SecureAPlus

User Guide

Version 3.4

September 2015

Copyright Information

Information in this document is subject to change without notice. Companies, names and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the written permission of SecureAge Technology Pte Ltd.

Table of Contents

1 About SecureAPlus

SecureAge SecureAPlus combines application whitelisting and antivirus components to protect your computer from known and unknown malware more effectively. It scans and removes known malware like viruses, Trojan Horses and worms just like any other conventional antivirus – but better. It does what other conventional antivirus cannot do – it can block any new and advanced malware regardless of how they try to evade detection. It even alerts you when risky programs are attempting to run to prevent any accidental installation that potentially can harm your computer. Hence, SecureAge SecureAPlus is the next generation antivirus that truly protects your computer without taking any chance.

This guide is designed for end-users of SecureAPlus software who are new to SecureAPlus or who want to learn more about SecureAPlus. All features available in SecureAPlus are included in this guide.

Note:

- This user guide is published based on Windows 7 environment.

Installation, uninstallation of SecureAPlus will not be covered in this user guide but can be found in the following SecureAPlus guides:

- SecureAPlus Installation Guide
- SecureAPlus Uninstallation Guide

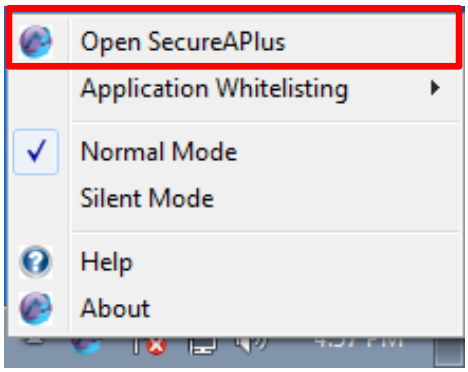
2 Getting Started

2.1 Starting SecureAPlus Software

The SecureAPlus software will start when you logon to your Windows. When SecureAPlus is running, it appears as an icon in the System Tray, located at the bottom-right corner of your Windows screen.

To navigate to the SecureAPlus Main console, follow the steps below:

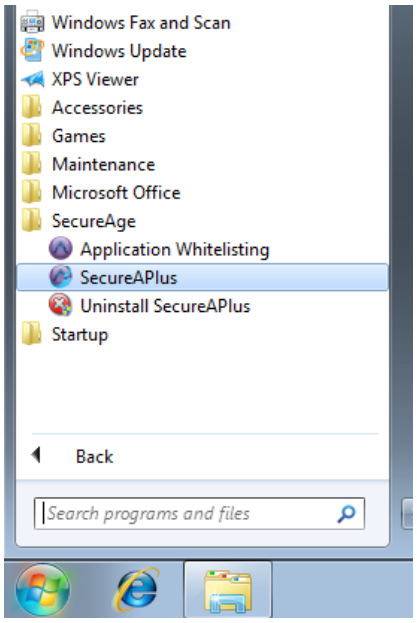
- Right click on **SecureAPlus** tray icon, click on **SecureAPlus** on the menu.



- Alternatively, you can also left click on the **SecureAPlus** tray icon to launch the **SecureAPlus Main Console**.

If SecureAPlus does not launch during Windows start up, starting SecureAPlus involves the following steps:

- Click **Start**, point to **All Programs**. Click on **SecureAge** and click on **SecureAPlus** to launch SecureAPlus.

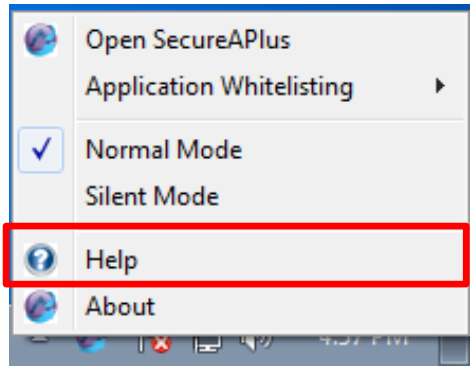


The SecureAPlus Main Console will launch.

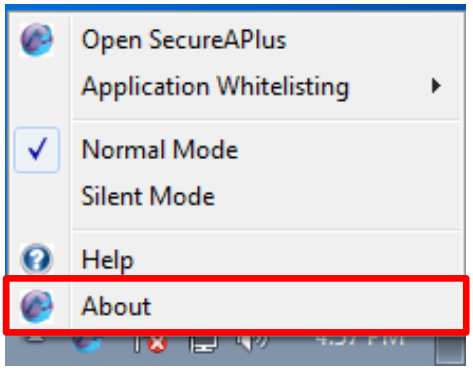
2.2 SecureAPlus Tray Icon Menu

To navigate the right click menu of SecureAPlus tray icon, follow the steps as below:

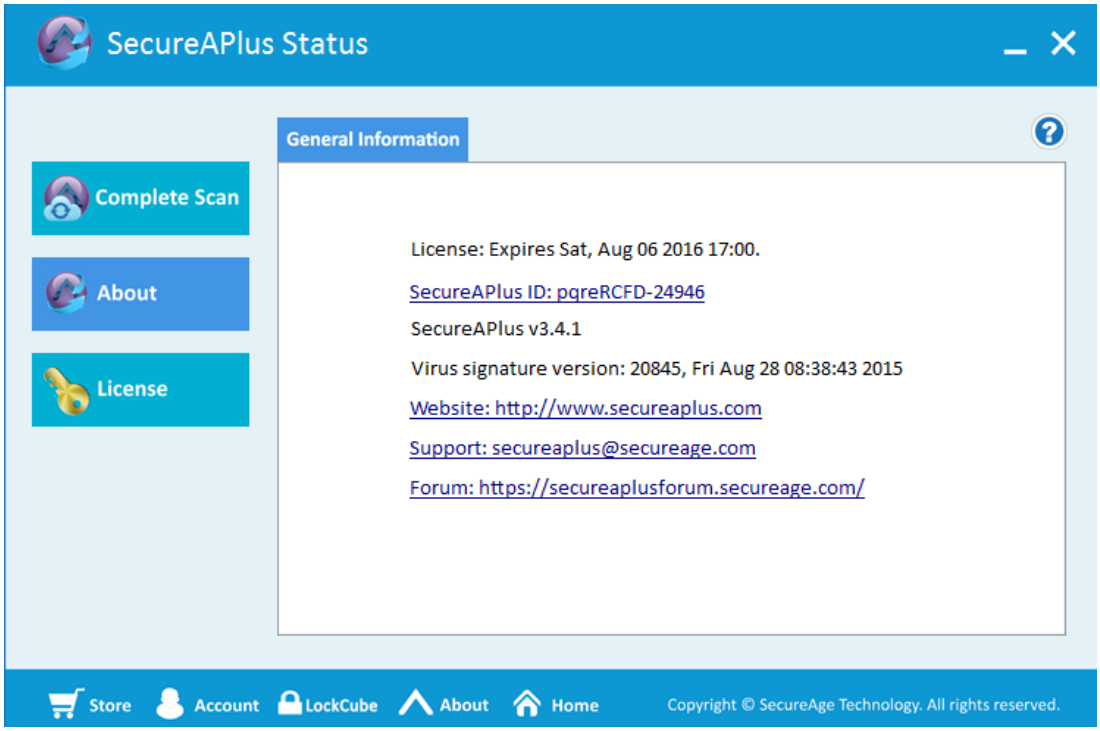
- Right click on **SecureAPlus** tray icon, click on **Help** on the menu, it will launch the SecureAPlus user guide using the default pdf reader.



- Right click on **SecureAPlus** tray icon and click on **About** on the menu.



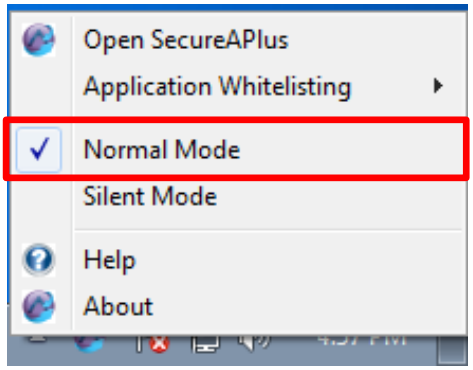
- The **General Information** about the **SecureAPlus Status** will be displayed as shown below.



2.2.1 Normal Mode

To switch SecureAPlus to Normal Mode, follow the step as below:

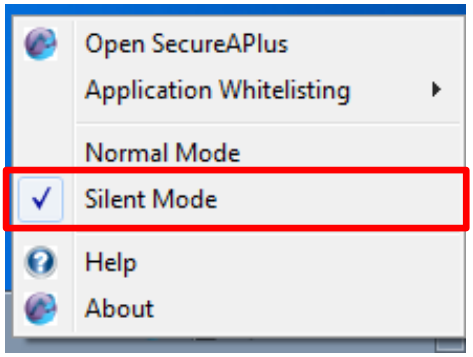
- Right click on **SecureAPlus** tray icon, select **Normal Mode**.



2.2.2 Silent Mode

To switch SecureAPlus to Silent Mode, follow the step as below:

- Right click on **SecureAPlus** tray icon, select **Silent Mode**.



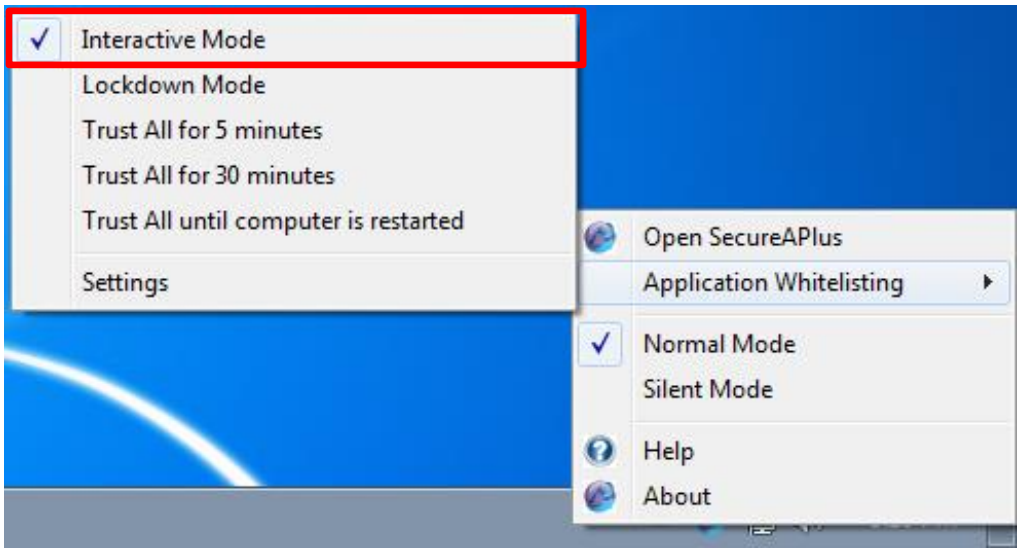
Note:

- When SecureAPlus is in Silent Mode:
  - Application whitelisting will block untrusted applications from running without any prompt.
  - Real-time scanning will automatically quarantine any detected threat without prompting.
- Silent Mode will be automatically switched to Normal Mode when the user clicked on Complete Scan icon located in the **SecureAPlus** main console window.

2.2.3 Interactive Mode

To turn SecureAPlus to Interactive Mode, follow the steps below:

- Right click on **SecureAPlus** tray icon, click on **Application Whitelisting** on the menu and select **Interactive Mode**.



- The SecureAPlus icon in the system tray will change to the normal icon to indicate that SecureAPlus is currently in the Interactive Mode.

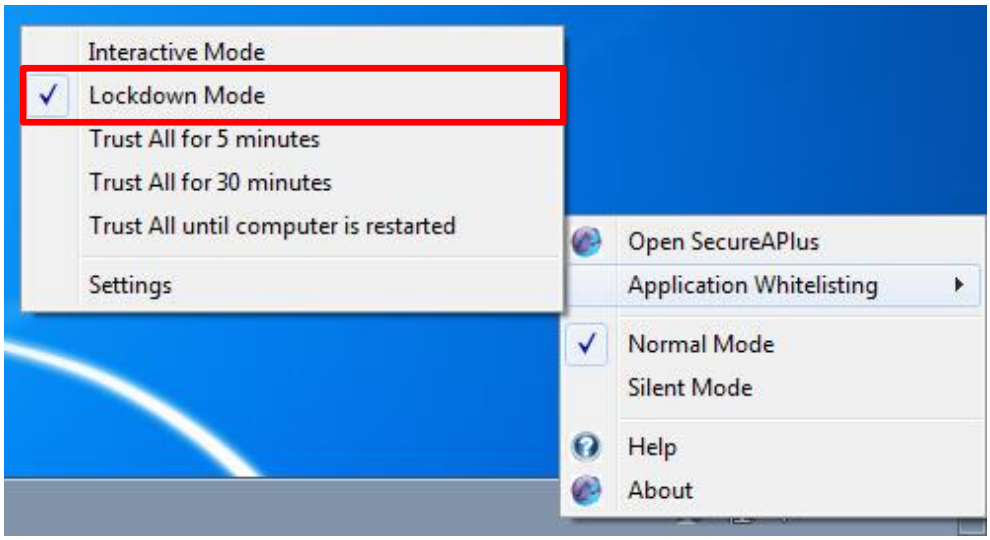
Note:

- When SecureAPlus is in the Interactive Mode, it will have more interactions with users by prompting them for further actions by Application Whitelisting such as whether to allow an untrusted file to execute and etc.
- This corresponds to selecting the modes via the SecureAPlus Main Console (**Section 3.8 – Application Whitelisting Modes**).

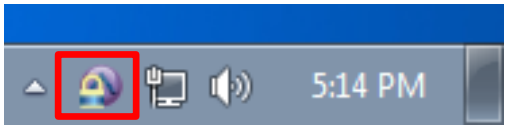
2.2.4 Lockdown Mode

To turn SecureAPlus to Lockdown Mode, follow the steps below:

- Right click on **SecureAPlus** tray icon, click on **Application Whitelisting** on the menu and select **Lockdown Mode**.



- The SecureAPlus icon in the system tray will change to the lockdown icon to indicate that SecureAPlus is currently in the Lockdown Mode.



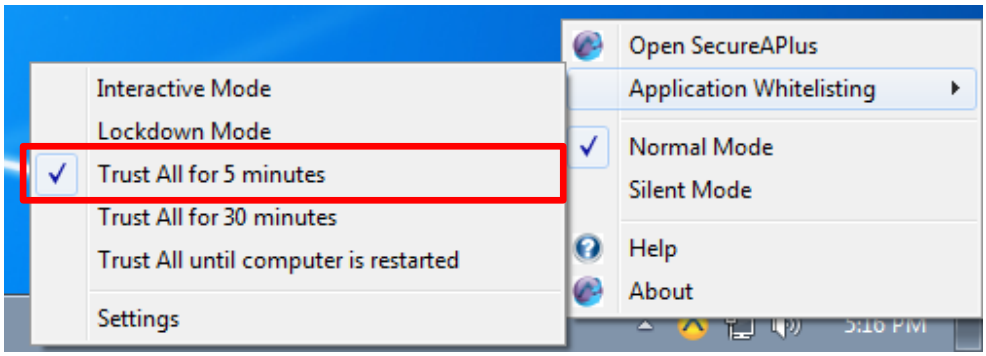
Note:

- When SecureAPlus is in the Lockdown Mode, any untrusted files which try to execute will be blocked straight away without any prompting by Application Whitelisting for further actions from user.
- This corresponds to selecting the modes via the SecureAPlus Main Console (**Section 3.8 – Application Whitelisting Modes**).

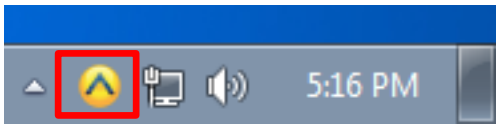
2.2.5 Trust All for 5 minutes

To turn SecureAPlus to **Trust All for 5 minutes** mode, follow the steps below:

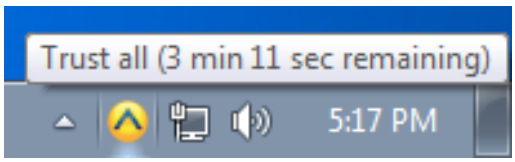
- Right click on **SecureAPlus** tray icon, click on **Application Whitelisting** on the menu and select **Trust All for 5 minutes**.



- The SecureAPlus icon in the system tray will change to a gold icon to indicate that SecureAPlus is currently in the limited trusting time period.



- When you do a mouse-over the SecureAPlus icon, it will show how much time left for trust all.



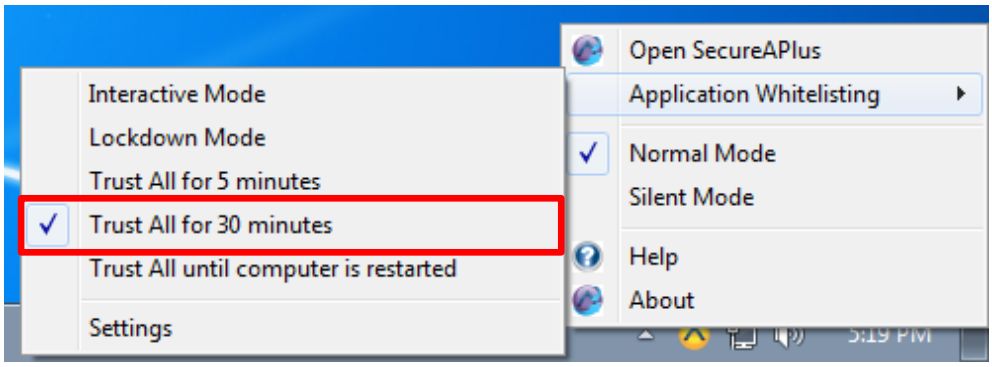
Note:

- When SecureAPlus is in the **Trust All for 5 minutes** mode, any untrusted files which try to execute within the 5 minutes will be trusted without any prompting by Application Whitelisting for further actions from user.
- After 5 minutes is up, it will switch back to the mode that SecureAPlus is previously in. For example, if it is in Interactive Mode before changing to Trust All for 5 minutes, it will switch back to Interactive Mode after 5 minutes. Likewise if it is in Lockdown mode previously.
- This corresponds to selecting the modes via the SecureAPlus Main Console (**Section 3.8 – Application Whitelisting Modes**).

