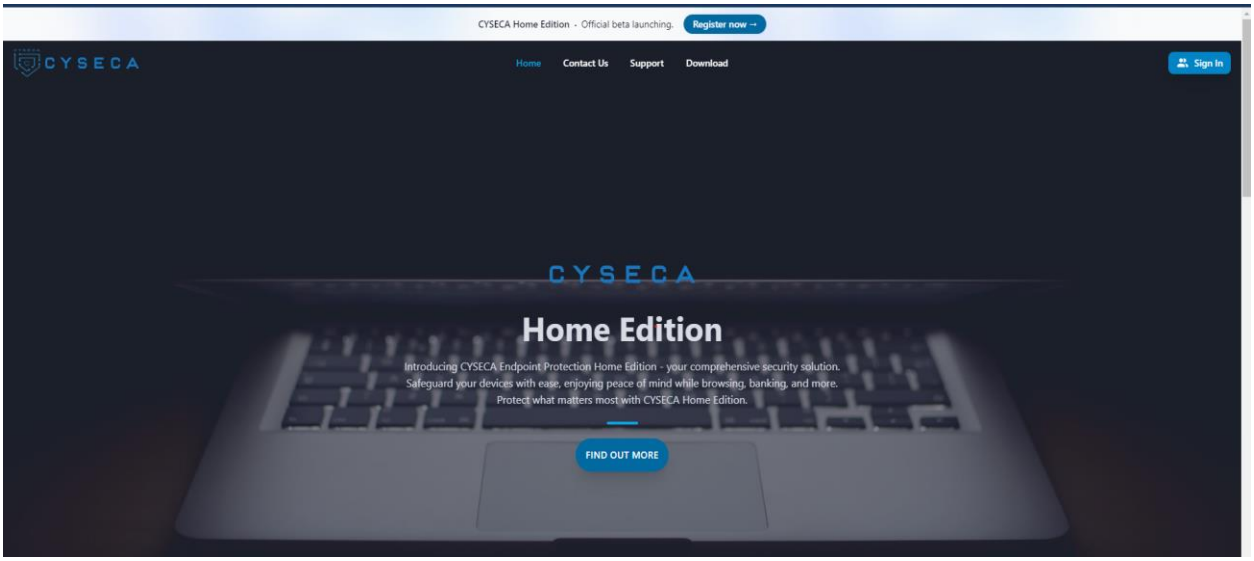
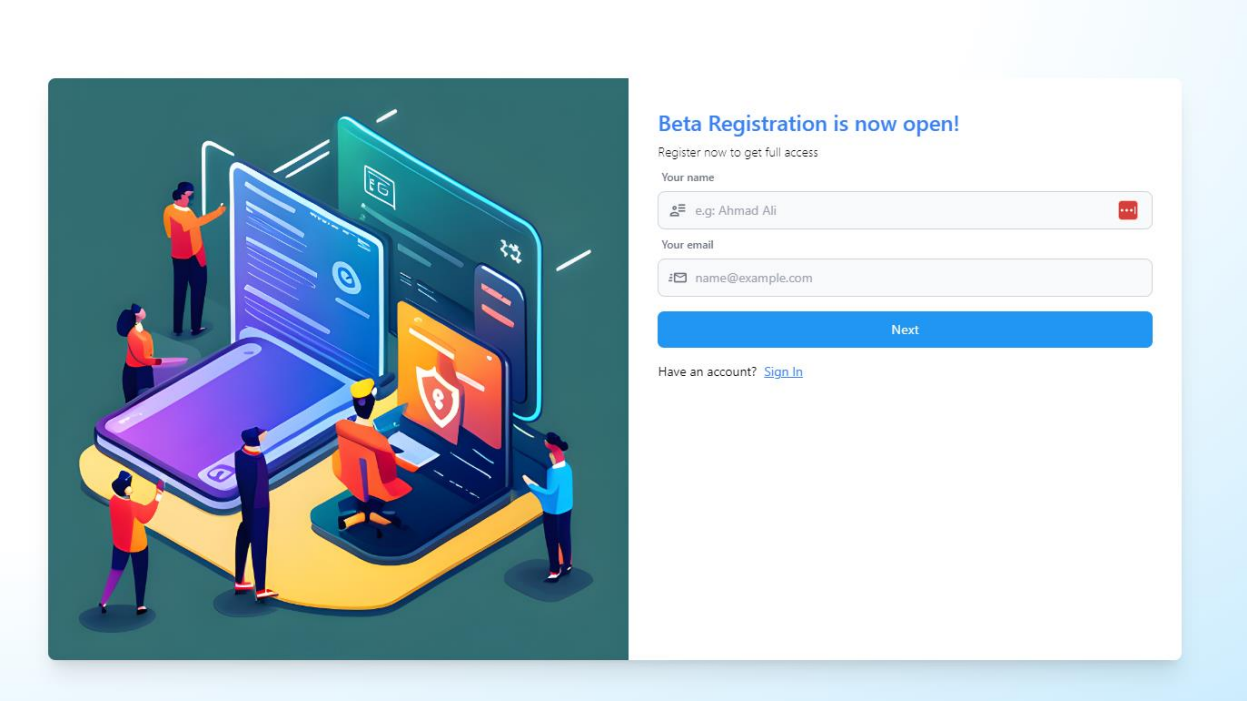
Registration

To obtain CYSECA Endpoint Application Control installer, user will have to register through a portal. The URL for the portal is https://www.cyseca.com.my/home-edition. The figure below shows the webpage. User must create and account first by click on register now to obtain CYSECA Home Edition installer and installation key.





User will have to fill in their name and email address for registration. User will also have to enter a strong password for the account. After successful registration, a confirmation email will be sent to the user for account activation.

CYSECA Home Edition · Official beta launching. Register now →

Home Contact Us Support Download

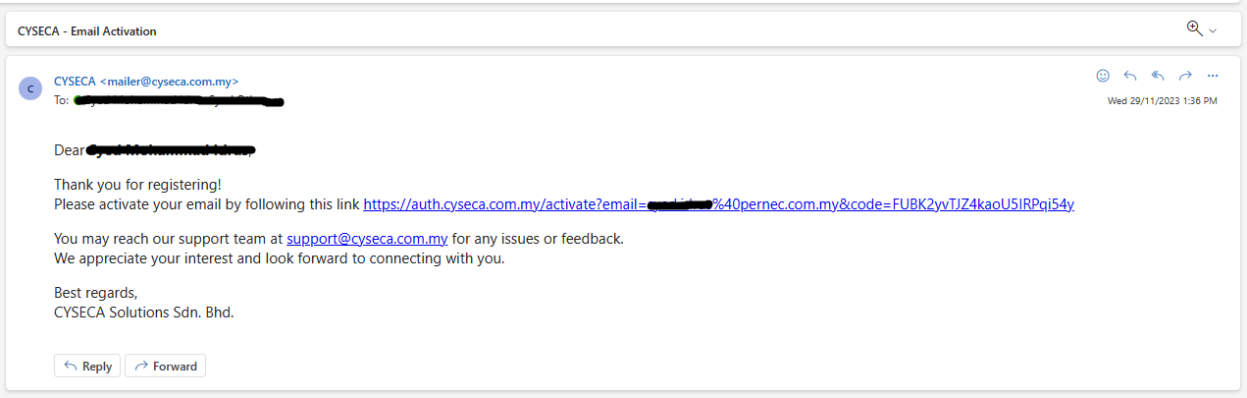
Congratulations!

Your registration has been successful.
We will send you an activation link to your registered email shortly.
Don't forget to check your spam folder too.

Back to Home

Account Activation and Verification

The figure below shows confirmation email sent for account verification. Click on the link to activate the account created. User will be navigated to the sign in page, and can proceed for retrieving license key and installer. Note that after registration, user will also have access to CYSECA Forum where user can give feedback, report bug and also interact with other users.

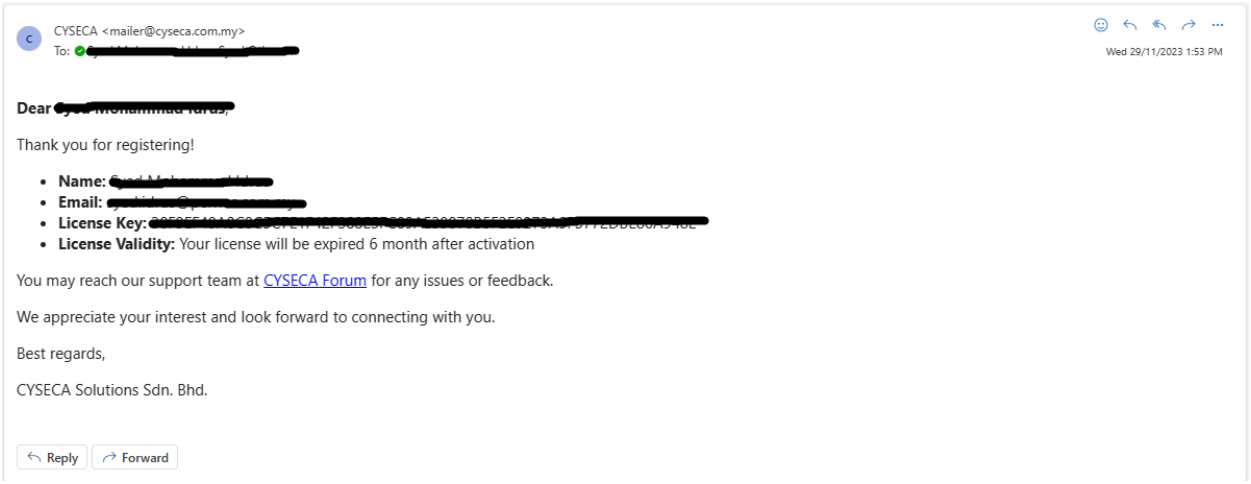


Your account is now activated

Click here to continue (2)

Privacy Policy • Terms of use

After account is activated, an email will be sent to the user containing Name, email, license key and license key validity. There is also a link to the CYSECA Forum. Figure below shows the email.



CYSECA <mailer@cyseca.com.my>
To: [redacted]

Wed 29/11/2023 1:53 PM

Dear [redacted],

Thank you for registering!

- **Name:** [redacted]
- **Email:** [redacted]
- **License Key:** [redacted]
- **License Validity:** Your license will be expired 6 month after activation

You may reach our support team at CYSECA Forum for any issues or feedback.

We appreciate your interest and look forward to connecting with you.

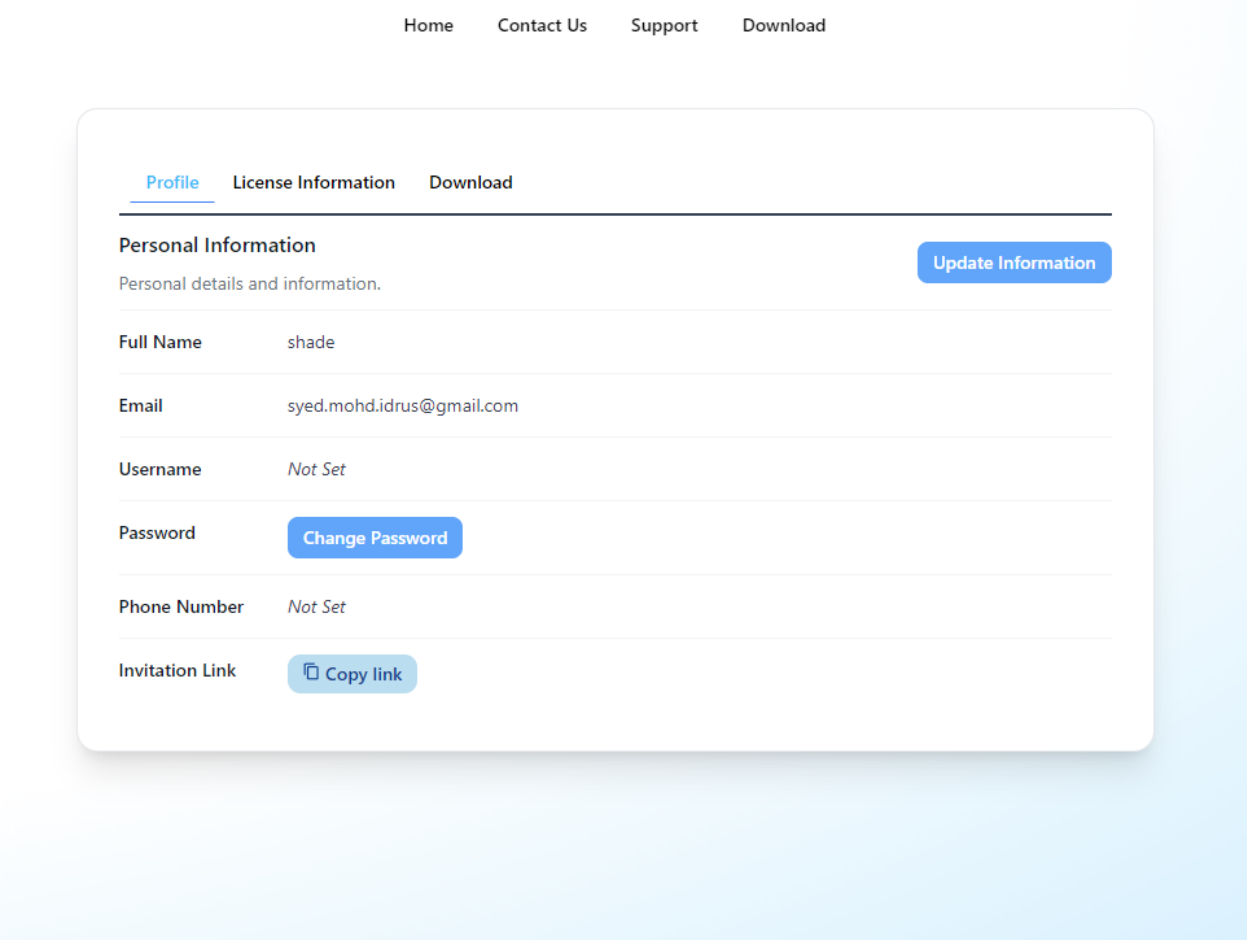
Best regards,

CYSECA Solutions Sdn. Bhd.

