username who can connect to the database.
db_pass	The credentials for the specified username to connect to the database instance.

4. Oracle MySQL Database

Oracle MySQL database support is implemented using the MariaDB JDBC driver. The format for the MariaDB JDBC connection string for MySQL is:

jdbc:mysql://<host>:<port>/<database>?<key1>=<value1>&<key2>=<value2>...

For example:

jdbc:mysql://172.20.25.187:3306/TestDB?user=db_user&password=db_password

Notable Optional parameters involve ensuring JDBC connections are made via SSL presented in the table below:

Property Name	Property Description
user	The database username.
password	The credentials for the specified user to connect to the database instance. CIS-CAT does not support the use of "&" (ampersand) for this database type.
useSSL	Force the usage of SSL on the connection.
trustServerCertificate	When using SSL, do *not* verify the server's certificate.

serverSslCert	Server's certificate in DER form, or server's CA certificate. Can be used in one of 3 forms: *serverSslCert=/path/to/cert.pem: full path to a certificate* *serverSslCert =classpath:relative/cert.pem: relative to the current classpath* or as verbatim DER-encoded certificate string, starting with ------BEGIN CERTIFICATE-----