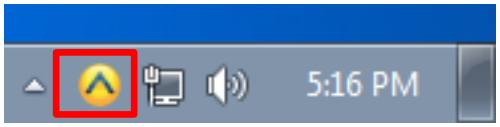
2.2.6 Trust All for 30 minutes

To turn SecureAPlus to **Trust All for 30 minutes** mode, follow the steps below:

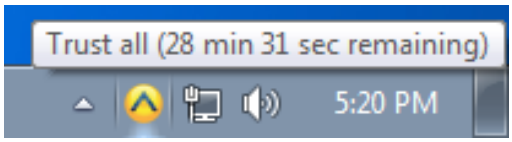
- Right click on **SecureAPlus** tray icon, click on **Application Whitelisting** on the menu and select **Trust All for 30 minutes**.



- The SecureAPlus icon in the system tray will change to a gold icon to indicate that SecureAPlus is currently in the limited trusting time period.



- When you do a mouse-over the SecureAPlus icon, it will show how much time left for trust all.



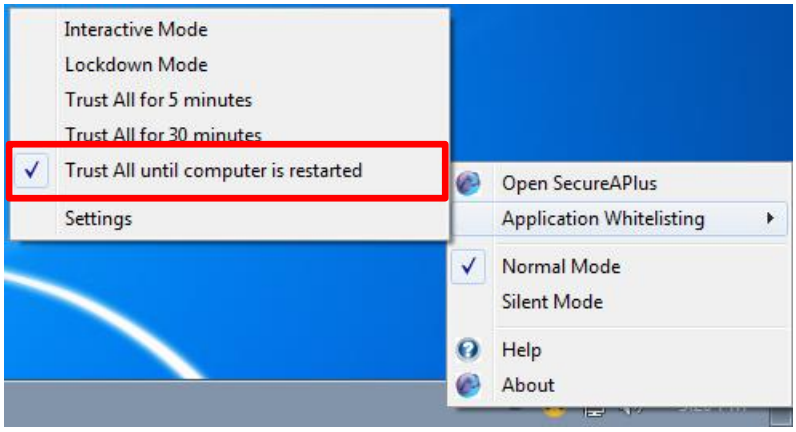
Note:

- When SecureAPlus is in the **Trust All for 30 minutes** mode, any untrusted files which try to execute within the 30 minutes will be trusted without any prompting by Application Whitelisting for further actions from user.
- After 30 minutes is up, it will switch back to the mode that SecureAPlus is previously in. For example, if it is in Interactive Mode before changing to Trust All for 30 minutes, it will switch back to Interactive Mode after 30 minutes. Likewise if it is in Lockdown mode previously.
- This corresponds to selecting the modes via the SecureAPlus Main Console (**Section 3.8 – Application Whitelisting Modes**).

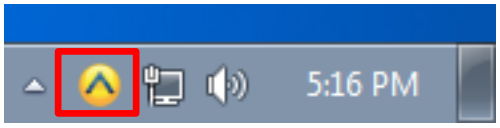
2.2.7 Trust All until computer is restarted

To turn SecureAPlus to **Trust All until computer is restarted** mode, follow the steps below:

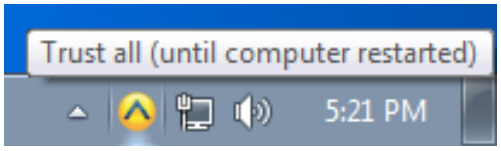
- Right click on **SecureAPlus** tray icon, click on **Application Whitelisting** on the menu and select **Trust All until computer is restarted**.



- The SecureAPlus icon in the system tray will change to a gold icon to indicate that SecureAPlus is currently in the limited trusting time period.



- When you do a mouse-over the SecureAPlus icon, it will show that it will trust all until computer restarted.



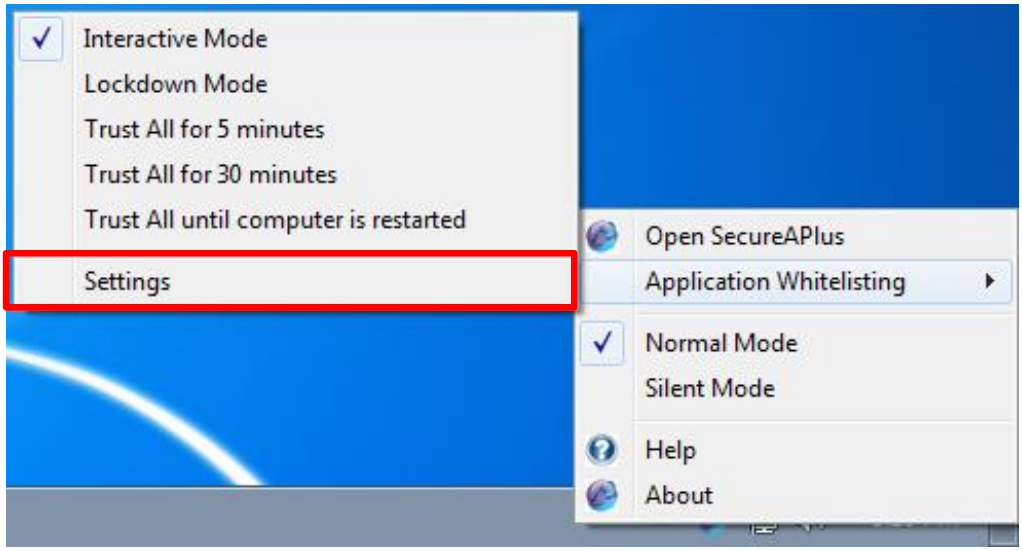
Note:

- When SecureAPlus is in the **Trust All until computer is restarted** mode, any untrusted files which try to execute will be trusted without any prompting by Application Whitelisting for further actions from user.
- After the computer restarted, it will switch back to the mode that SecureAPlus is previously in. For example, if it is in Interactive Mode before changing to Trust All until computer is restarted, it will switch back to Interactive Mode after computer restarted. Likewise if it is in Lockdown mode previously.
- This corresponds to selecting the modes via the SecureAPlus Main Console (**Section 3.8 – Application Whitelisting Modes**).

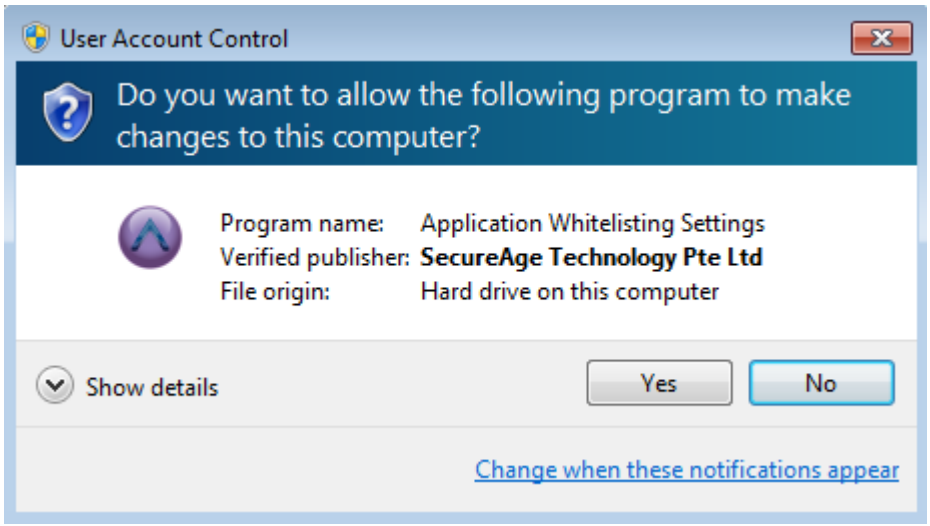
2.2.8 Settings

For fast navigation to Application Whitelisting Settings, follow the steps below:

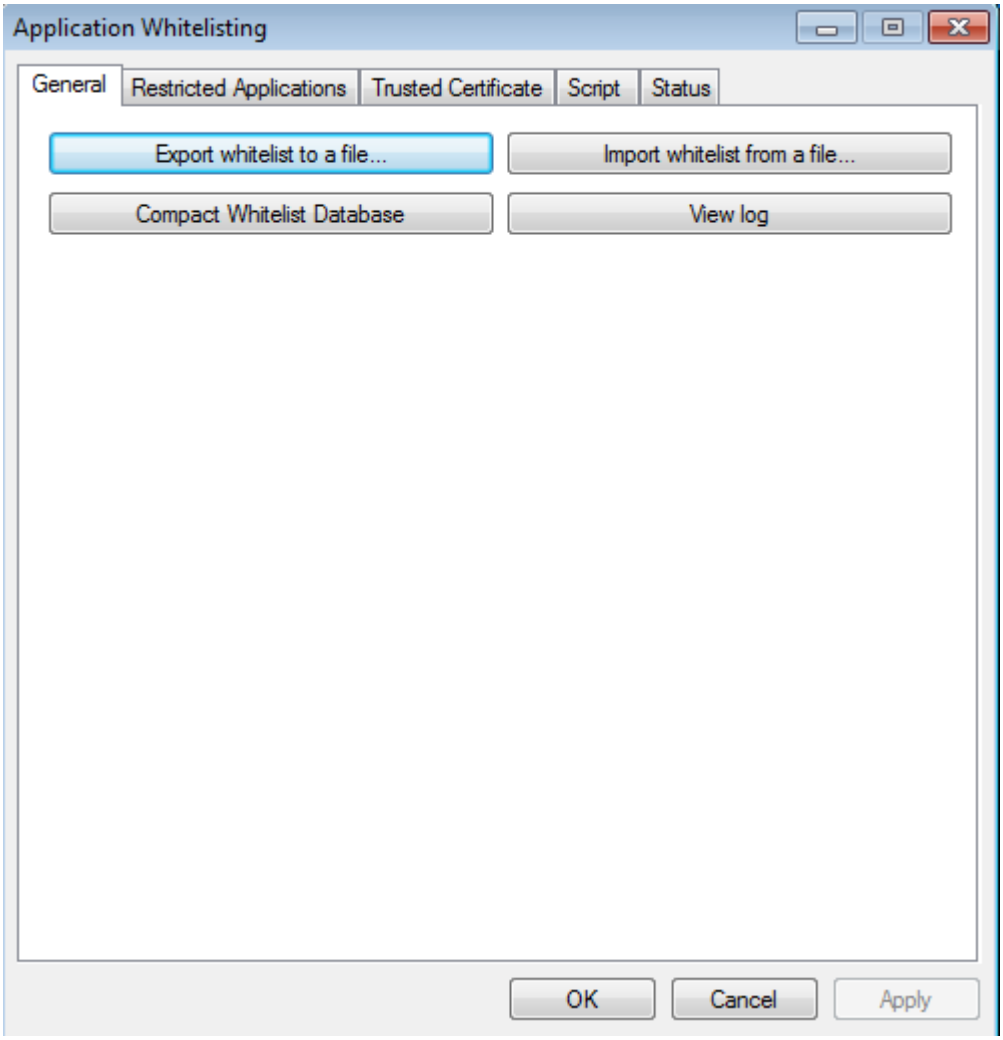
- Right click on **SecureAPlus** tray icon, click on **Application Whitelisting** on the menu and select **Settings**.



- In **User Account Control** window, click **Yes** to allow Application Whitelisting Settings to run.



- The **Application Whitelisting** window will launch.

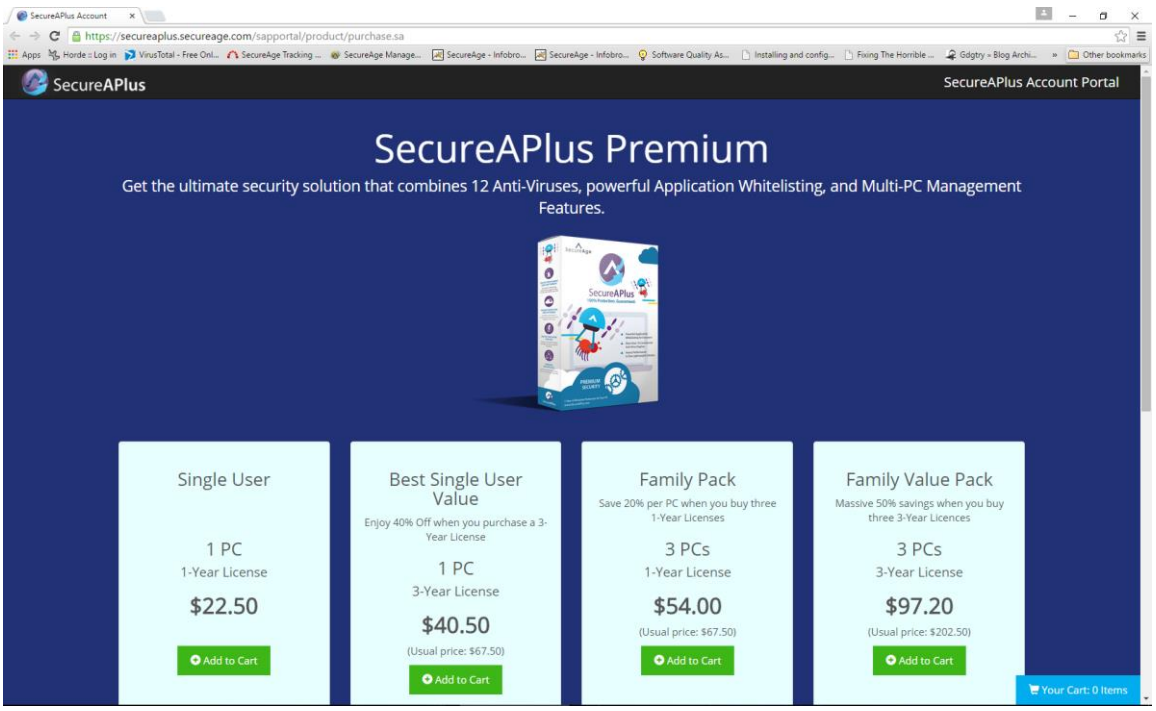


- Refer to **Section 7.2** for more detailed settings of Application Whitelisting.

3 SecureAPlus Main Console

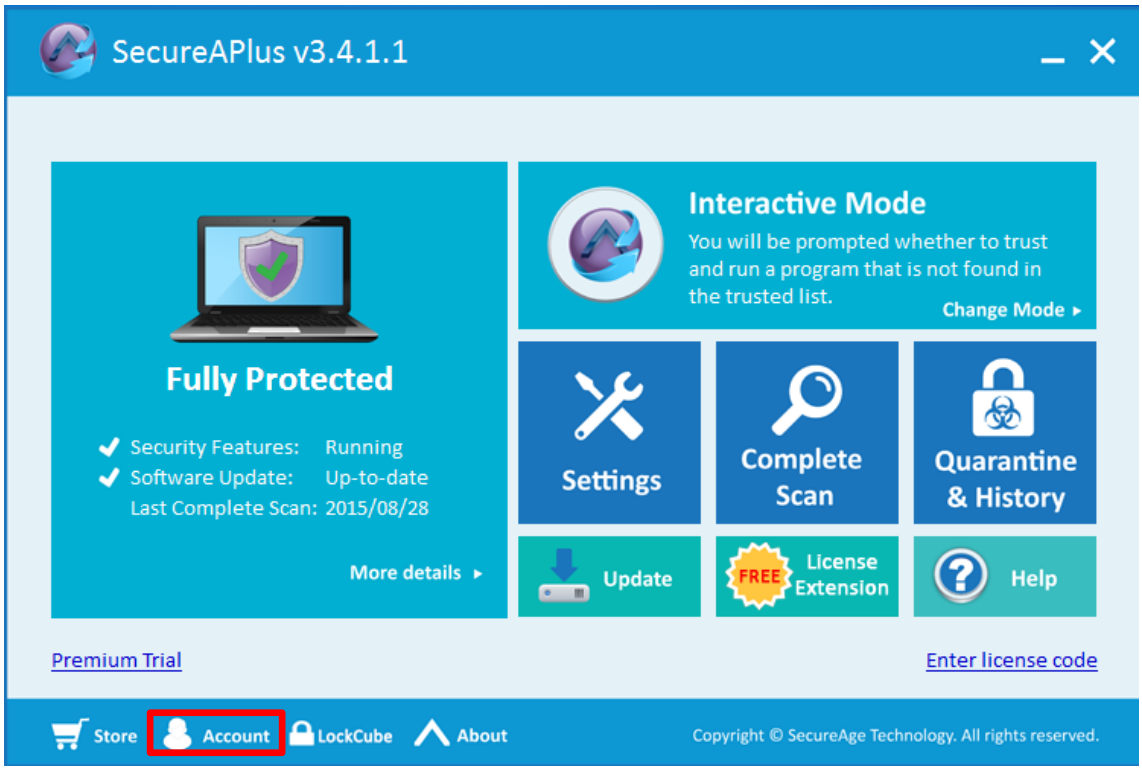
3.1 SecureAPlus Store

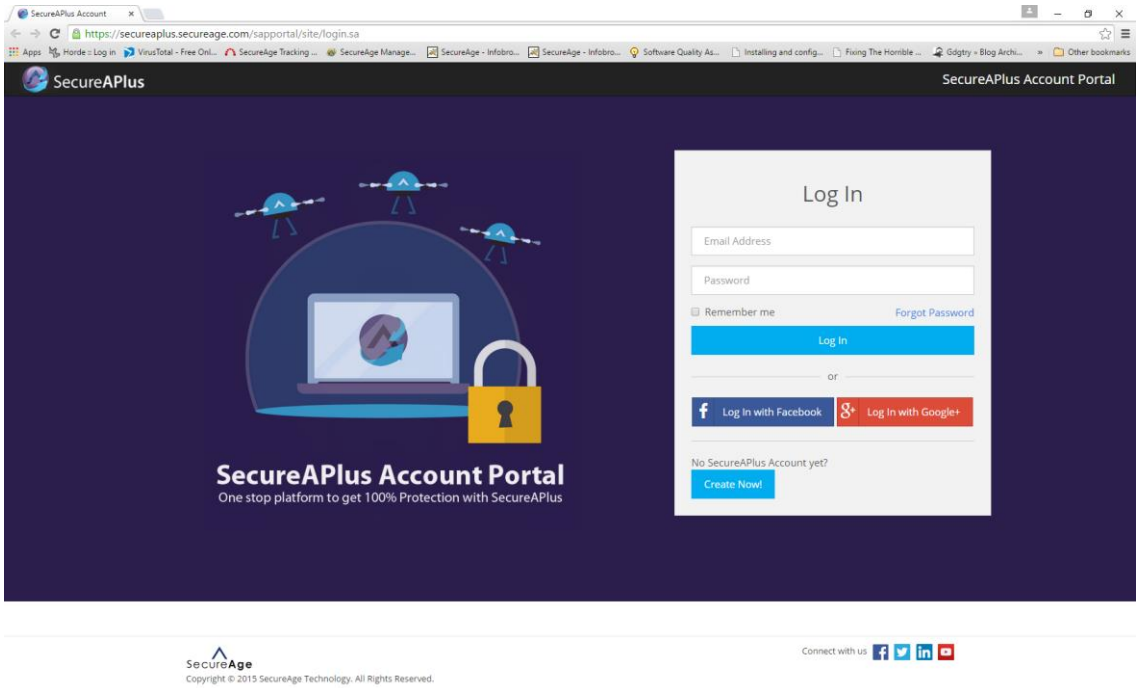
- Click on **Store** icon located at the bottom left in the **SecureAPlus** window, it will launch the SecureAge SecureAPlus Store webpage using the default browser.