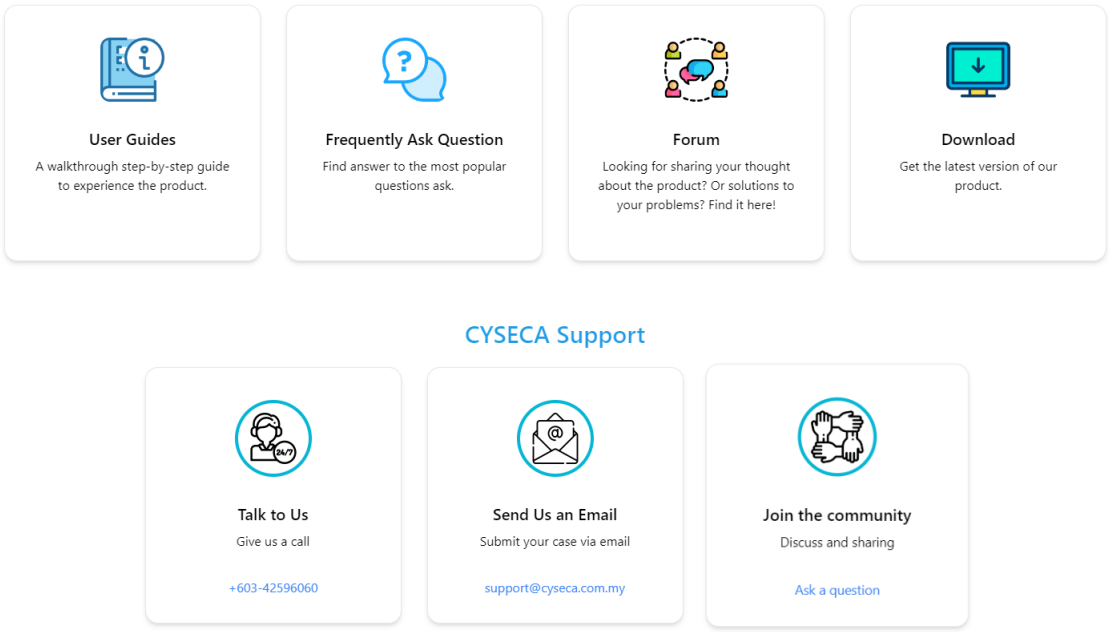
Reply Forward

Login and Downloading Installer

After account is successfully created and activated, user can proceed into logging in and downloading the installer. Figure below shows webpage after successful login.



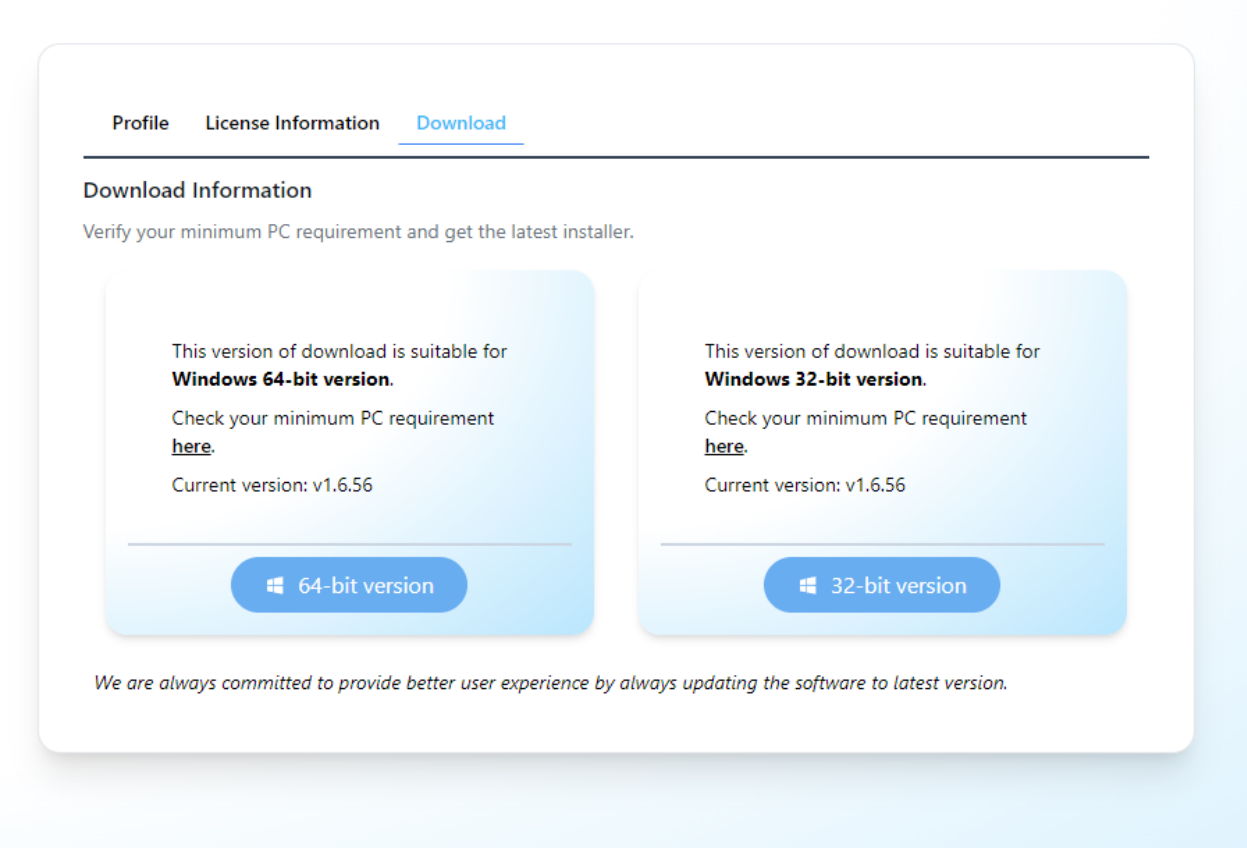
At this webpage, user can update profile, check license information and also download installer. User can also read information and guides about CYSECA Home Edition. Figure below shows the support and information page.



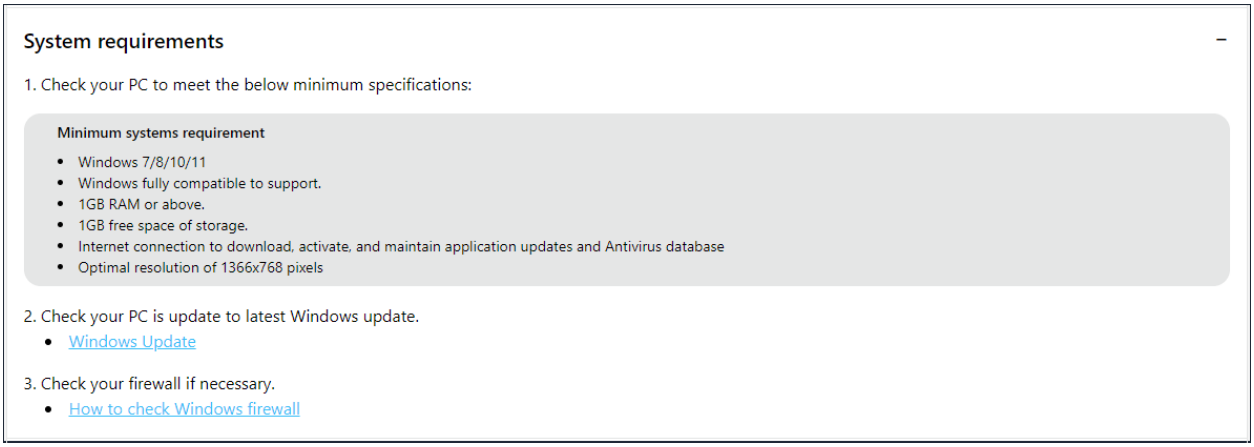
- **User Guides**: User can read about how to install and use CYSECA Home Edition
- **Frequently Ask Question**: User can explore on what is the common questions about CYSECA Home Edition
- **Forum**: User can access forum to report bugs, request new features and interact with other users
- **Download**: User can download installer of CYSECA Home Edition
- **Talk to Us**: User can call CYSECA operator for assistance
- **Send Us An Email**: User can email to support@cyseca.com.my for any inquiries

- **Join the community**: User can access the forum for discussing and sharing about CYSECA Home Edition

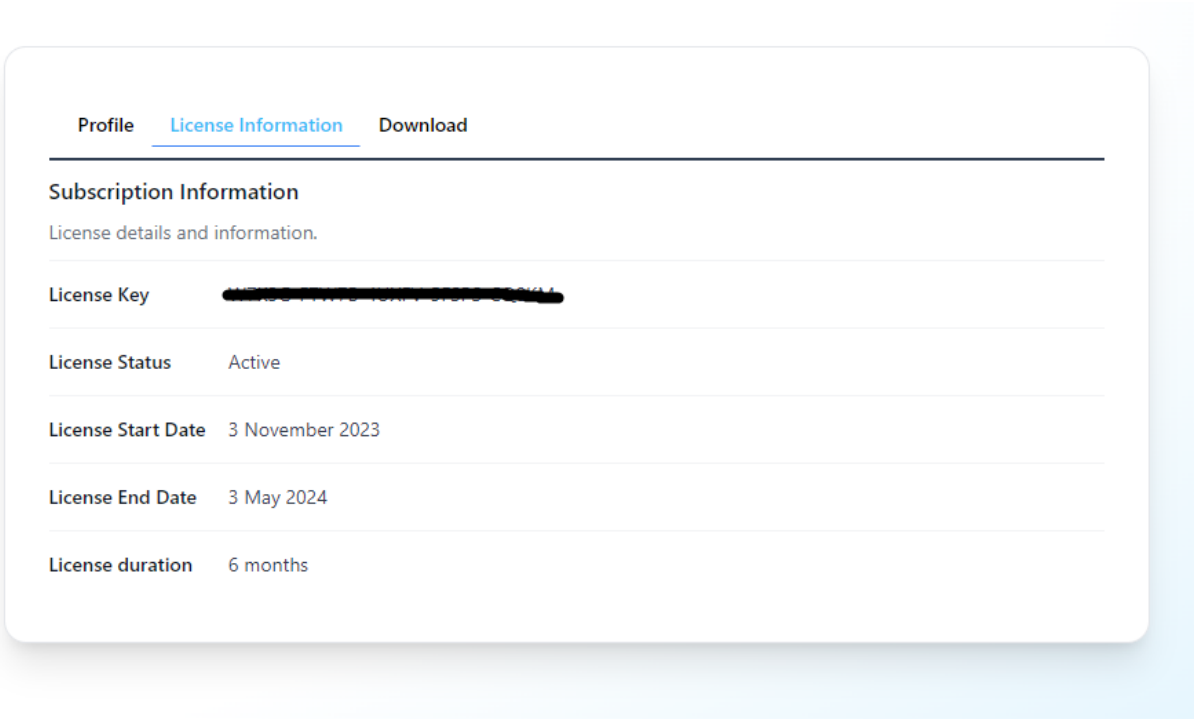
For downloading installer, click on the download button. Choose between 32-bit operating system and 64-bit operating system and click download. Figure below shows the download page.



User can also check system requirements, which is shown in the next figure.

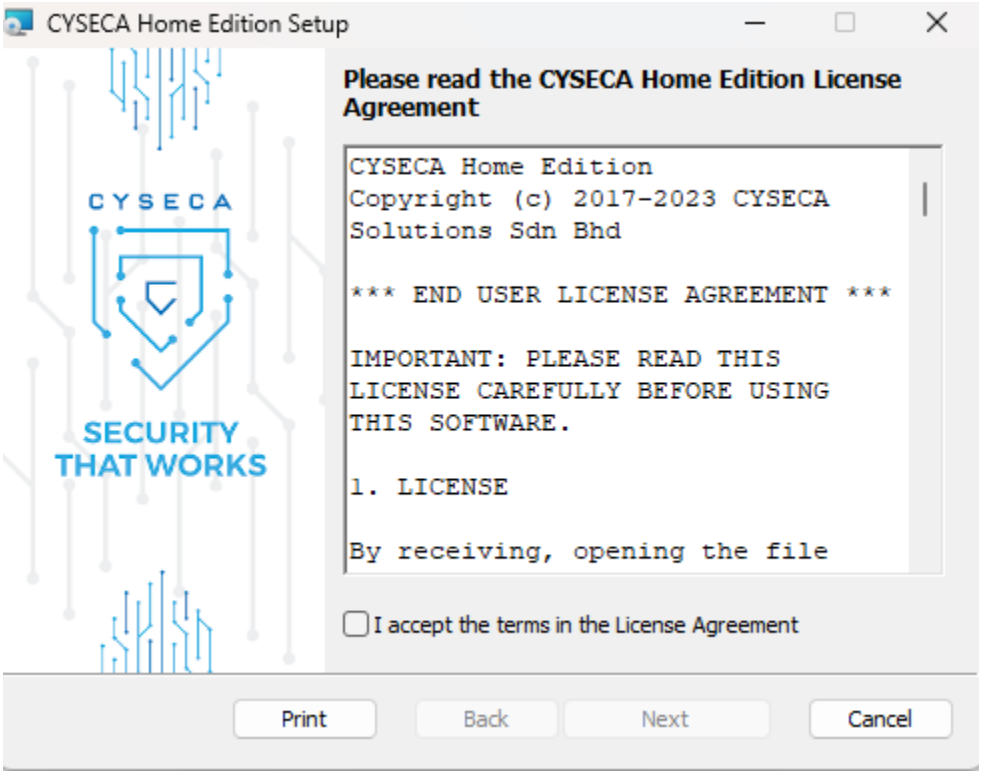


Do not forget to copy license key since the key will be needed during installation process. Figure below shows license key page. Note that license key can be obtained from the license key page or email sent after successful account activation.

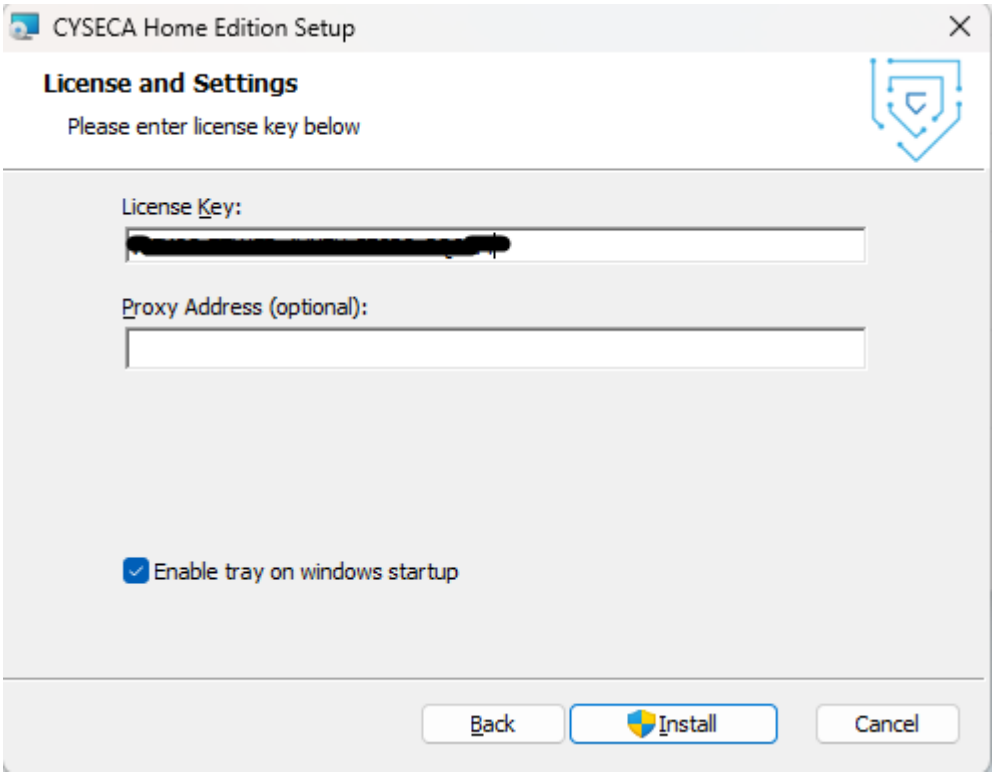


Installation

Installing CYSECA Home Edition is easy and fast. The following figures shows the installation process.

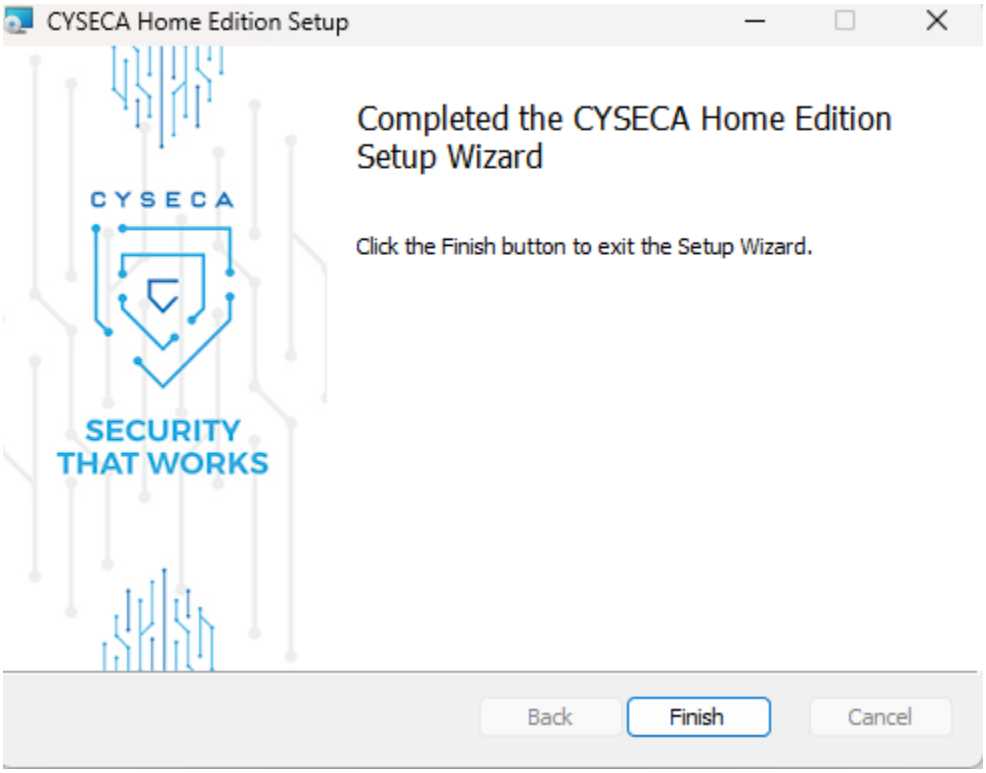


Accept the terms in the License Agreement and click “Next”.



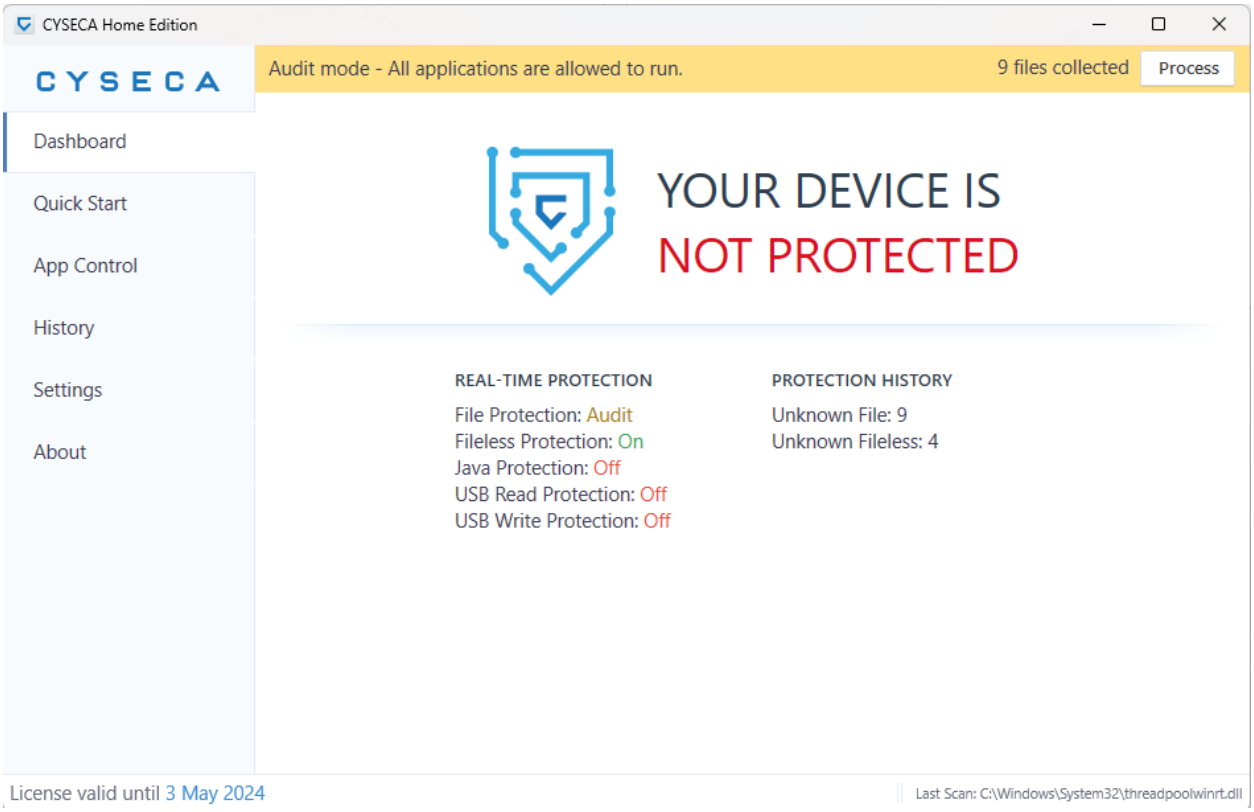
Enter the license key. If proxy is available, user can enter the proxy address. CYSECA Tray can be enabled/disabled during startup. However, it is recommended to enable CYSECA tray. It is also compulsory to have internet connection during and after the installation process, for activating license and downloading whitelist rules.

Figure below shows completed installation process.

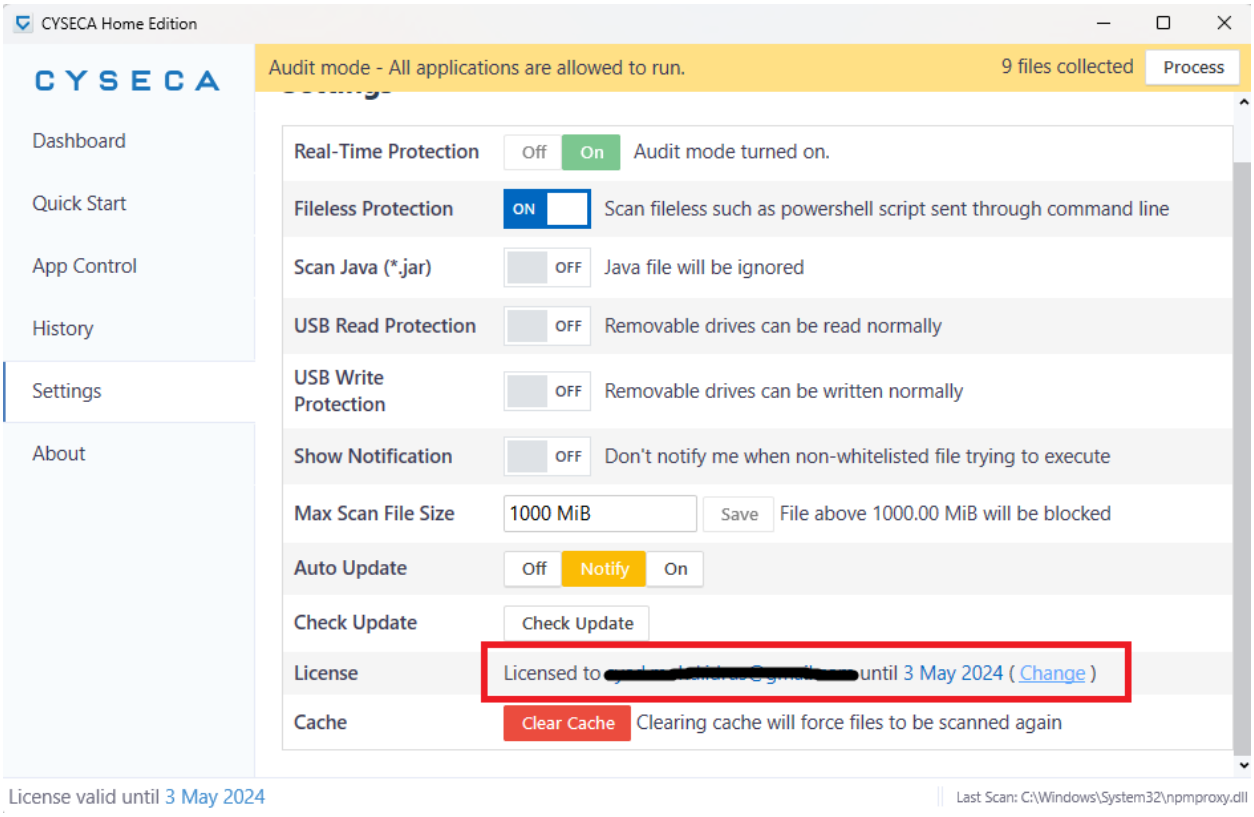


CYSECA Home Edition Dashboard

Figure below shows CYSECA Home Edition Dashboard. From there, user can see protection status, protection history, license validity, audit mode process and also last scan file.