3.2 SecureAPlus Account

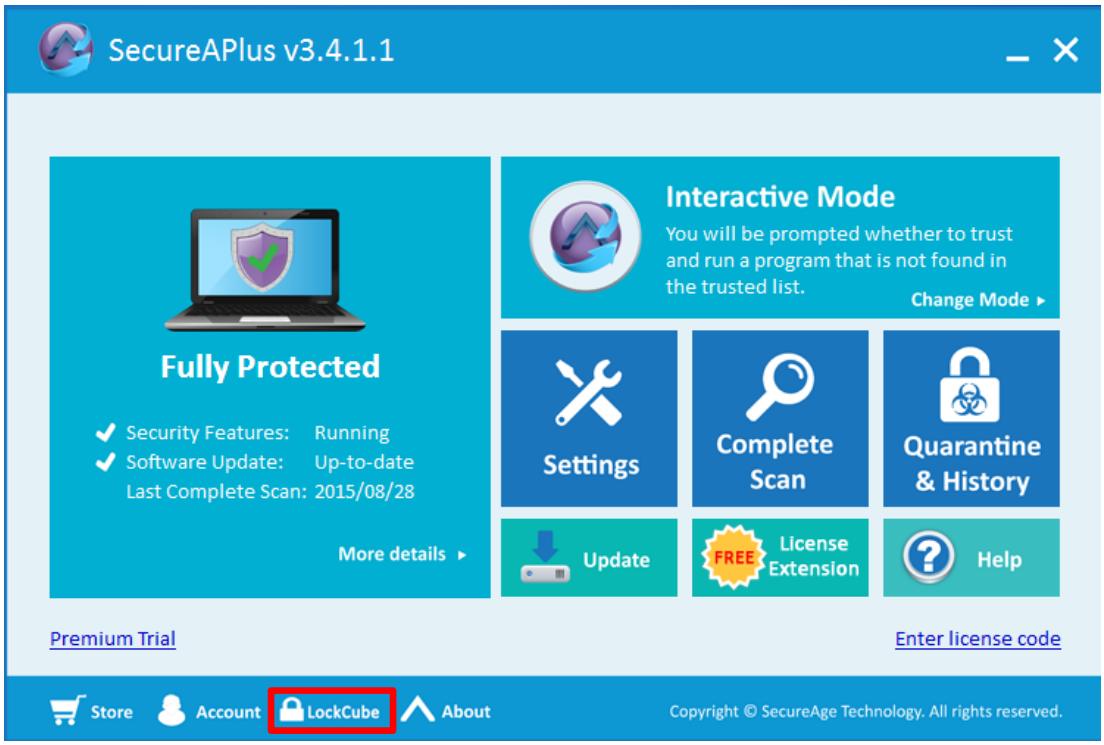
- Click on **Account** icon located at the bottom left in the **SecureAPlus** window, it will launch the SecureAge SecureAPlus Account Login webpage using the default browser.

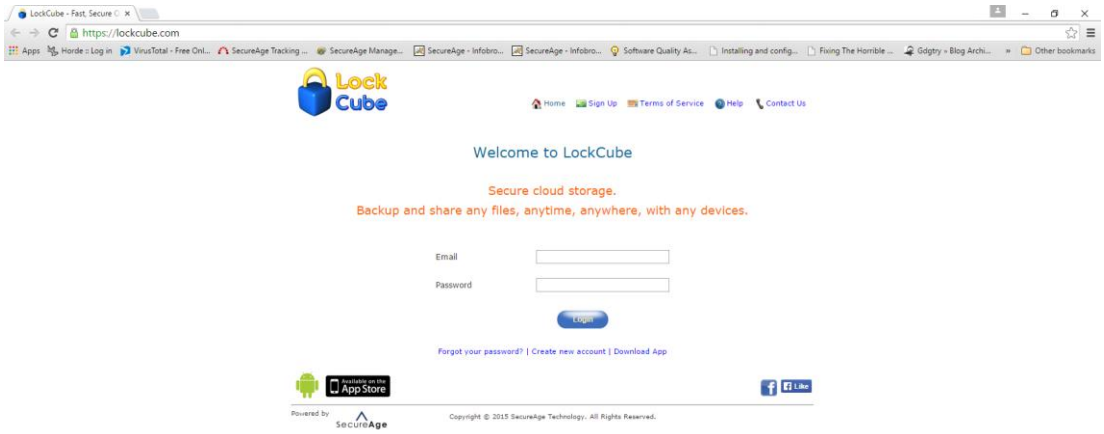




3.3 Lockcube (Secure Cloud Storage)

- Click on **Lockcube** icon located at the bottom left in the **SecureAPlus** window, it will launch the Lockcube Account Login webpage using the default browser.





Note:

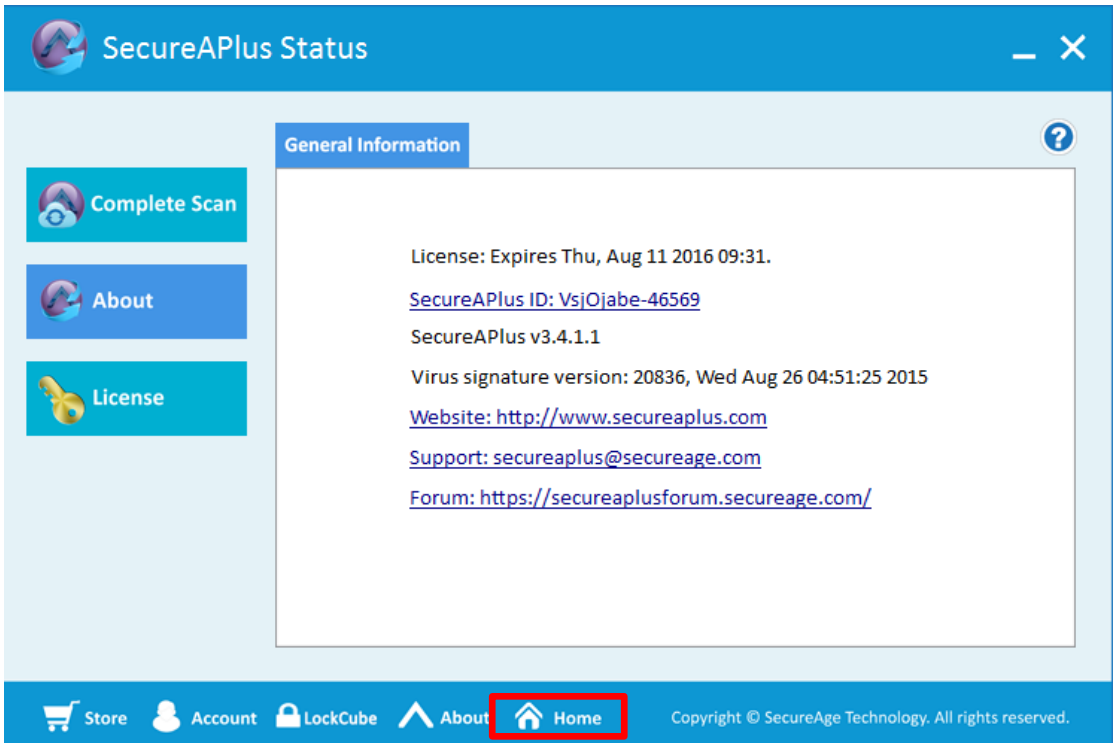
- Visit http://www.secureage.com/prd_SecureCloudStorage.jsp to find out more about Lockcube.

3.4 About

To know more about SecureAPlus Main Console, follow the steps below:

- Start SecureAPlus. Please refer to **Section 2.1** for the steps to start SecureAPlus.
- In the **SecureAPlus** window, click on the **About** icon on the bottom left of the window.

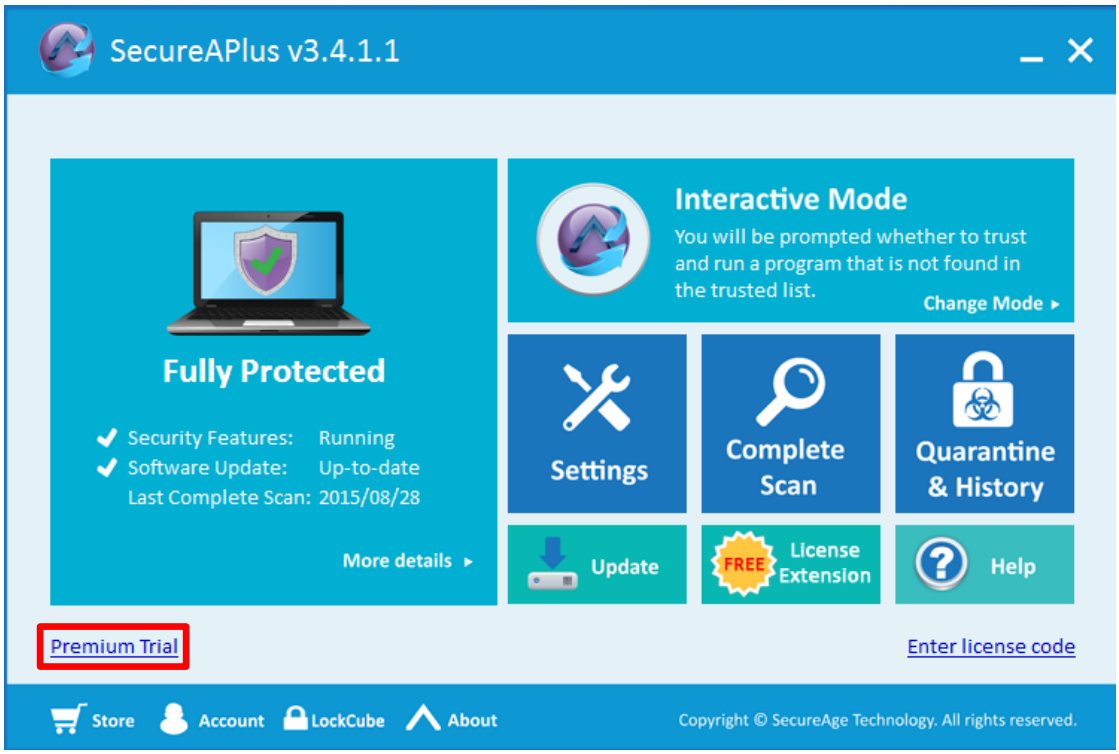
- The **General Information** will be displayed as shown below.

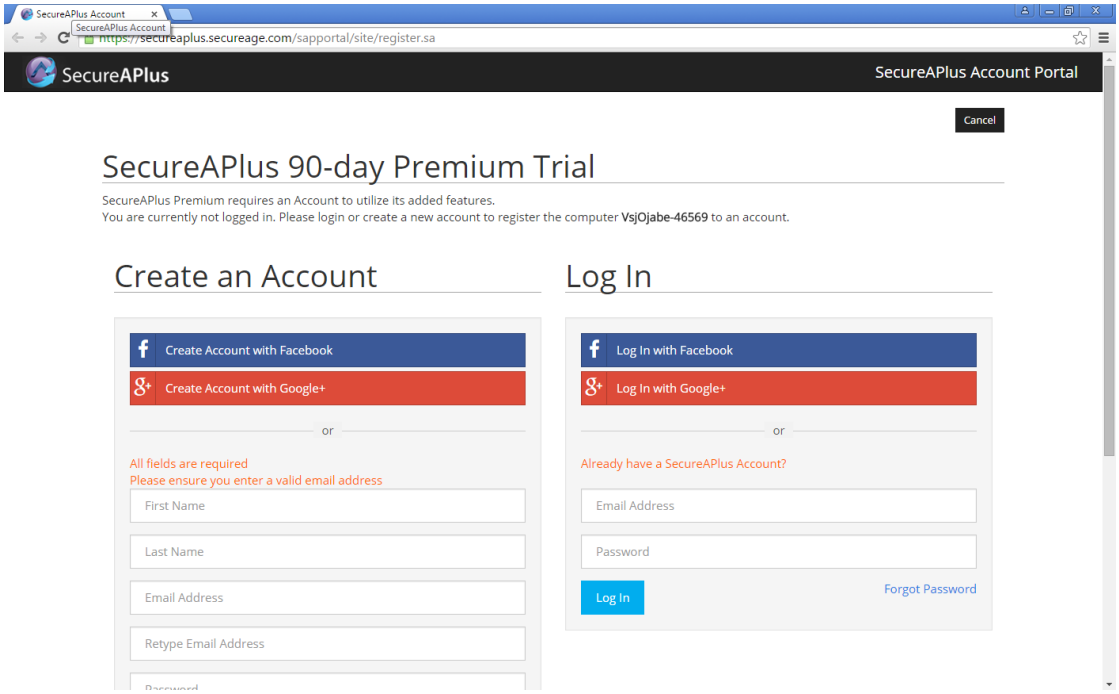


- Click on **Home** icon at the bottom to navigate back to the SecureAPlus main console window.

3.5 SecureAPlus Premium Trial

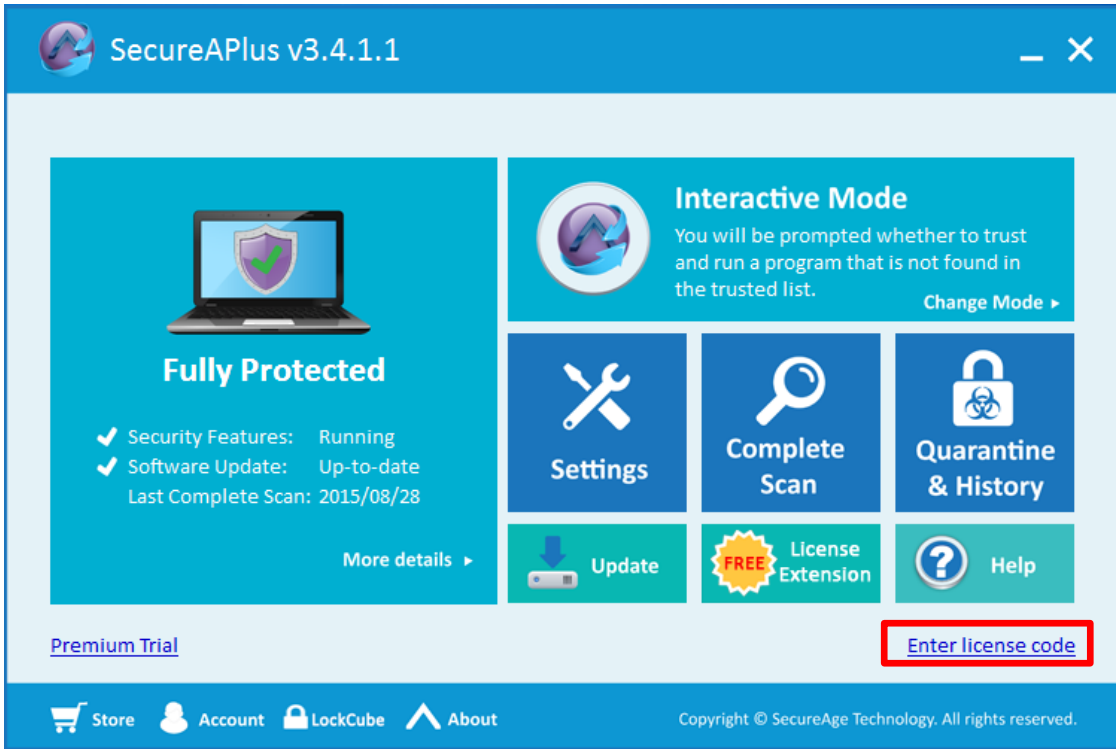
- Click on **Premium Trial** hyperlink located at the bottom left in the **SecureAPlus** window, it will launch the SecureAPlus 90-day Premium Trial webpage using the default browser.



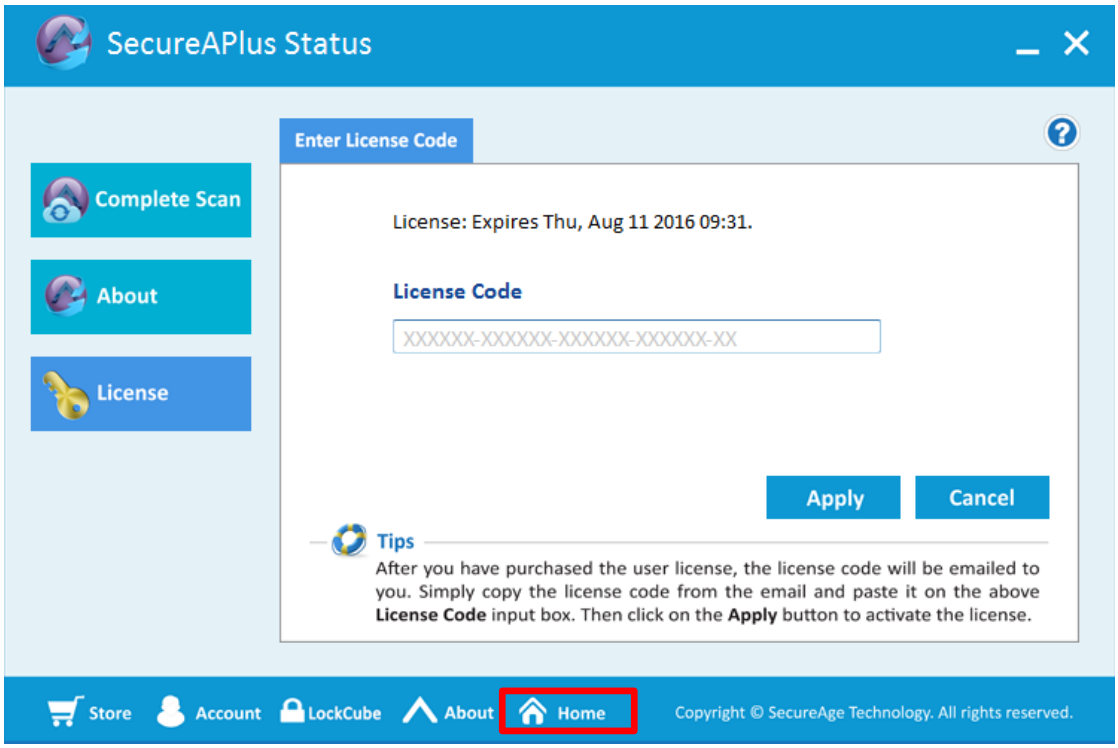


3.6 SecureAPlus License

- Click on **Enter license code** hyperlink located at the bottom right in the **SecureAPlus** window.