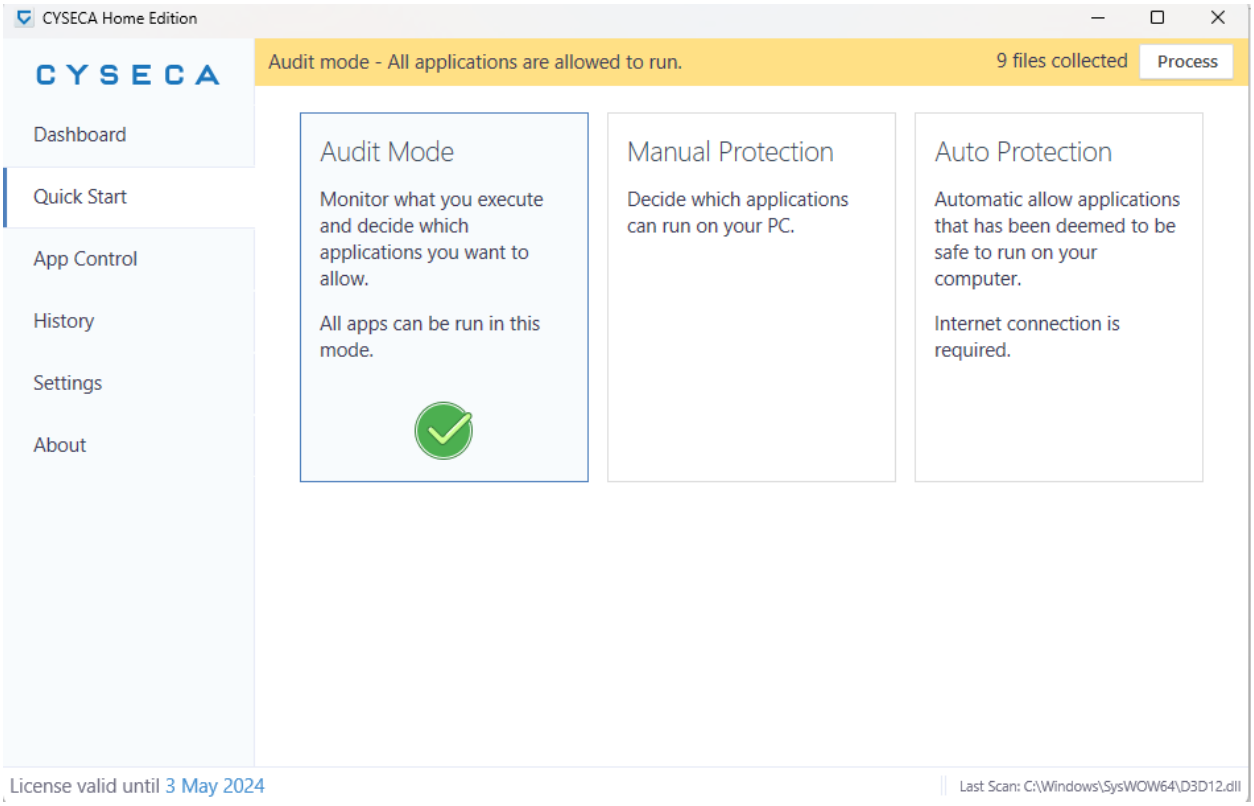
To check the license information, click on Settings, as shown in the figure below.



Quick Start

In the Quick Start, user can select which protection mode they wanted to use. There are three (3) protection mode available:

- Audit Mode - Monitor what the user executes, and the executed application will be listed. In this mode, all application will be allowed. The user can also add the executed application during audit mode into a new custom application
- Manual Protection – The user decide which application can be run on the pc. User will be redirected to rules page if the option is selected. The application in the rules page is fetched from CYSECA Server.
- Auto Protection – Automatically allow applications that has been deemed safe to run on user computer.

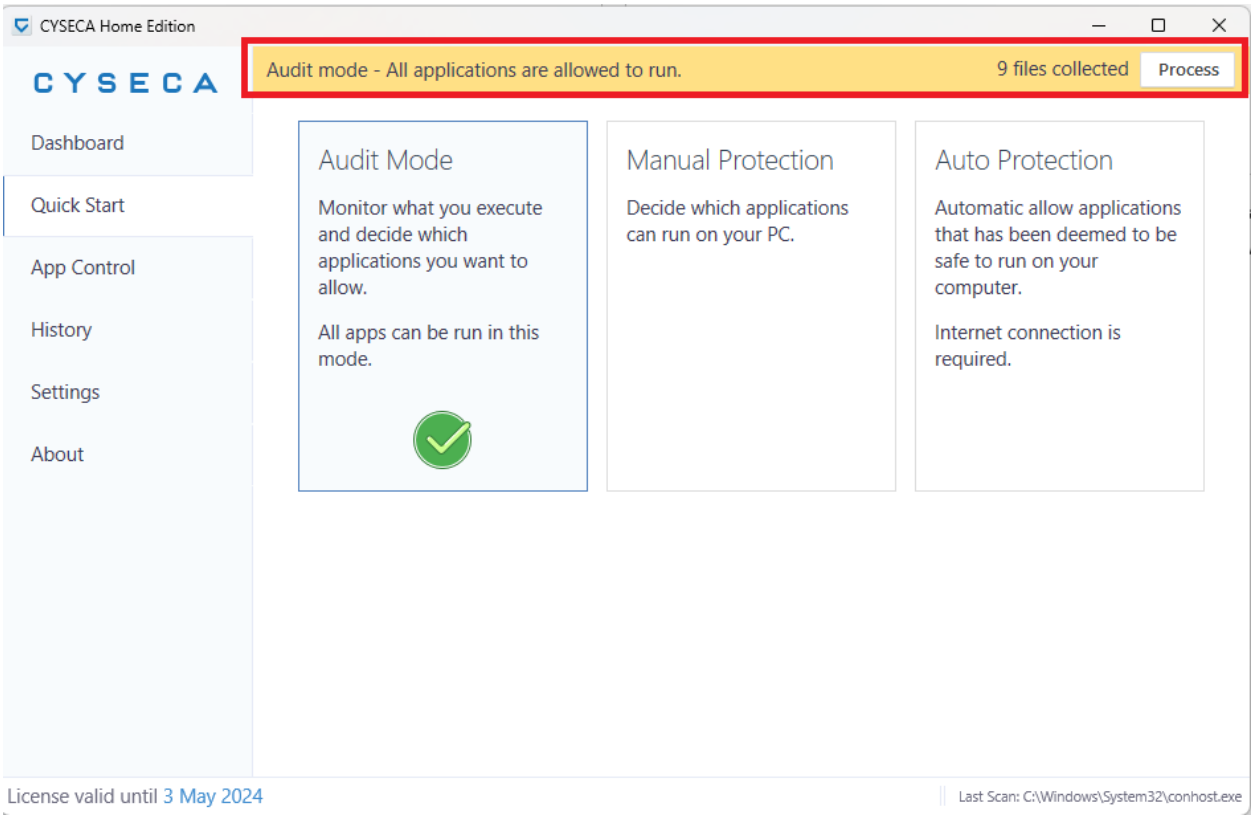

CYSECA Home Edition
CYSECA
Audit mode - All applications are allowed to run.
9 files collected
Process
Dashboard
Quick Start
App Control
History
Settings
About
Audit Mode
Monitor what you execute and decide which applications you want to allow.
All apps can be run in this mode.
Manual Protection
Decide which applications can run on your PC.
Auto Protection
Automatic allow applications that has been deemed to be safe to run on your computer.
Internet connection is required.
License valid until 3 May 2024
Last Scan: C:\Windows\SysWOW64\D3D12.dll

Audit Mode

Audit mode enables user to execute all application. User can process the recorded application execution and store them in custom application. Note that **execution logs will not be updated during audit mode**.

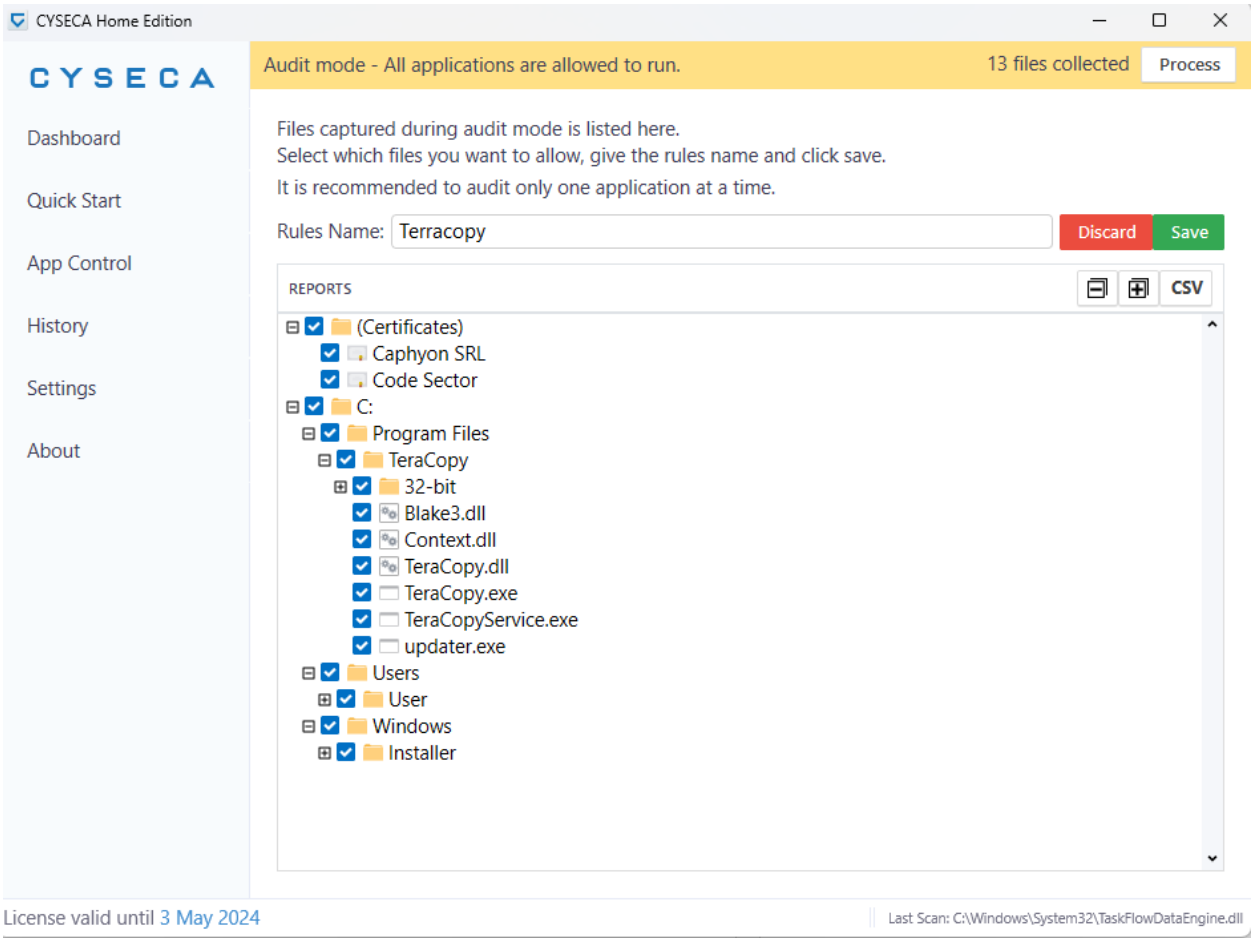
Steps to add application to a new custom application is as follows:

1. Select Audit Mode



The highlighted text box above reminds user that in audit mode, execution of files will be recorded, and the user can manually decide whether to add or not the files recorded in custom application rules.

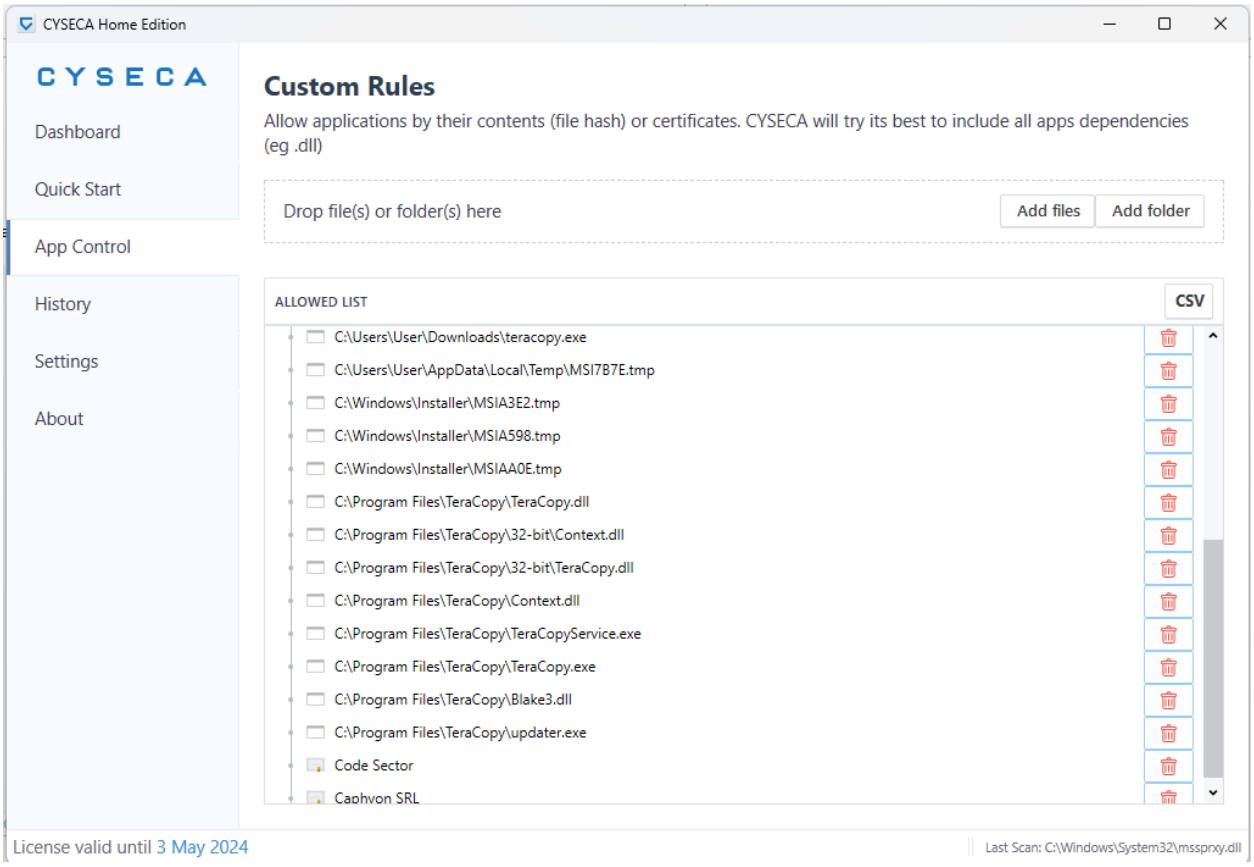
2. Execute any application



For this scenario, TeraCopy was used as unknown file to be added into custom rule. When the user clicks on Process button on the right of the user interface, the above menu will appear. Rules name can be changed, and **please click on the "Save" button to make sure the rules recorded is saved by CYSECA**. The application will be shown in tree view, and there may be some unintended execution of application during this process. User can untick the application to exclude from the rule. User can also export the list as csv.

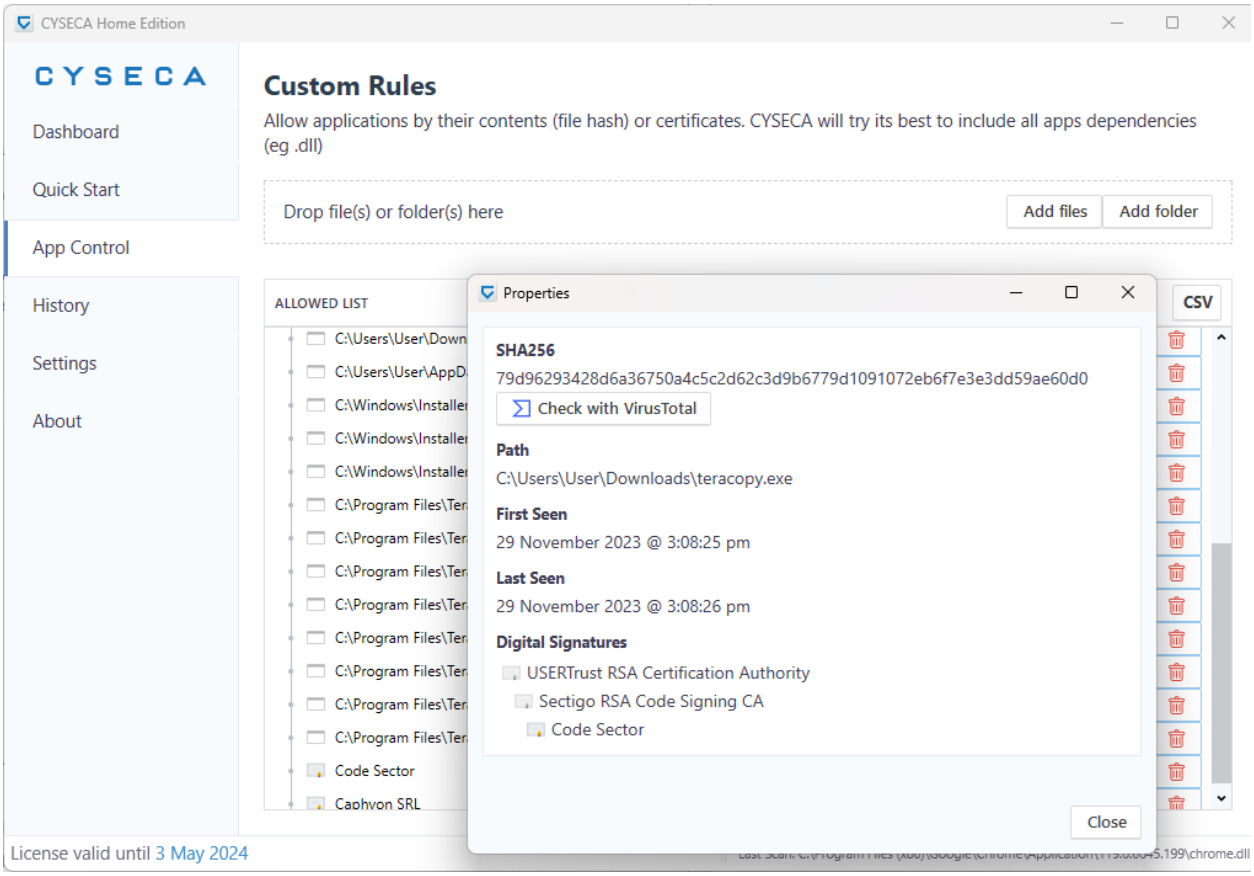
3. Save and editing custom rules

Saved rules can be edited and viewed by user. The menu is shown below:



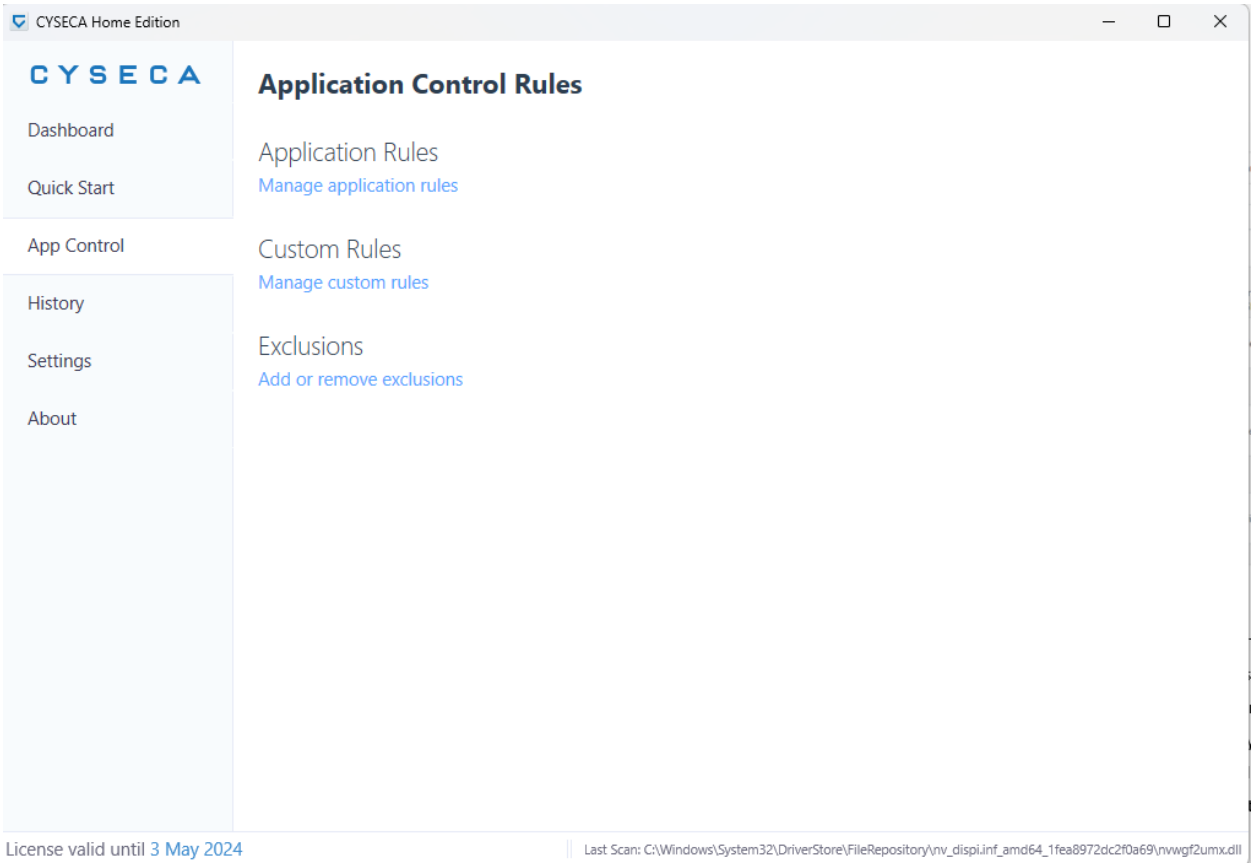
User can add files, folders and delete added folders which are whitelisted. Saved rules from audit mode will also appear here, as from the name saved in step (2). User can also export the rules as csv.