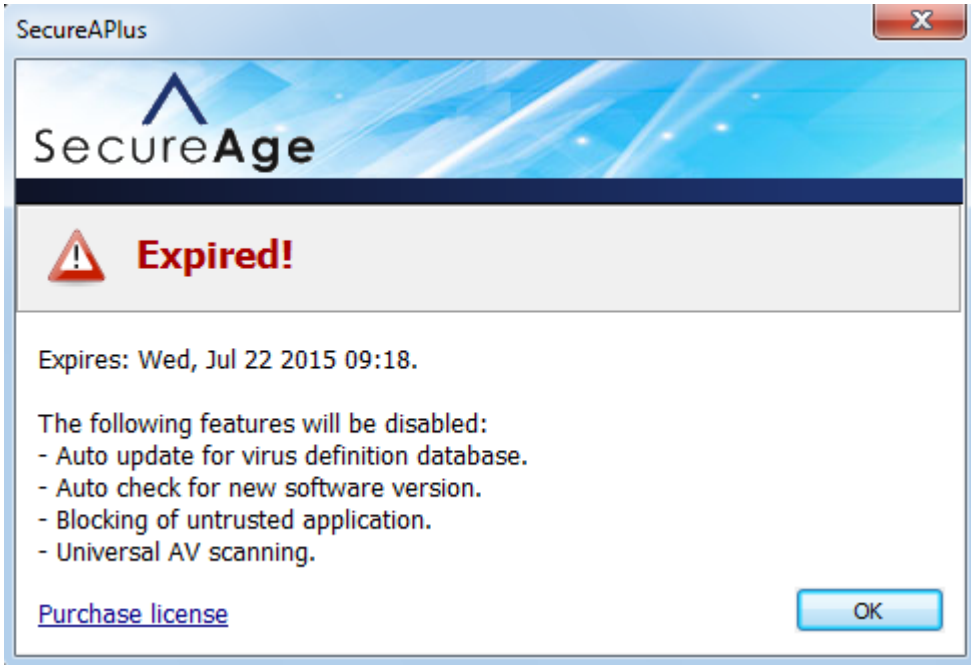
- The **Enter License Code** tab under **License** will be displayed as shown below.

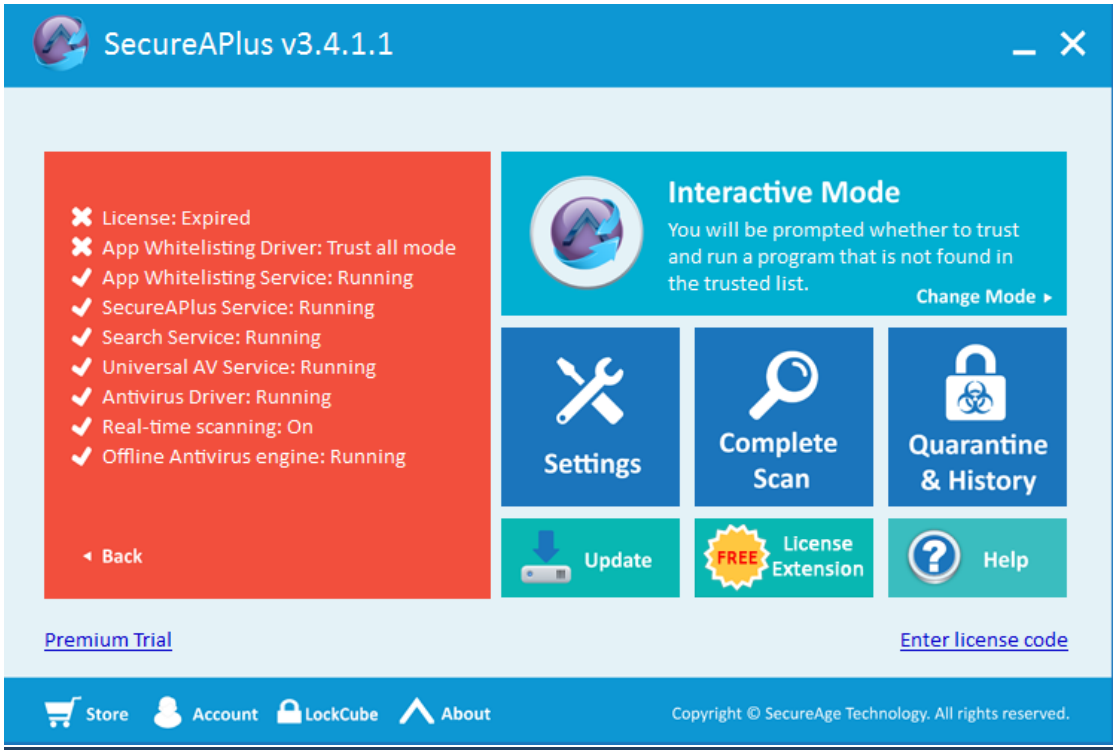


- Enter the new license code and click on **Apply** button to activate the new license.
- Click on **Home** icon at the bottom to navigate back to the SecureAPlus main console page.

Note:

- When the SecureAPlus license is expired, certain SecureAPlus features will be disabled and the SecureAPlus Main Summary will be display as shown below.

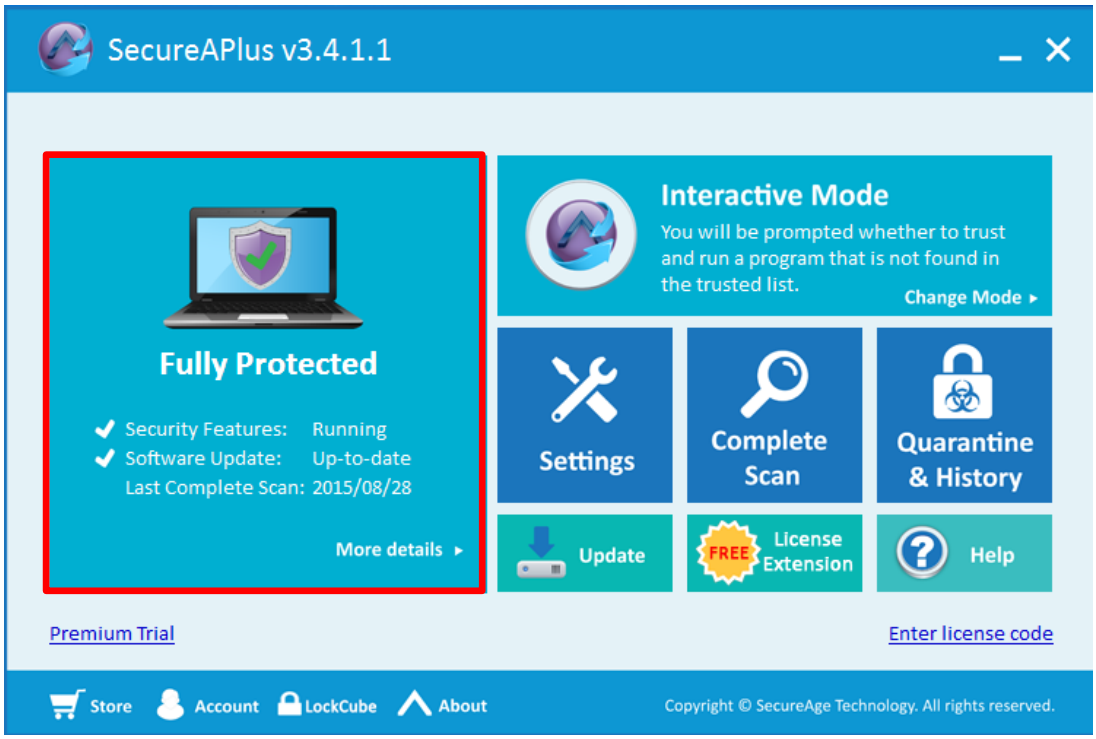




3.7 Main Summary

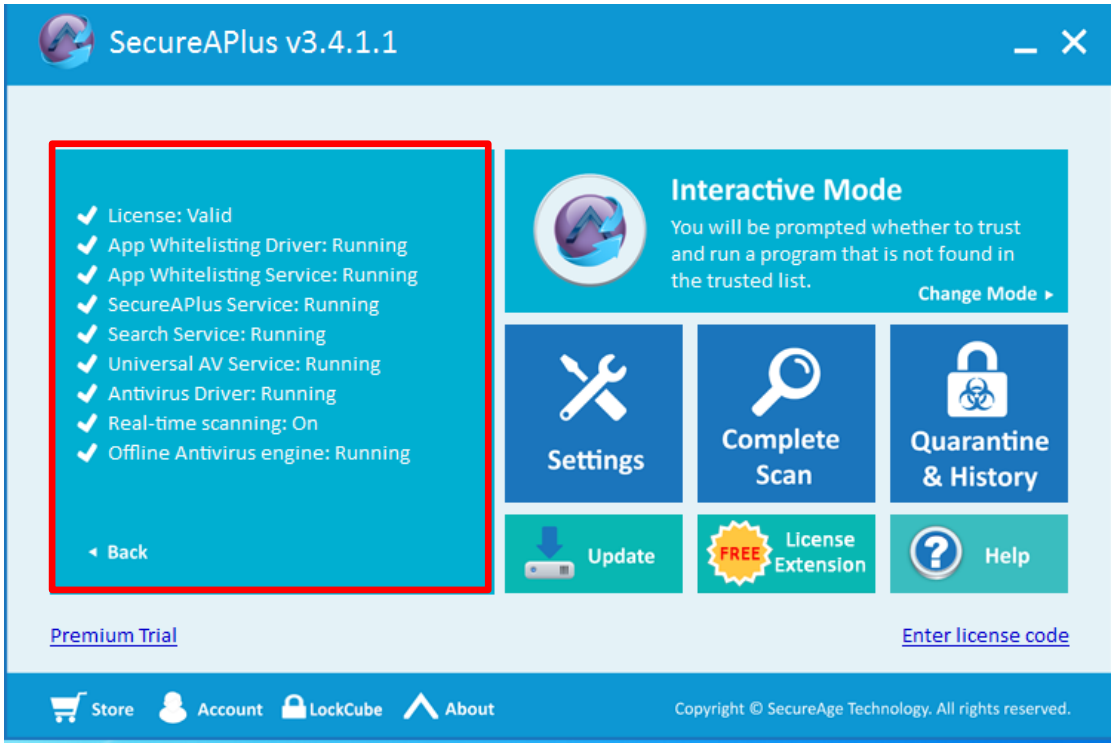
To know more about SecureAPlus Main Summary, follow the steps below:

- Start SecureAPlus. Please refer to **Section 2.1** for the steps to start SecureAPlus.
- In **SecureAPlus** window, on the left side will show the current status of the machine.



- Click on **More details** to view more details of the status.

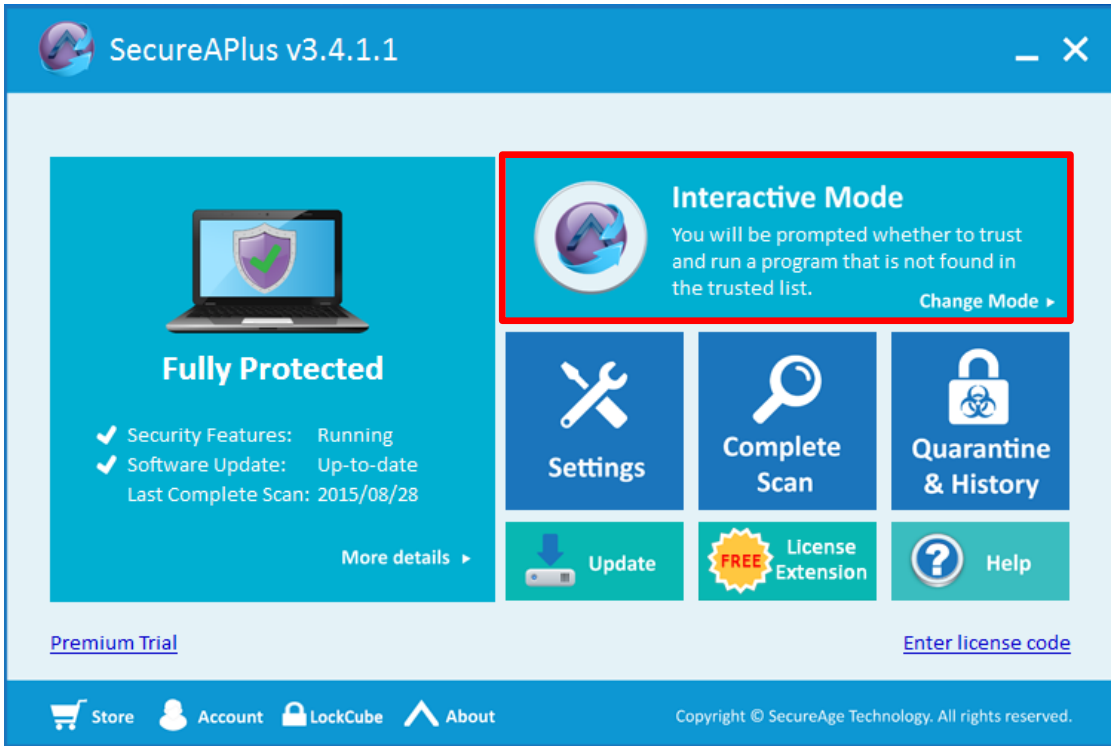
  - All the status should be displayed as **Running** or **On** when SecureAPlus is working normally.



3.8 Application Whitelisting Modes

To view the current SecureAPlus mode, follow the steps below:

- Start SecureAPlus. Please refer to **Section 2.1** for the steps to start SecureAPlus.
- In the **SecureAPlus** window, the current mode is indicated on the top.



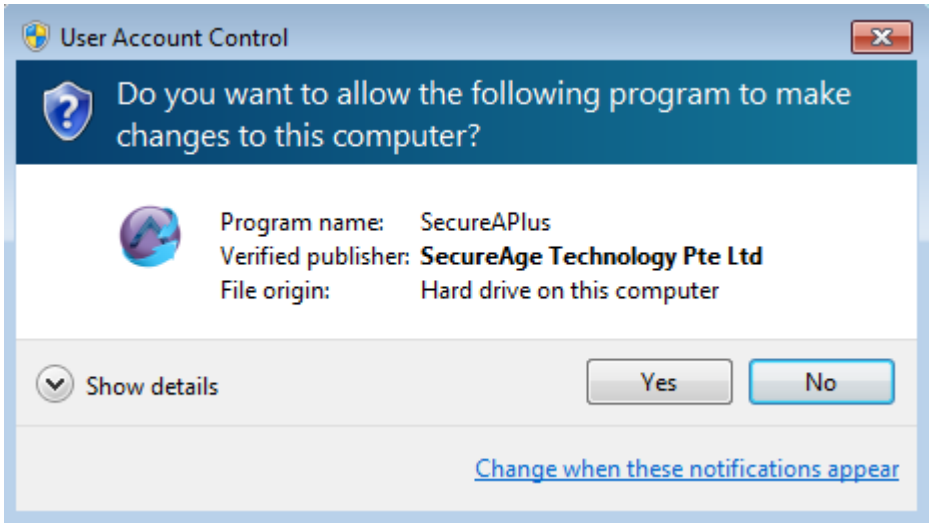
To change the current SecureAPlus mode, follow the steps below:

- Start SecureAPlus. Please refer to **Section 2.1** for the steps to start SecureAPlus.
- In the **SecureAPlus** window, click on **Change Mode**.

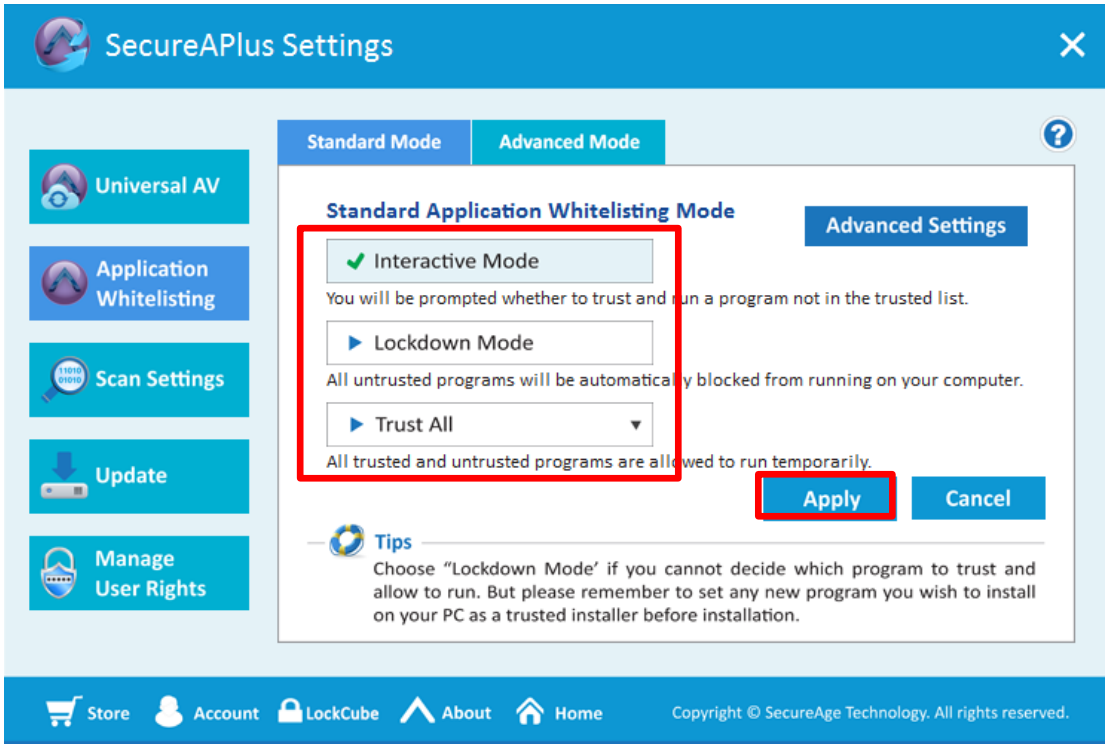
Note:

- This corresponds to selecting the modes via the SecureAPlus Tray Icon Menu (**Section 2.2**).