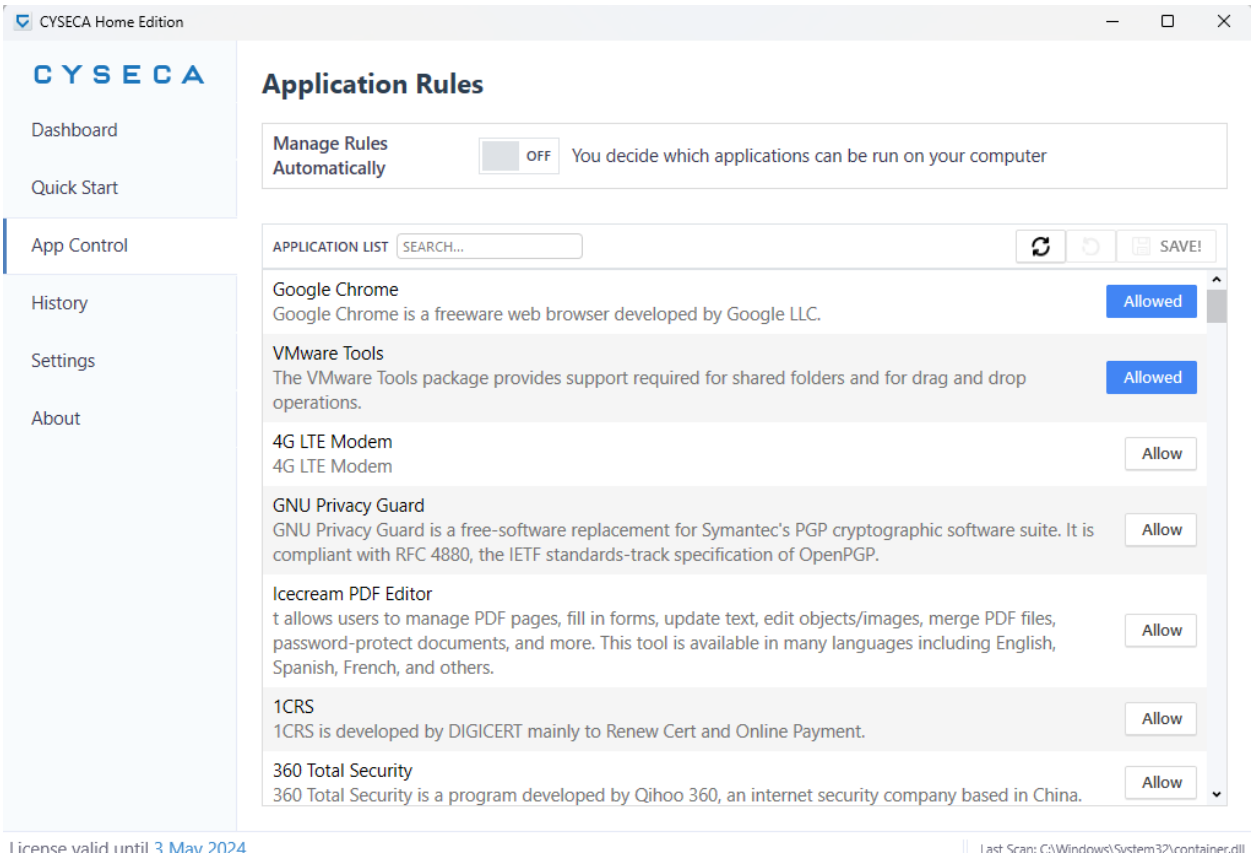
User can also view file and certificate information, and also check the file whether it is safe or not with VirusTotal. VirusTotal is a webpage where user can search and upload file information to check whether the file is safe for use or not. VirusTotal is trusted by many parties and organization as one of the best place to identify safe and malicious files.



App Control (Application Rules)

Application rules is a page where user can manage rules to be allowed by CYSECA. Application rules can only be used if Manual Protection is selected. By default, Manual Protection will block all application other than application that has been allowed to run. Figure below shows the Application Control Menu.





User can search, allow, disallow and refresh the rules list. If the “Manage Rules Automatically” button is turned on, auto-protection mode will be selected, and these rules will all be allowed automatically. If the user wanted to allow a rule, for example, Notepad++, user can search and click on allow. Don’t forget to save otherwise Notepad++ will not be allowed. Once allowed and saved, Notepad++ will can be executed.

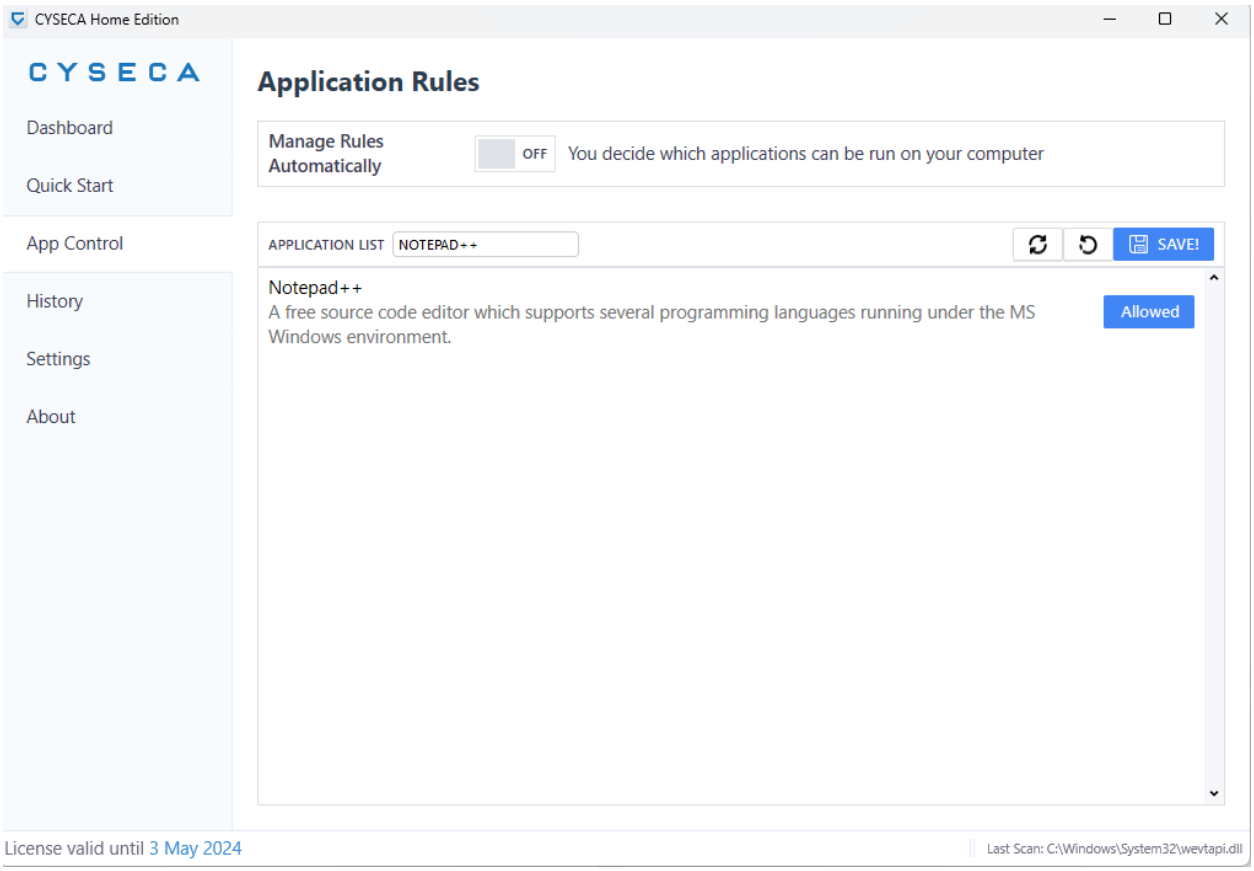
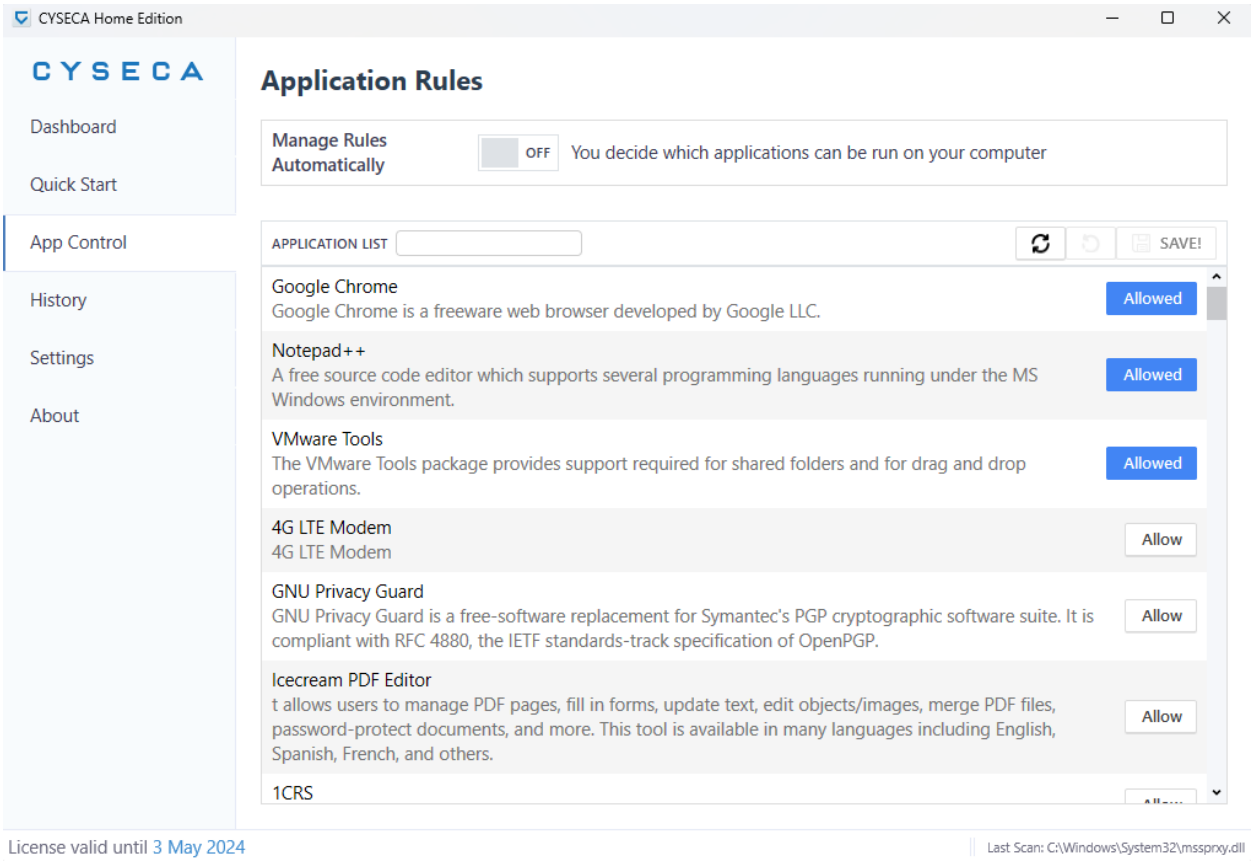
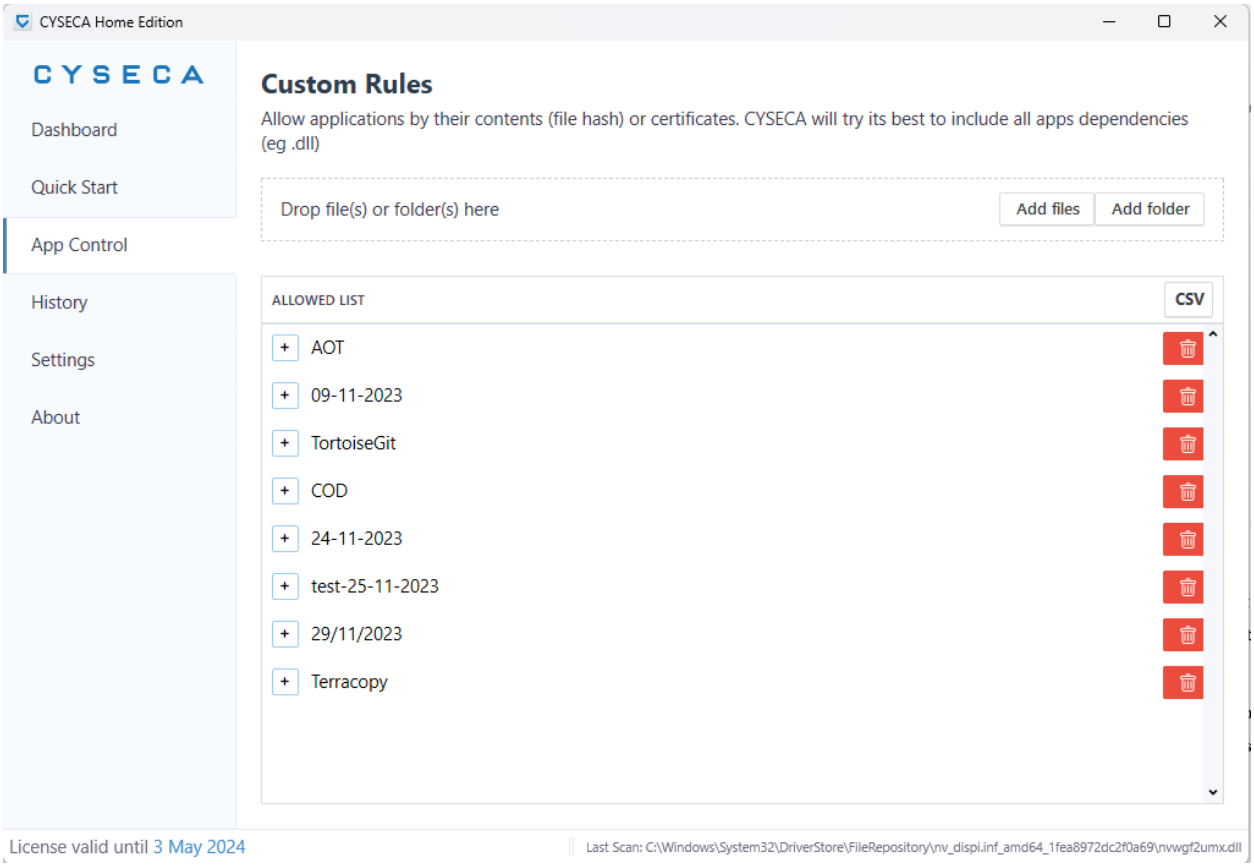


Figure above shows searching and allowing Notepad++.