- In **User Account Control** window, click **Yes** to allow SecureAPlus to run.

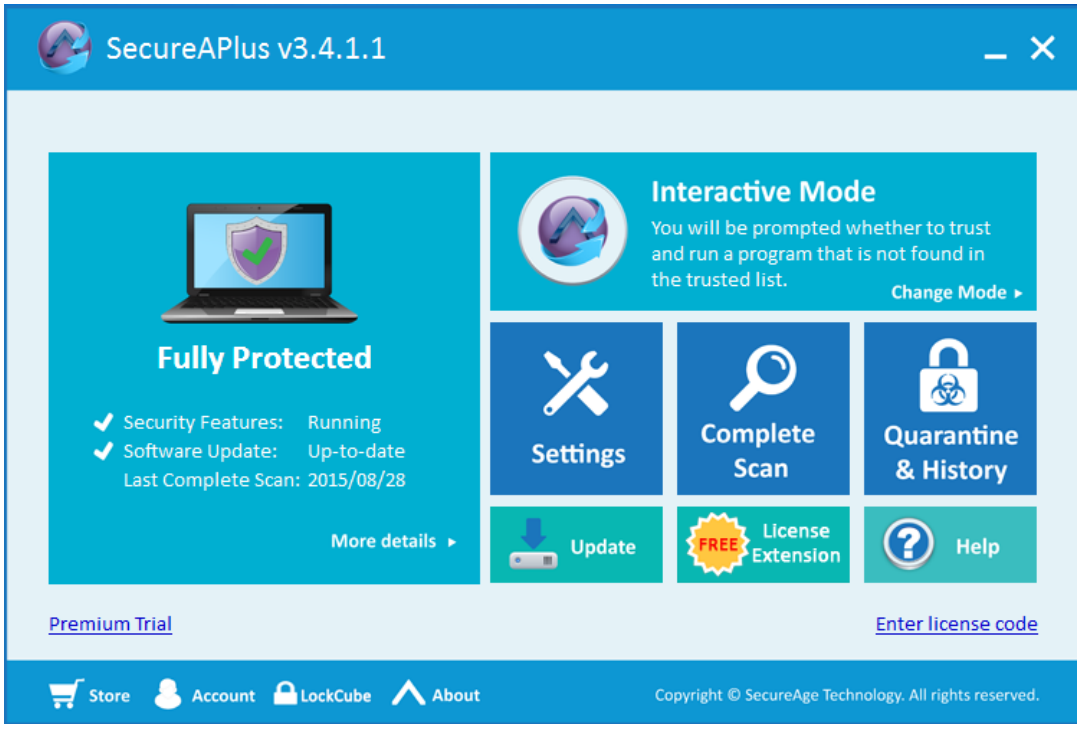


- The **Application Whitelisting Standard Mode** under **Application Whitelisting** within the **SecureAPlus Settings** will be displayed.

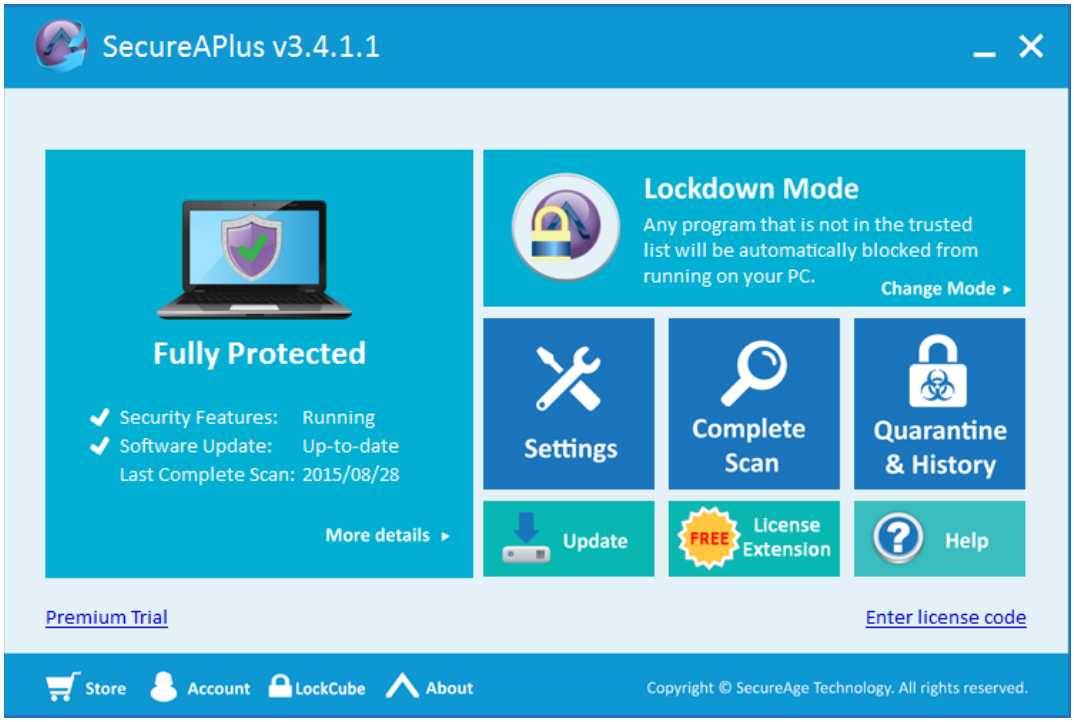


- Select the **Standard Application Whitelisting Mode** and click on **Apply** button.
- Click on **Home** icon at the bottom to navigate back to the SecureAPlus main console page, the SecureAPlus Main Console should change accordingly as shown below:

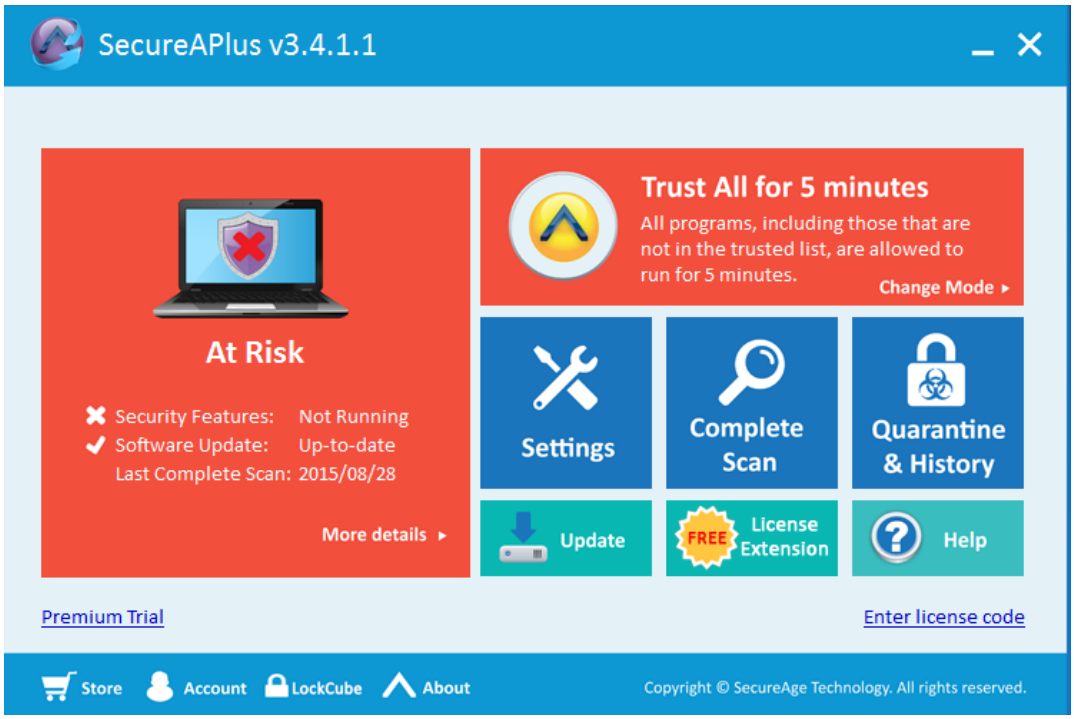
Interactive Mode



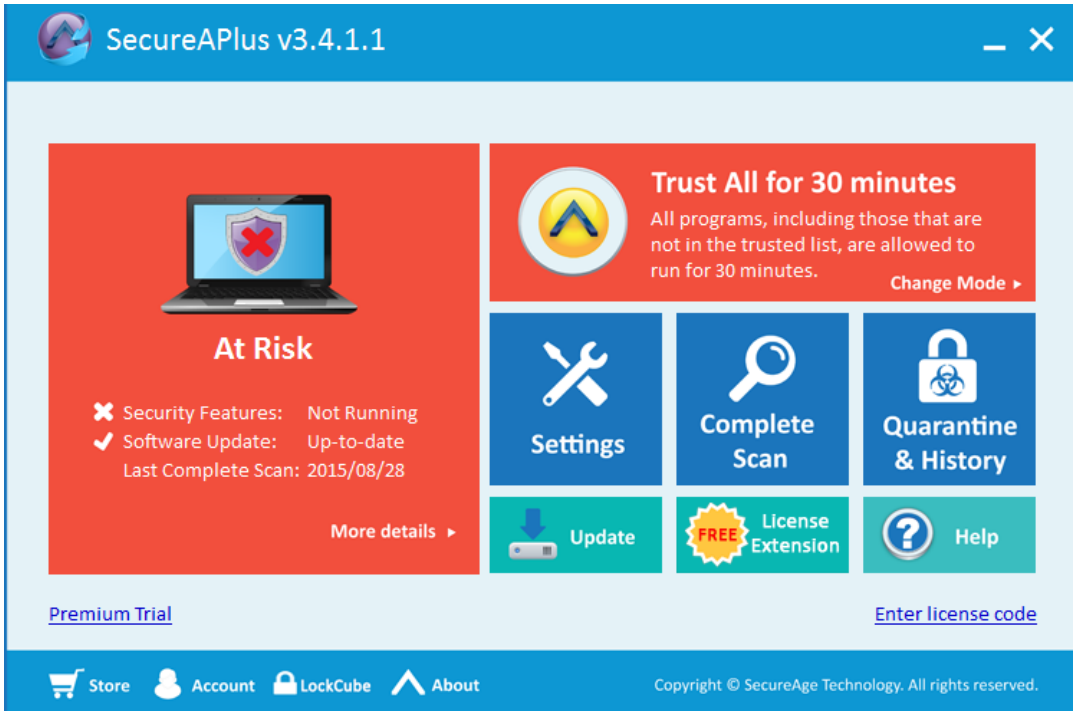
Lockdown Mode



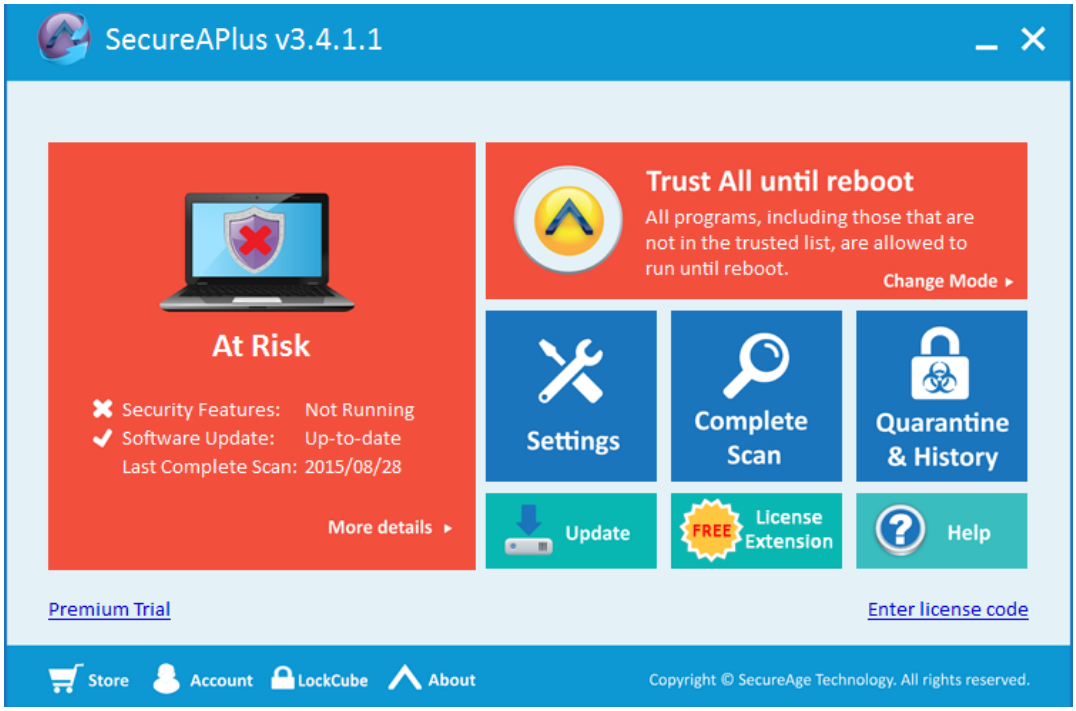
Trust All for 5 minutes



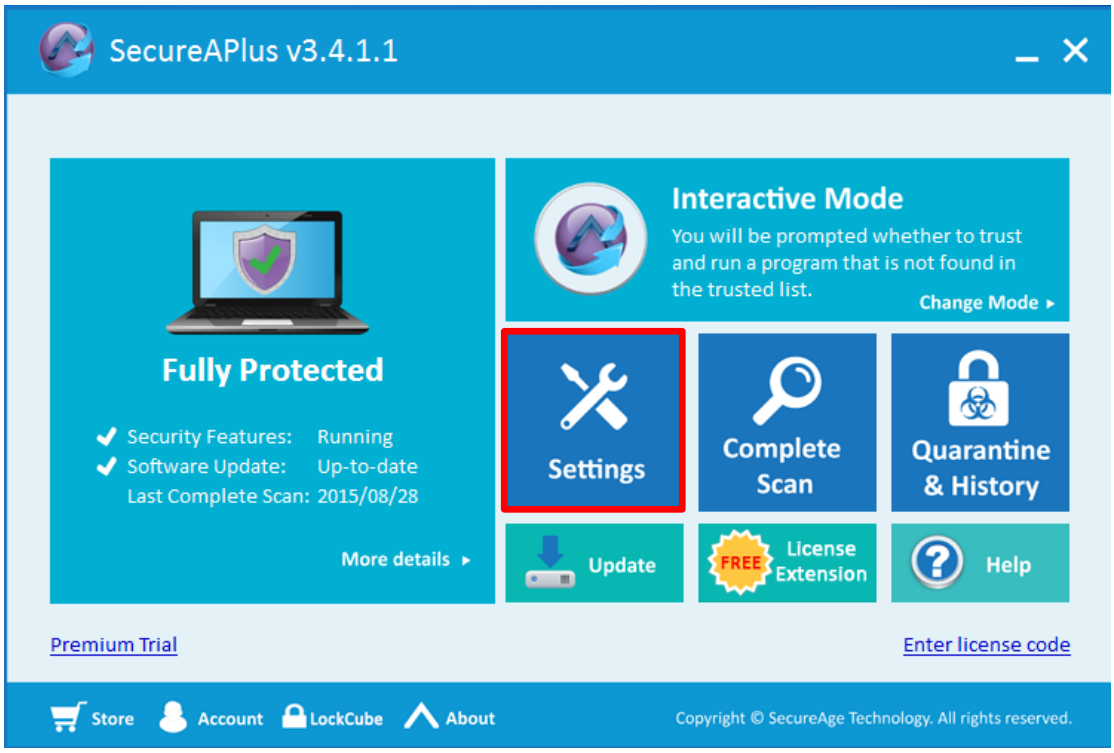
Trust All for 30 minutes



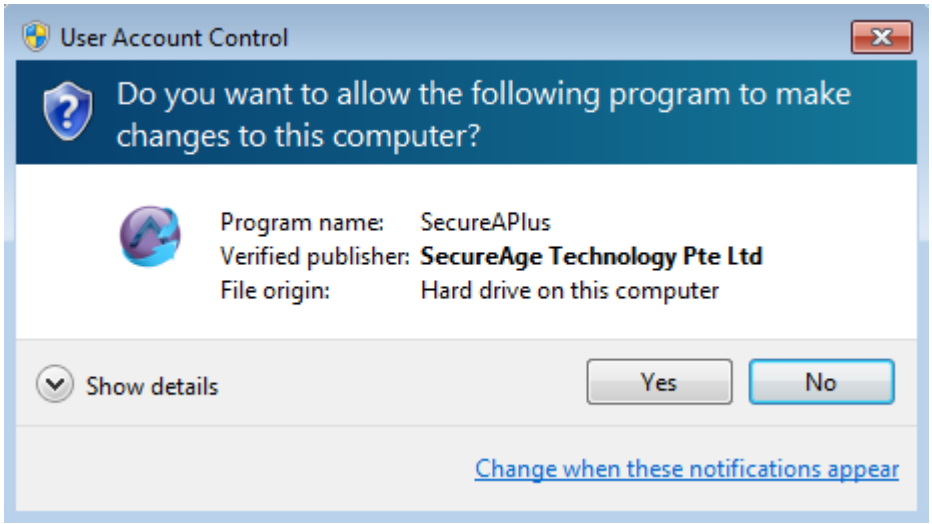
Trust All until computer is restarted



3.9 SecureAPlus Settings

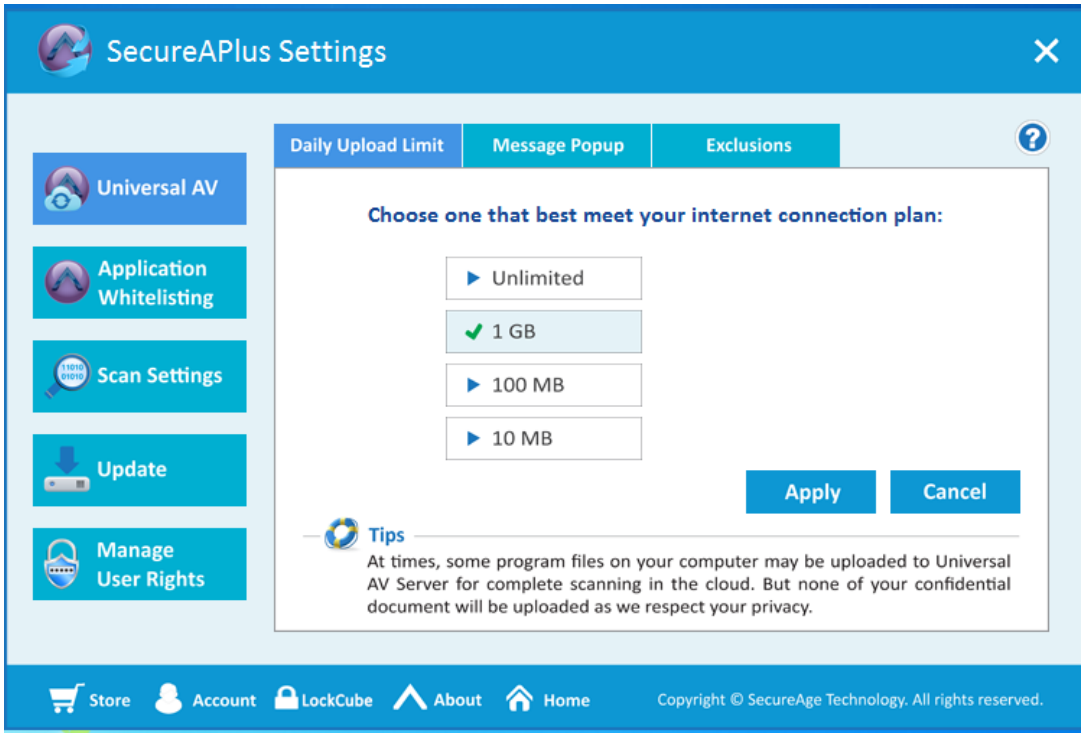


- In **User Account Control** window, click **Yes** to allow SecureAPlus to run.



- The **SecureAPlus Settings** window will launch.

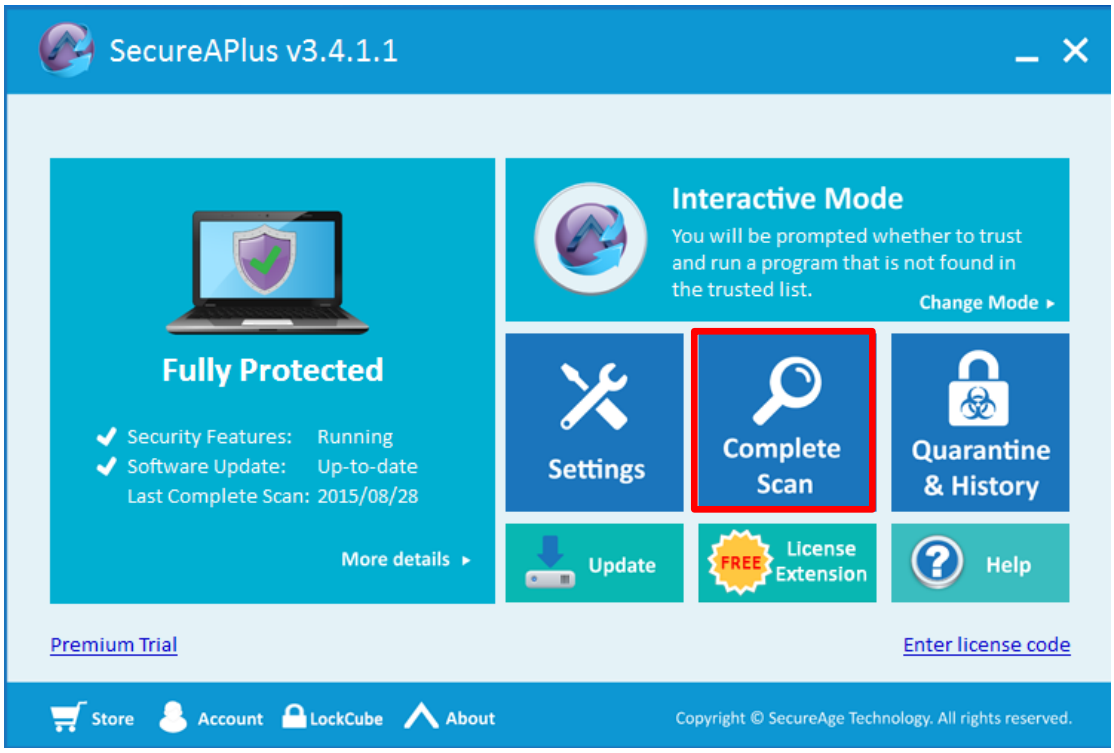
.



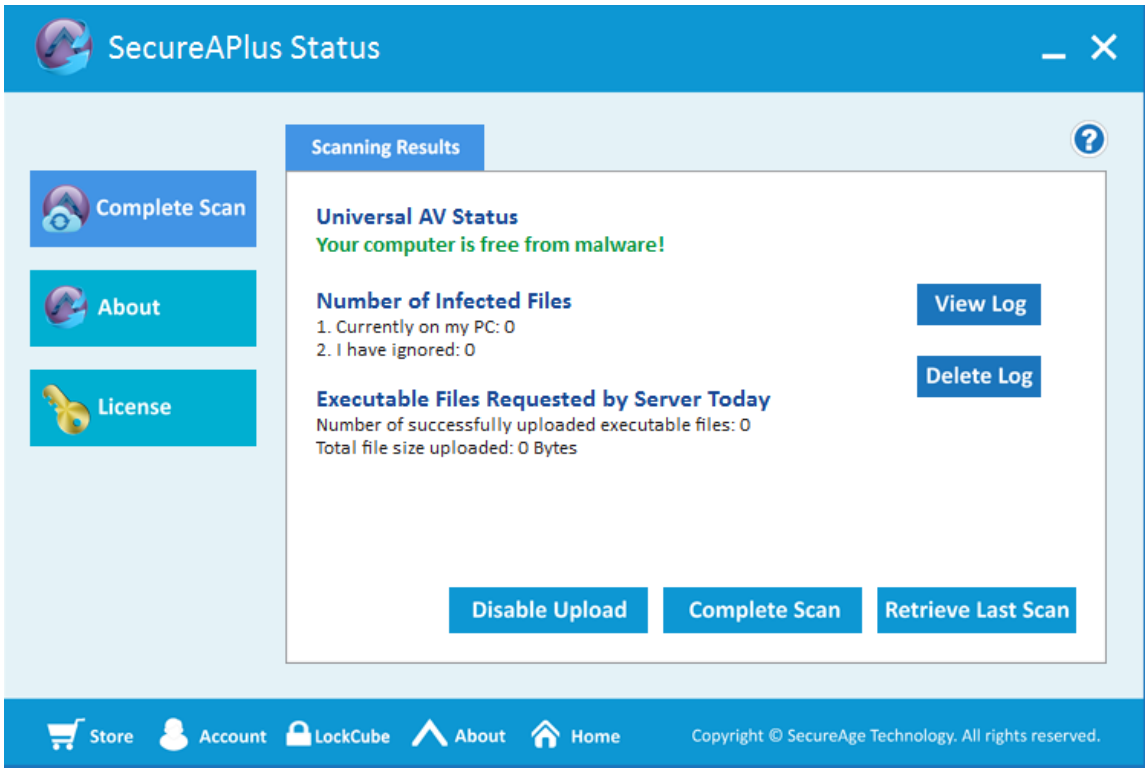
Note:

- Refer to **Section 4** for more details on SecureAPlus Settings.

3.10 SecureAPlus Complete Scan



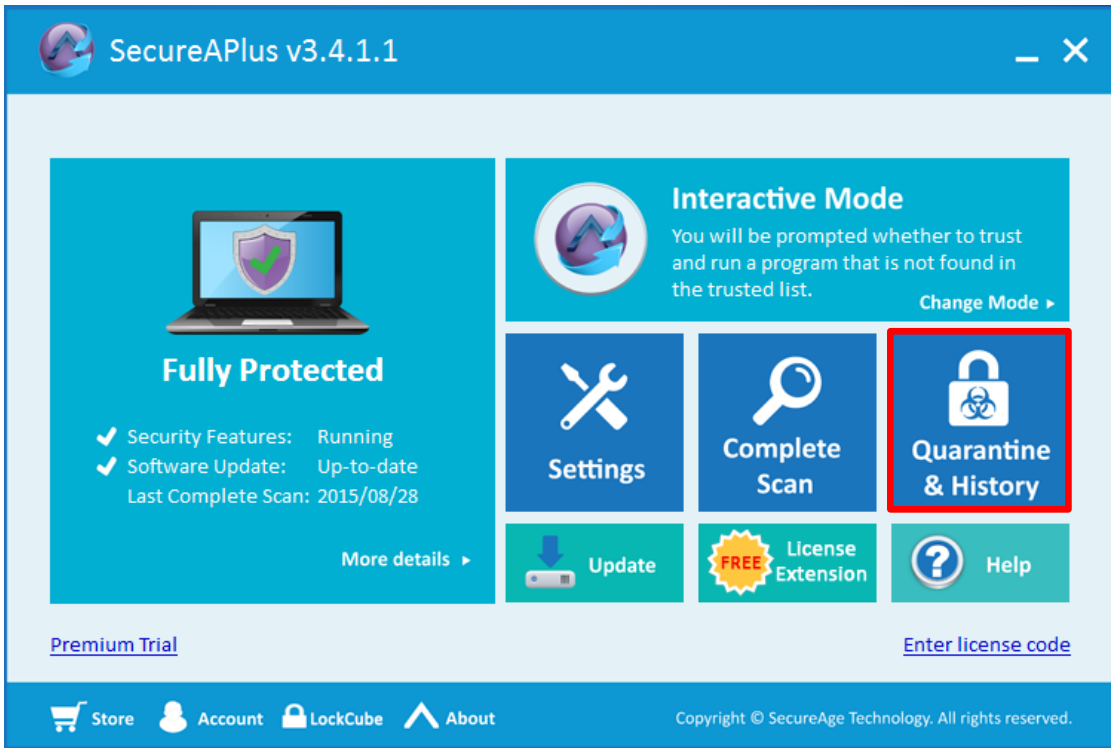
- The **SecureAPlus Status** window will appear, showing the current state of the Universal AV and the latest details of the Universal AV scan results will be displayed.



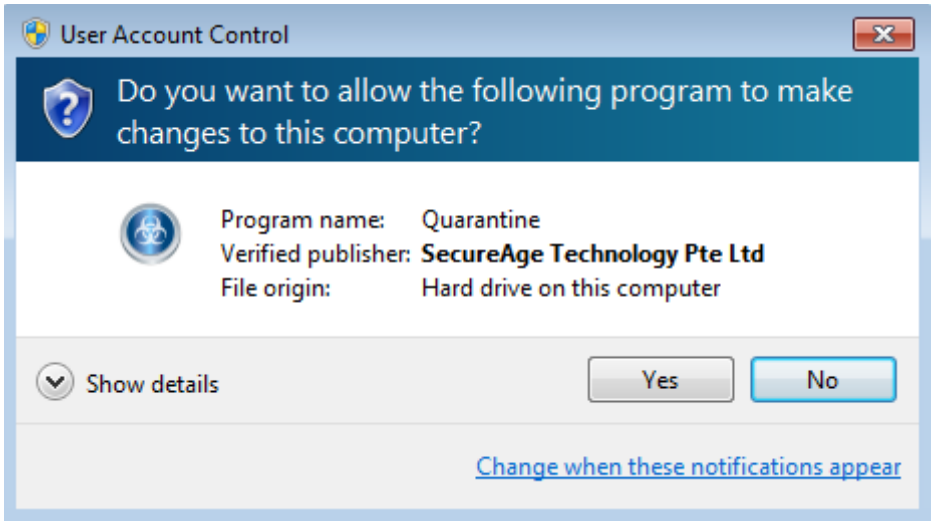
Note:

- Refer to **Section 5** for more details on Universal AV.

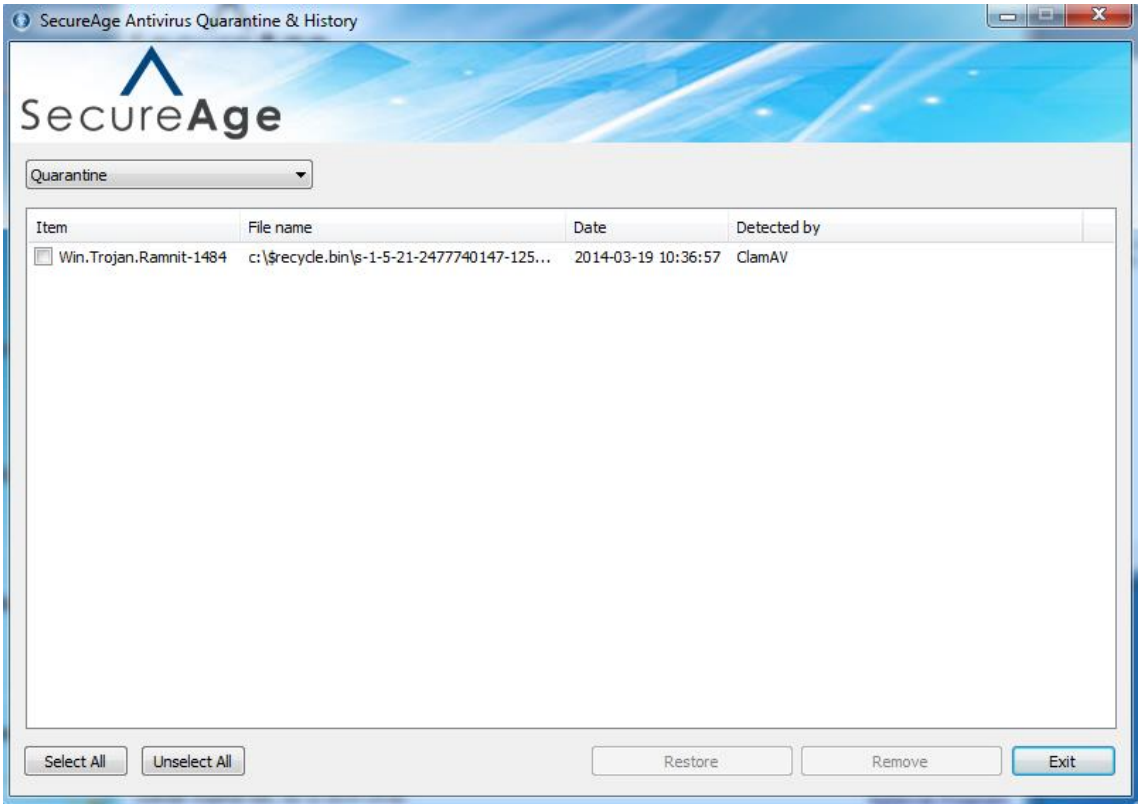
3.11 SecureAPlus Quarantine & History



- In **User Account Control** window, click **Yes** to allow Quarantine to run.



- The **SecureAge Antivirus Quarantine & History** window will launch.



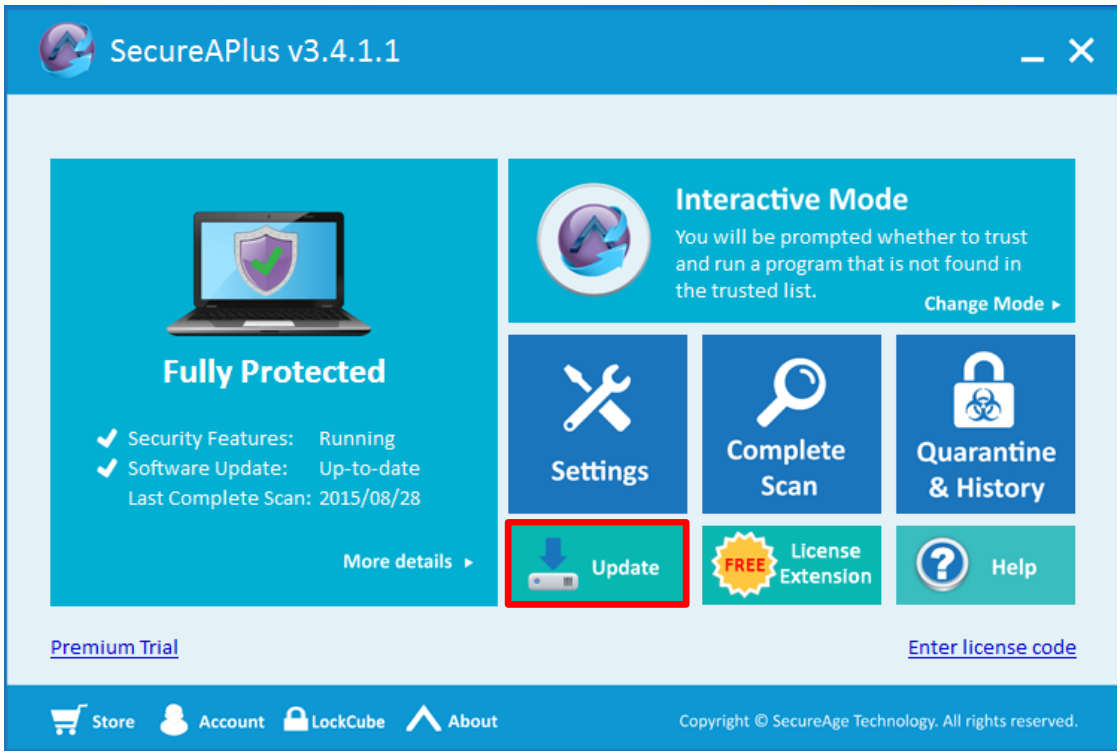
Note:

- Refer to **Section 6** for more details on Quarantine & History.