Based on figure above, it is shown that only 3 application were allowed, which are Google Chrome, Notepad++ and VMware Tools. This shows that only the 3 application can be executed. Other application will be blocked.

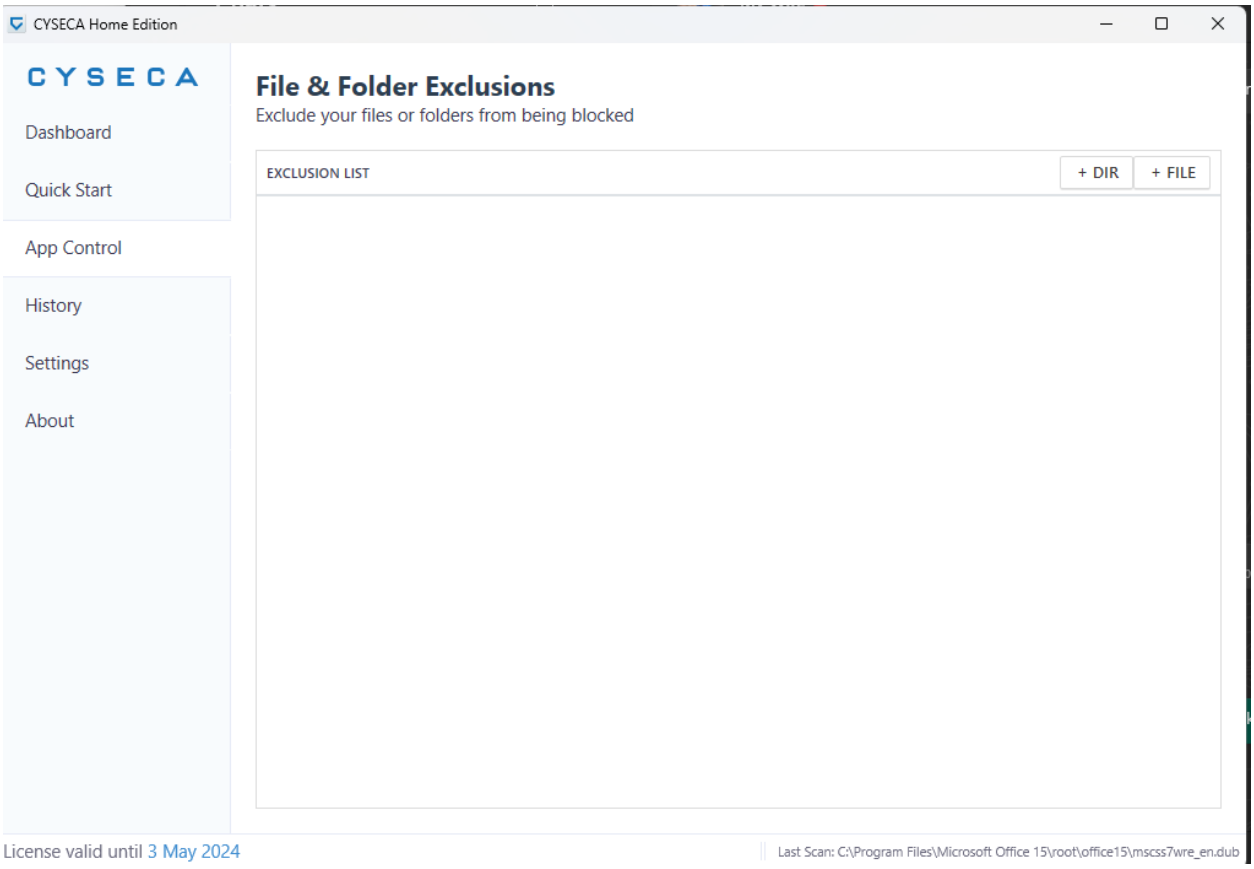
Custom Rules



Custom Rules is a page where user can add application manually. This can be done by clicking on “Add Files” or “Add Folder” button. User can also drag and drop application into the label “Drop files/folder here”. User can also view added files, delete and export the files as csv.

Exclusions

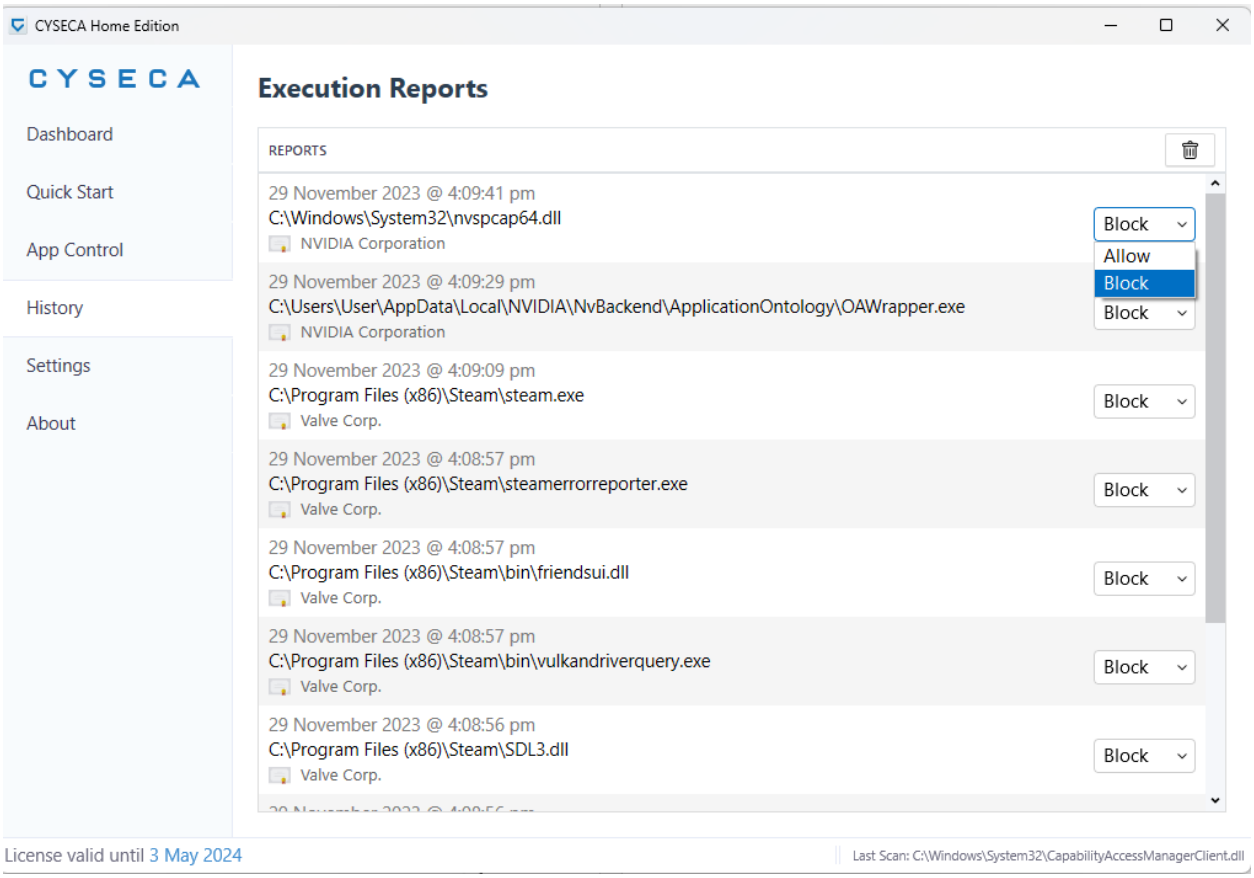
User can exclude application from being scanned by CYSECA. Note that CYSECA will totally ignore the files, so please do not exclude malicious application. Figure below shows exclusion page.



User can either exclude file or folder. To exclude folder, click on “+DIR” button and to exclude file, click on “+File Button”.

History (Execution Logs)

Execution log displays all the execution of PE in the agent. User can view, block and allow any file scanned by CYSECA. User can also check file information from the log. Figure below shows the execution logs as well as file information.



User can click on the dropdown to Allow/Block the application.

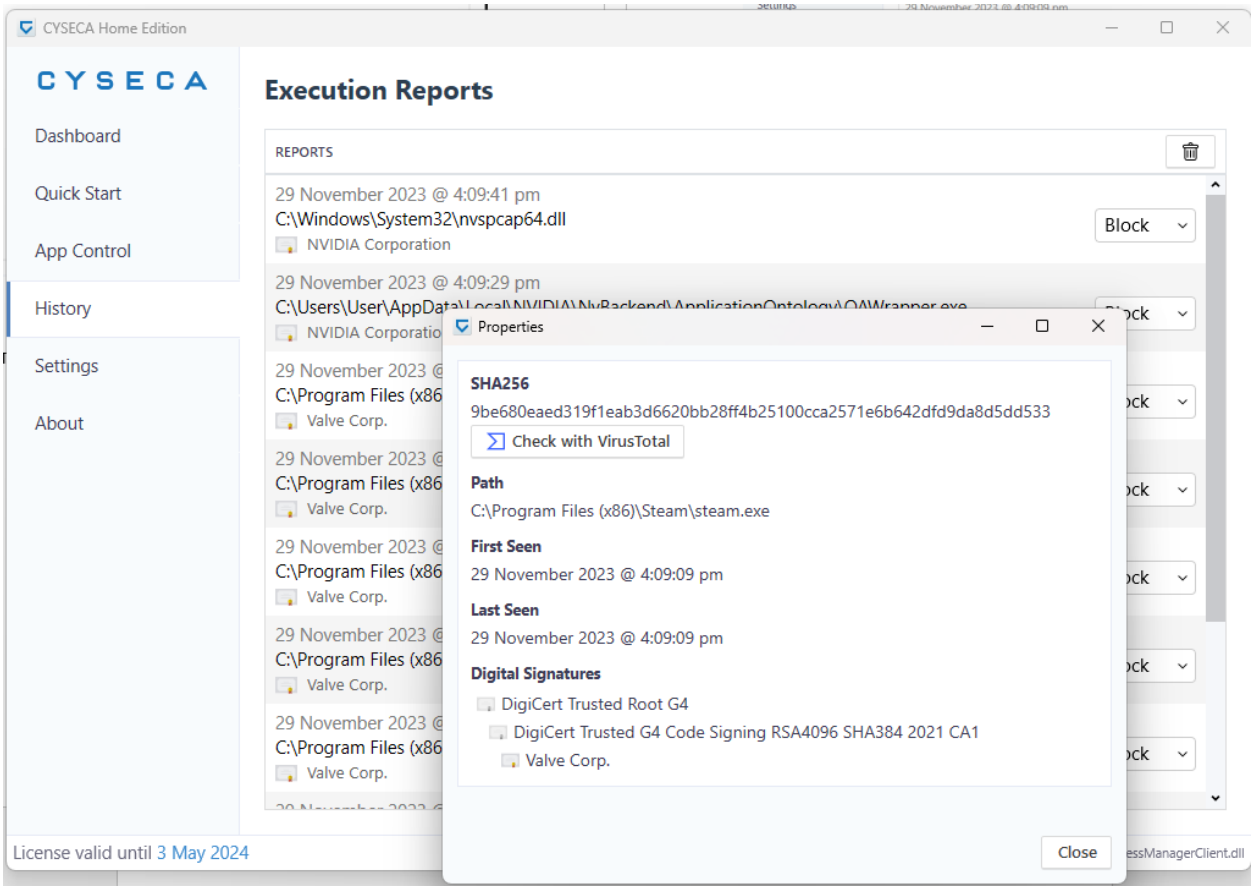


Figure above shows file information from execution logs.

History (Fileless Log)

Fileless log will display all the execution of scripts/commands in the agent. Note that this will only display pure fileless script. Execution of .vbs, .py, and .ps1 will be shown in file execution logs

What is fileless threats?