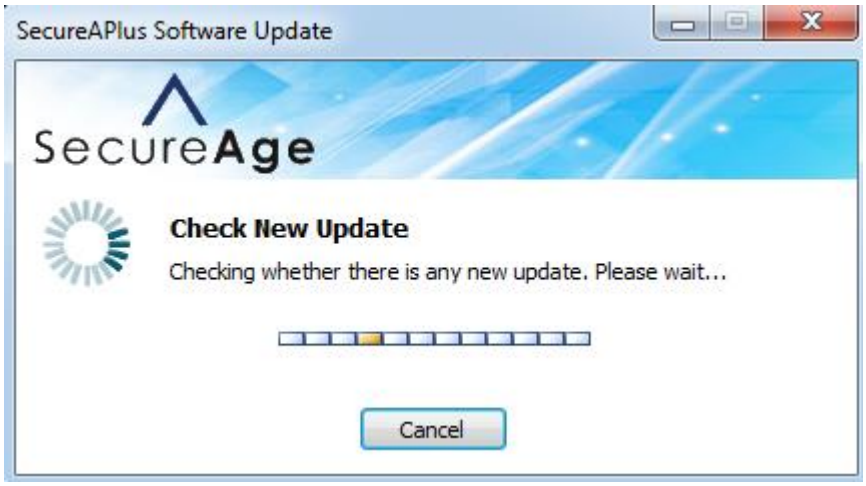
3.12 SecureAPlus Software Update

To update the SecureAPlus software, follow the steps below:

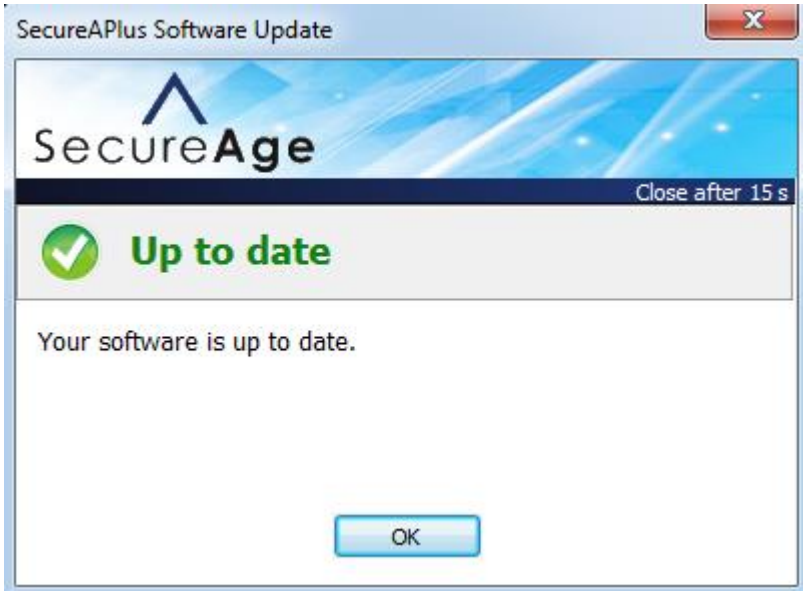
- Start SecureAPlus. Refer to **Section 2.1** for the steps to start SecureAPlus.
- In the **SecureAPlus** window, click on the **Update** icon.



- SecureAPlus software will check for new update.



- If the current SecureAPlus software version is the up to date, a message will be prompt as shown below.



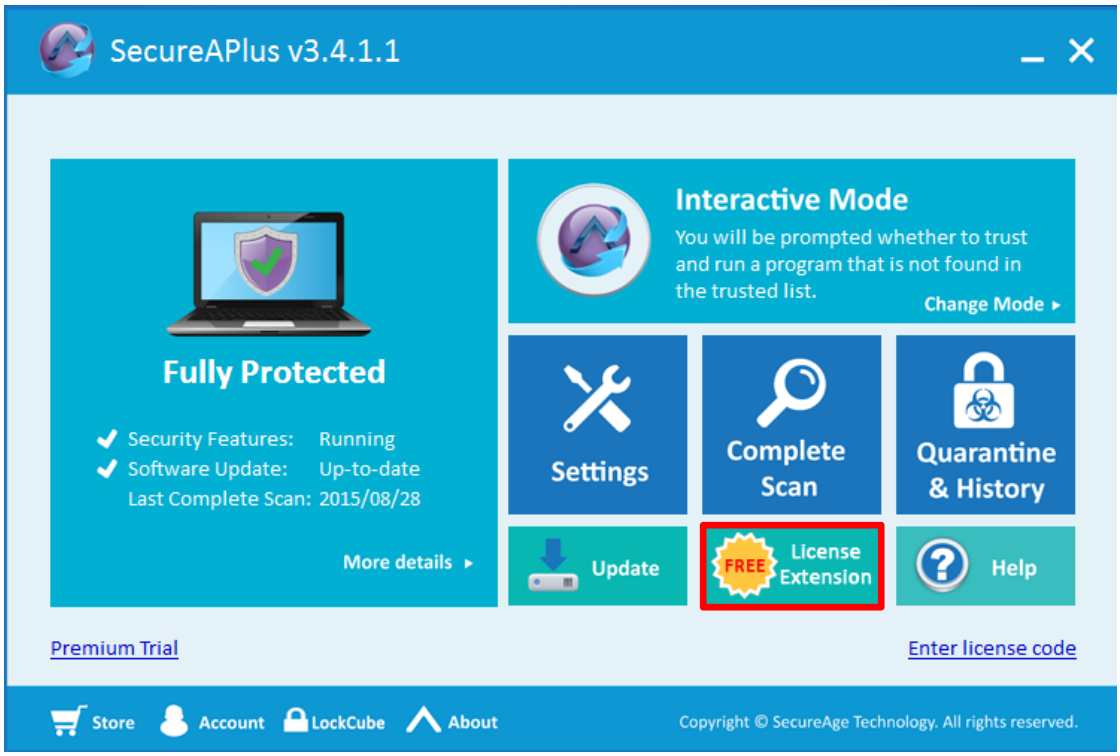
- If the current SecureAPlus software version is not up to date,

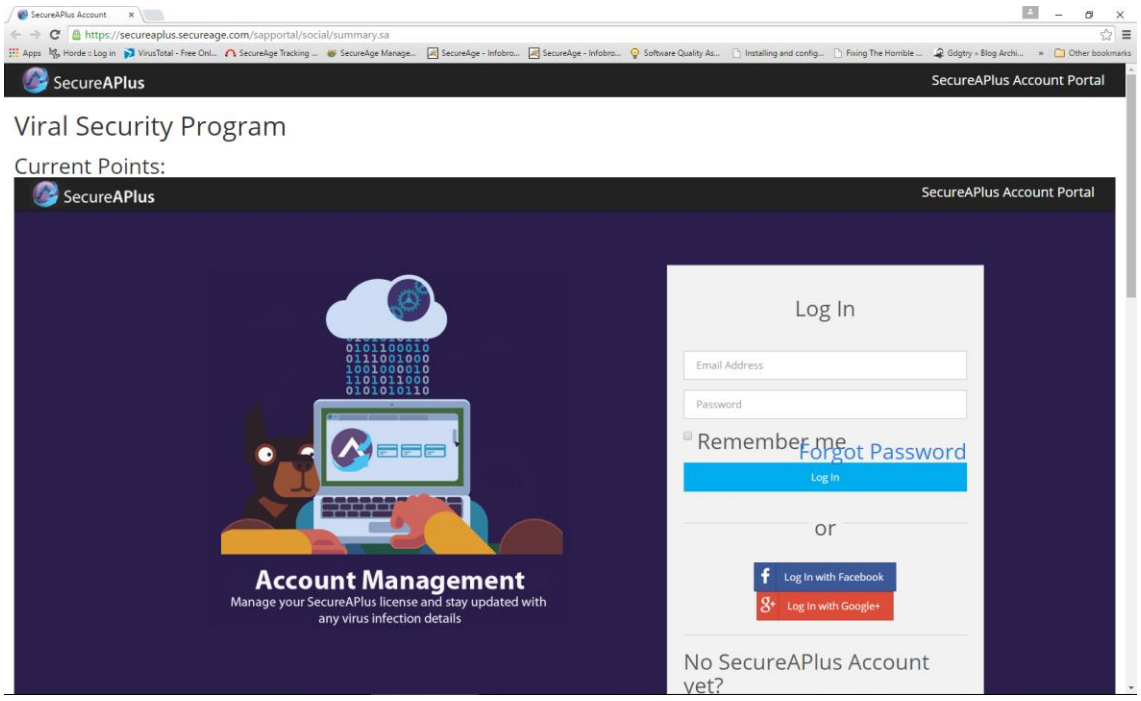
Note:

- Refer to **Section 4.4.1** for more details on Software Updates.

3.13 License Extension

- Click on **License Extension** icon located in the **SecureAPlus** window, it will launch the SecureAge SecureAPlus Account webpage using the default browser.





3.14 Help

- Click on the **Help** icon located in the **SecureAPlus** window, it will launch the SecureAPlus user guide using the default pdf reader.

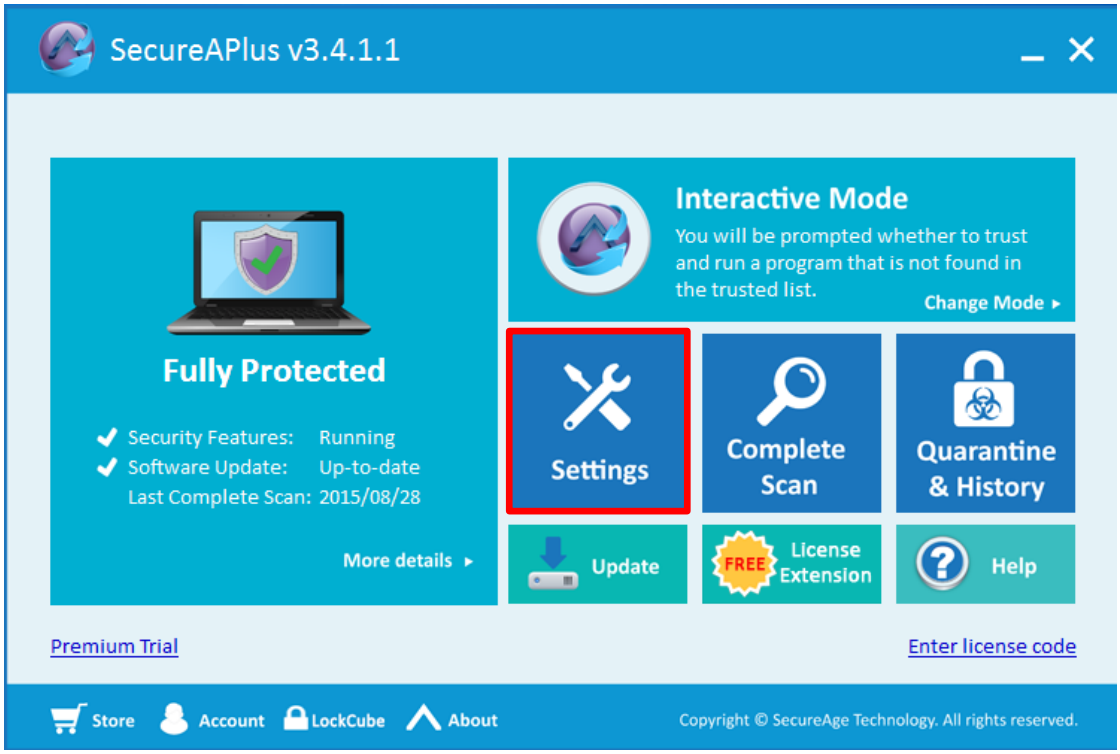
Note:

- This corresponds to launching the SecureAPlus User Guide via the SecureAPlus Tray Icon (**Section 2.2**).

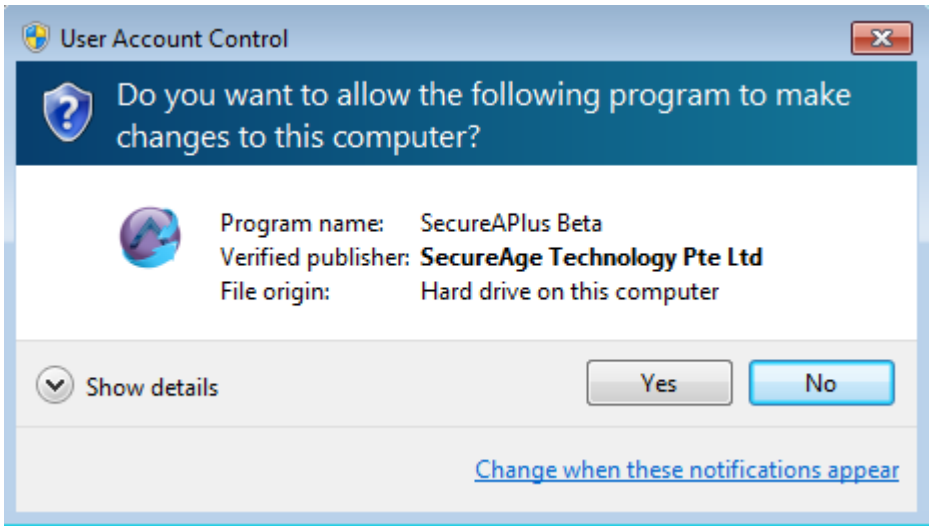
4 SecureAPlus Settings

To view the SecureAPlus settings, please do the following steps:

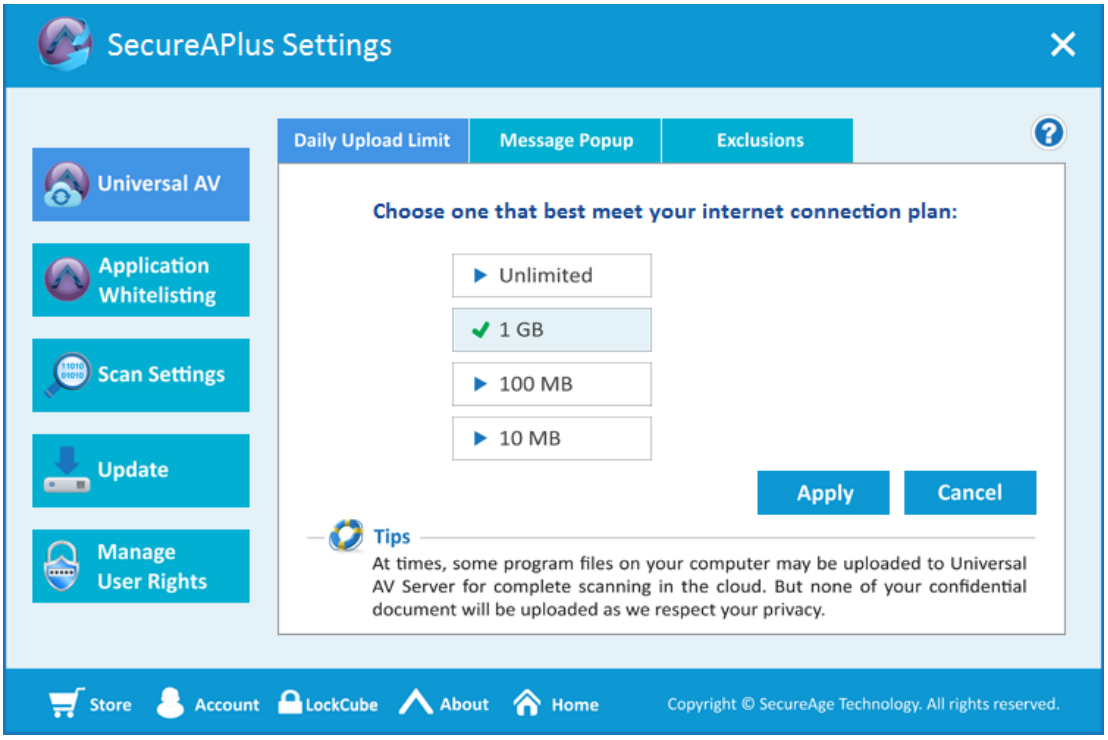
- Start SecureAPlus. Please refer to **Section 2.1** for the steps to start SecureAge.
- In **SecureAPlus** window, click on the **Settings** button to view the settings.



- In **User Account Control** window, click **Yes** to allow SecureAPlus Settings to run.



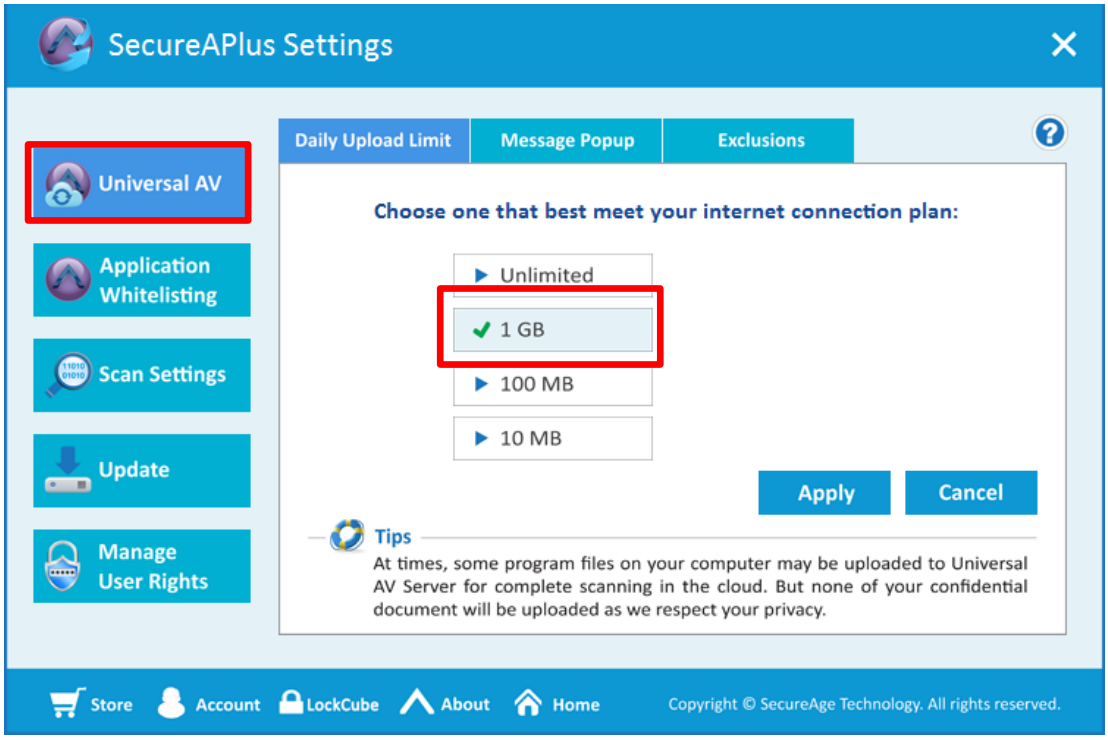
- The **SecureAPlus Settings** window will launch.