Fileless threat is a type of threat that does not come in form of file, instead, it uses memory to store its command. Fileless can come in three types, which are:

i. Type 1: No activity performed

A fully fileless malware can be considered one that never requires writing a file on the disk. A compromised device may also have malicious code hiding in device firmware (such as a BIOS), a USB peripheral (like the BadUSB attack), or in the firmware of a network card. All these examples do not require a file on the disk to run and can theoretically live only in memory. The malicious code would survive reboots, disk reformats, and OS reinstalls. Infections of this type can be particularly difficult to detect because most antivirus products do not have the capability to inspect firmware. In cases where a product does have the ability to inspect and detect malicious firmware, there are still significant challenges associated with remediation of threats at this level. This type of fileless malware requires high levels of sophistication and often depends on hardware or software configuration. It is not an attack vector that can be exploited easily and reliably. While dangerous, threats of this type are uncommon and not practical for most attacks.

ii. Type 2: Indirect file activity

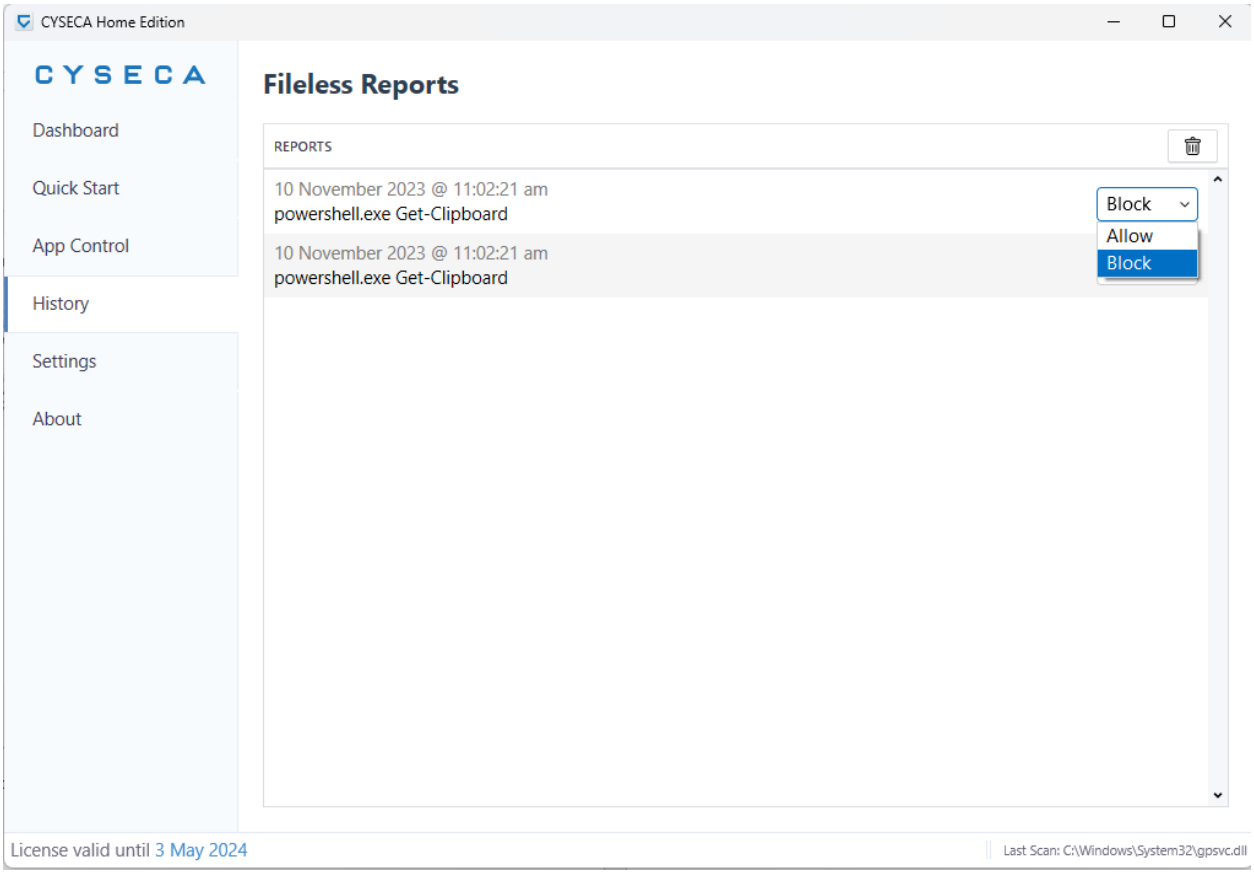
There are other ways that malware can achieve fileless presence on a machine without requiring significant engineering effort. Fileless malware of this type does not directly write files on the file system, but they can end up using files indirectly. This can be considered as

common attack type, which is the attacker uses legitimate command/scripts which were whitelisted by windows, such as Powershell, mshta, regsvr32 and wscript/script.

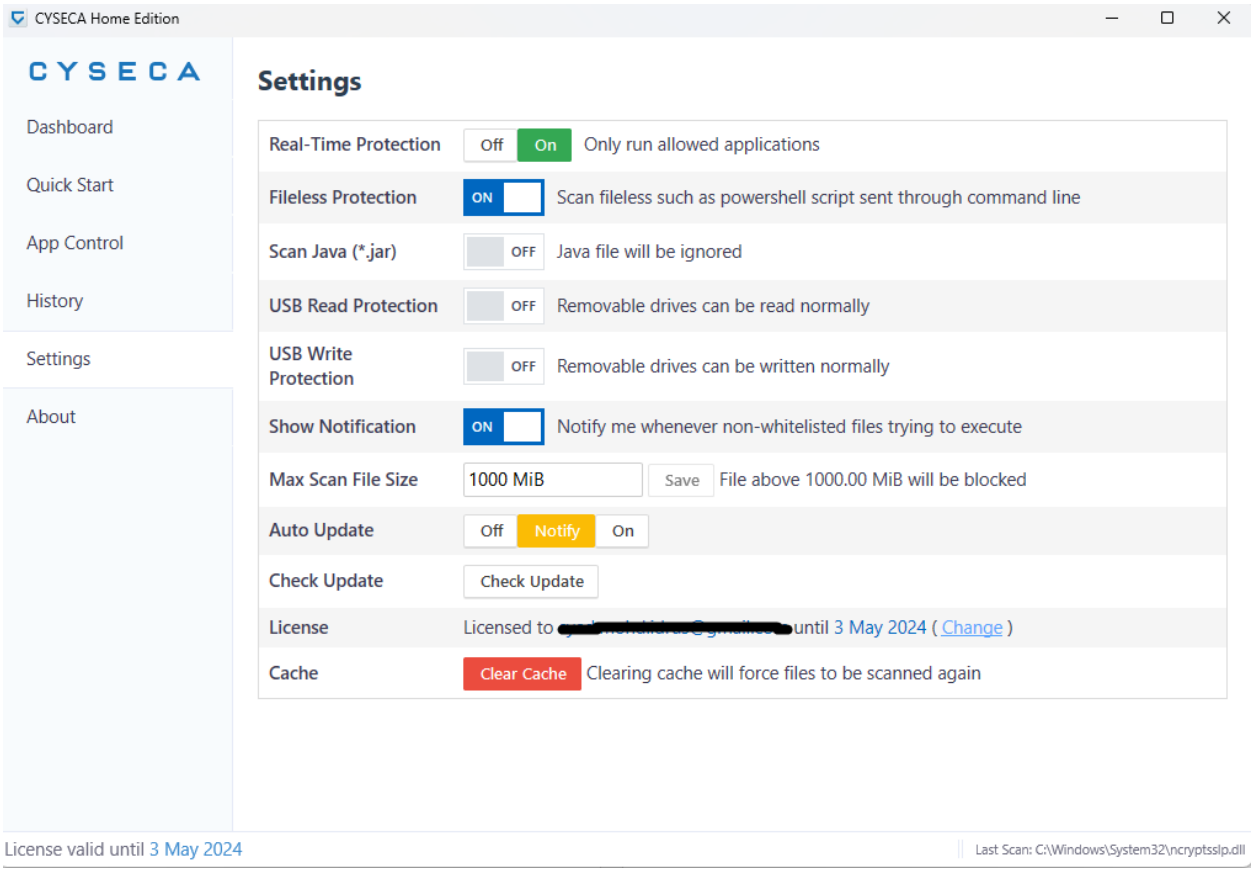
iii. Type 3: Files required to operate

Some malwares can have a sort of fileless persistence, but not without using files to operate. This type of attack will set certain verb/keyword which will be invoked by the script to open malicious command through legitimate Windows Shell command, such as mshta or wscript.

Figure below shows fileless log.



Settings

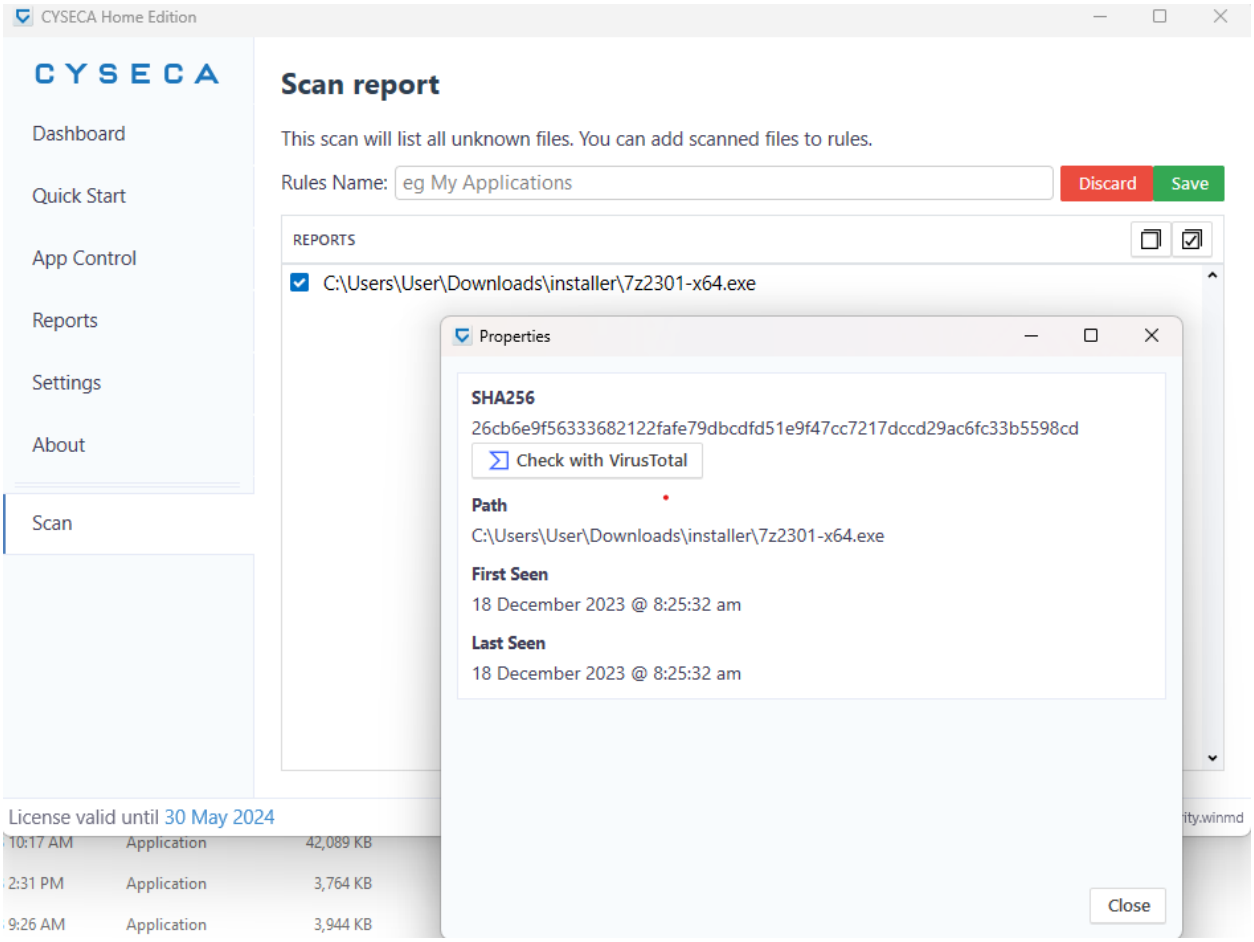


- **Real-Time Protection**: This can be toggled, for off, agent will not scan any execution of file. If on, agent will scan and log execution of file.
- **Fileless Protection**: If this is on, execution of fileless will be scanned.
- **Scan Java**: This is for java files. If enabled, agent will scan java files, and if not whitelisted, the java file will be blocked.
- **USB Read Protection**: For USB Read Protection, if enabled, user pc will block any read attempt from USB devices.
- **USB Write Protection**: For USB Write Protection, if enabled, user pc will block any write attempt from USB devices.
- **Show Notification**: If enabled, agent will show tray at user pc if any unknown file is executed.

- **Max Scan File Size**: User can set manually max file size for CYSECA to scan. According to the figure, max scan size is 1GB. This shows that CYSECA will only scan file which is less than 1GB.
- **Auto-Update**: If turned on, agent will automatically update to the latest if available. If Notify is selected, CYSECA will notify user that there is a new version available, and user will have to update manually. If off, CYSECA will not update agent to the latest if updates are available.
- **Check Update**: User can click on this button to check updates manually
- **License**: This shows license information
- **Clear Cache**: This will clean all recently files scanned by CYSECA from cache.

Scan With CYSECA

User can scan file/folder manually by using CYSECA. To perform this action, right click on any file/folder and click on “Scan with CYSECA”. Scan duration varies according to the size of the application. Results of scan will be displayed in CYSECA Home Edition UI. Figure below shows the result of the scan.



User can check the file with Virustotal. User can also Save/Discard the file. Saved file will be displayed on Custom Rules.

Example of Protected Device shown in UI