4.1 Universal AV

You can view the current daily upload limit of the Universal AV by following the steps as below:

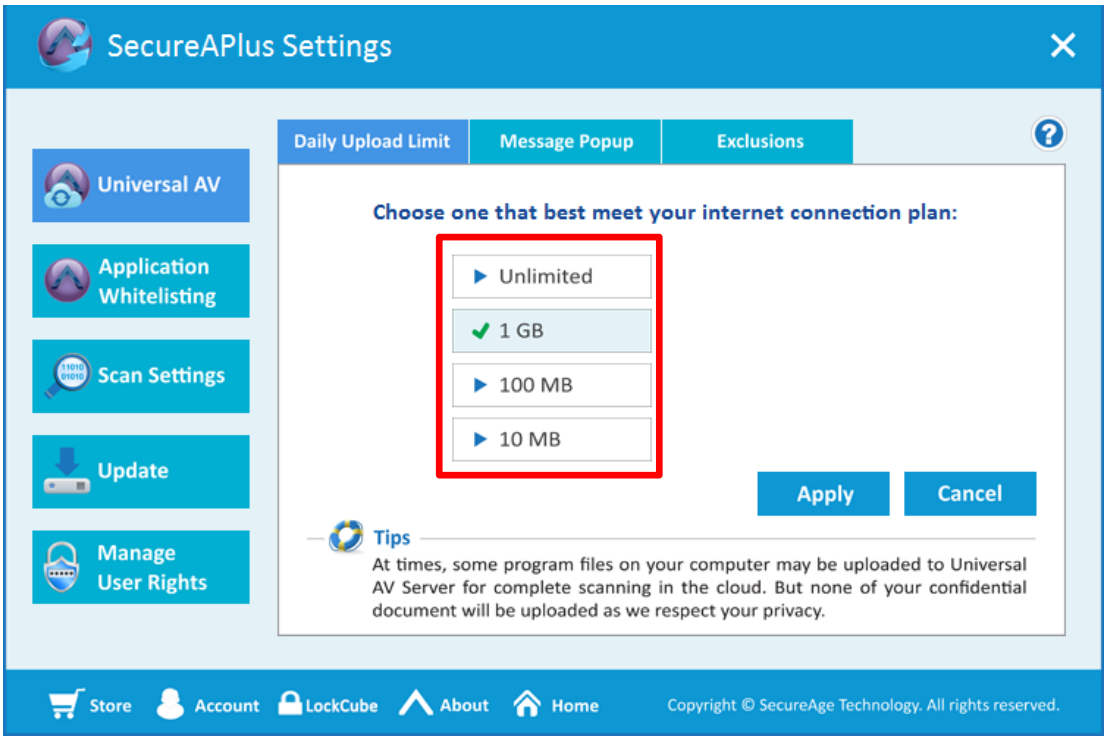
- Start SecureAPlus. Please refer to **Section 2.1** for the steps to start SecureAPlus.
- In **SecureAPlus** window, click on the **Settings** icon to view the settings.
- In the **SecureAPlus Settings** window, click on **Universal AV** on the left menu.
- Under the **Daily Upload Limit** tab, the selected option with a tick at the side is the current daily upload limit.



4.1.1 Daily Upload Limit

To restrict the daily upload limit, follow the step below:

- Select the options under **Daily upload limit** tab (default is 1GB). This is useful for users who have a limited internet bandwidth.



- Click on **Apply** button to apply the changes made.

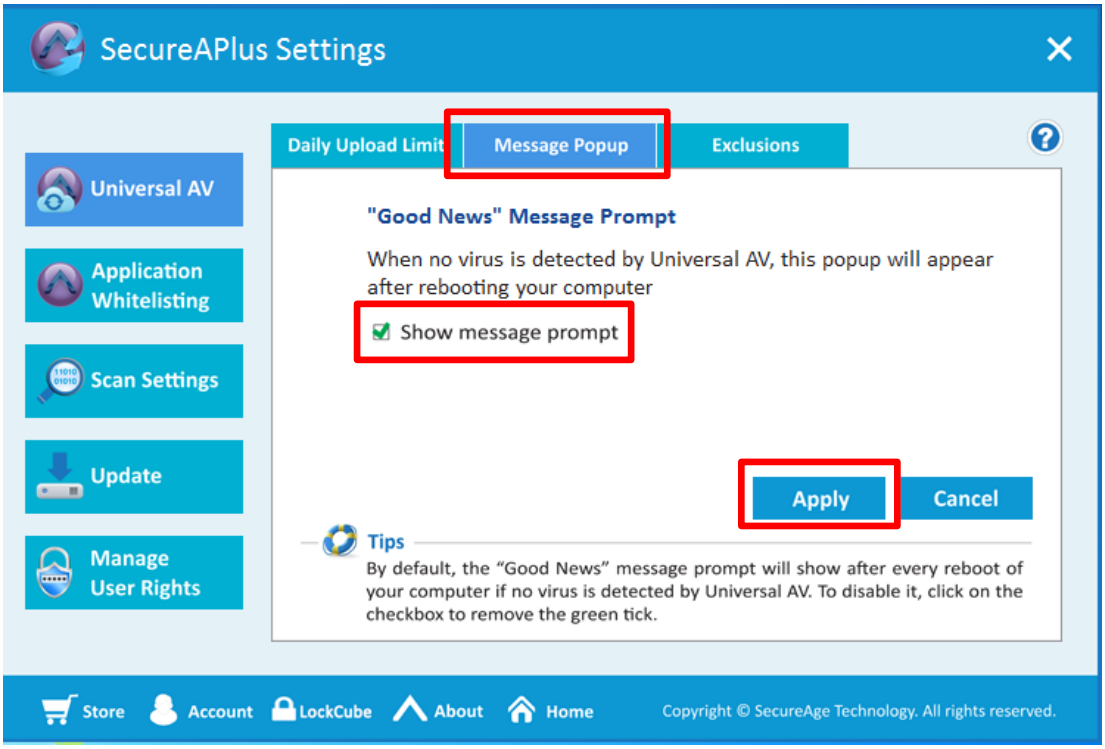
Note:

- When the **Total number of bytes uploaded today** reaches the limit set under **Daily upload limit** (Eg: 10MB/100MB/1GB/Unlimited), the number of hashes will still be uploaded but the number of sample files will not be uploaded. It will try again to submit the files to the server next time if it does not exceed the daily upload limit.

4.1.2 Message Popup ("Good News" Message Prompt)

To enable or disable the "Good News" Message prompt after your computer startup, follow the step below:

- In the **SecureAPlus Settings** window, click on **Universal AV** on the left menu and click on the **Message Popup** tab.

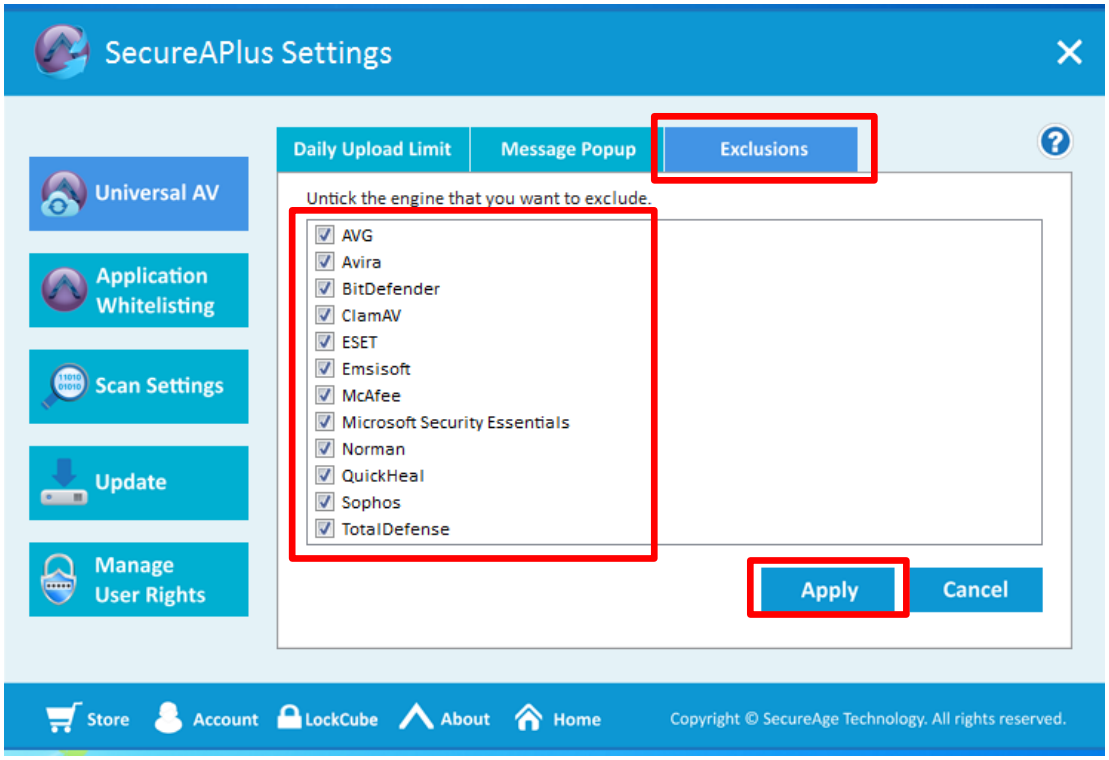


- Check or uncheck the **Show message prompt** to enable or disable the "Good News" message prompt when no virus is detected by Universal AV.
- Click on **Apply** button to apply the changes made.

4.1.3 UAV Engines Exclusions

To exclude the antivirus engine used by the Universal AV, follow the step below:

- In the **SecureAPlus Settings** window, click on **Universal AV** on the left menu and click on the **Exclusions** tab.

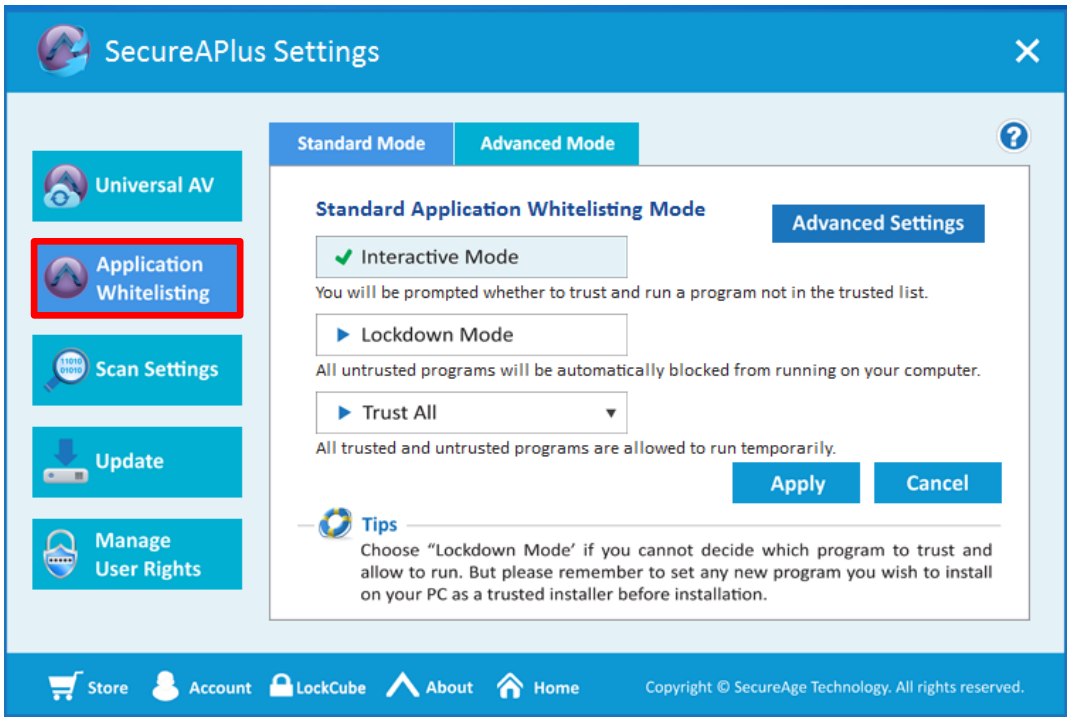


- Uncheck the engines that you want to exclude.
- Click on **Apply** button to apply the changes made.

4.2 Application Whitelisting

You can view the Application Whitelisting settings by following the steps as below:

- Start SecureAPlus. Please refer to **Section 2.1** for the steps to start SecureAPlus.
- In **SecureAPlus** window, click on the **Settings** icon to view the settings.
- In the **SecureAPlus Settings** window, click on **Application Whitelisting** on the left menu.
- The **Standard Mode** tab will be displayed.

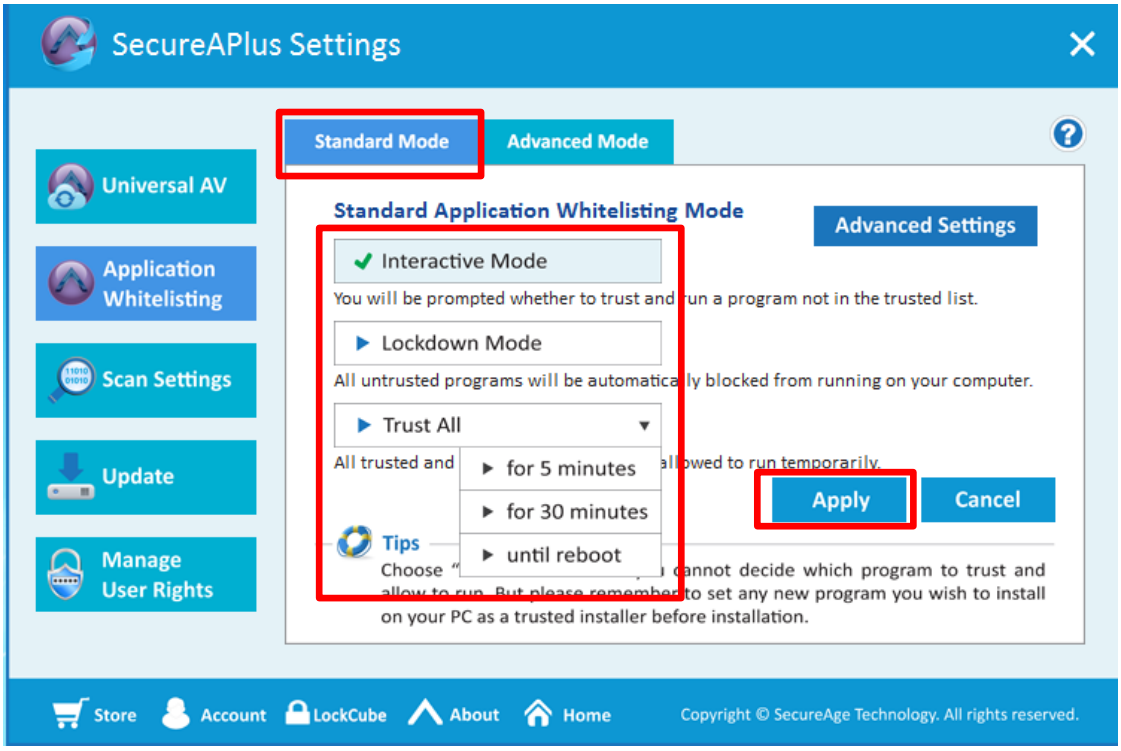


4.2.1 Application Whitelisting Standard Mode

In the **Standard Mode** tab, users can manage the Standard Application Whitelisting Mode.

- Select the options under **Standard Application Whitelisting Mode**:

- Interactive Mode (Default)
- Lockdown Mode
- Trust All for 5 minutes/30 minutes/until reboot



- Click on **Apply** button to apply the changes made.

Note:

- This corresponds to selecting the modes via the SecureAPlus Tray Icon Menu (**Section 2.2**).
- For users who are unable to decide which program to trust or allow to run, choose “Lockdown Mode” as it will block all untrusted files straight away instead of asking user for further actions.

4.2.2 Application Whitelisting Advanced Mode

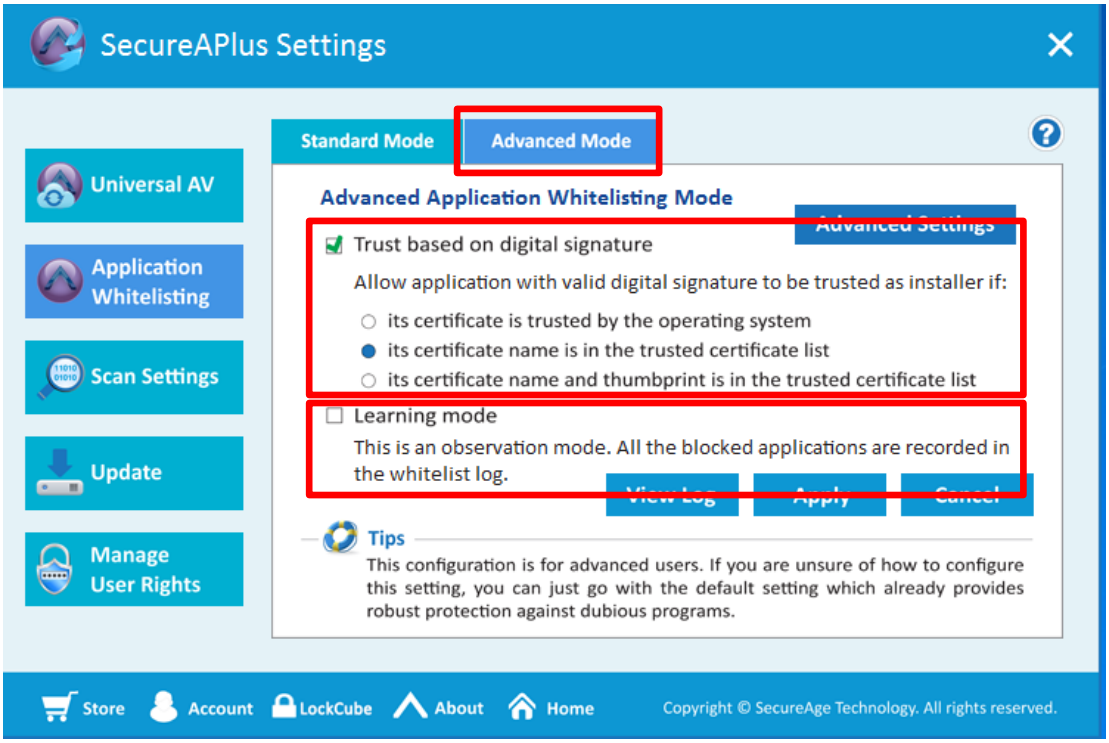
In the **Advanced Mode** tab, users can manage the Advanced Application Whitelisting Mode.

- **Trust based on digital signature** (default) – Check on the checkbox beside it to trust files as a trusted installer based on their digital signature even though these files are not in the Application Whitelisting.

  Allow application with valid digital signature to be trusted as installer if:

  - **its certificate is trusted by the operating system** – Select the radio button beside it to allow applications to be trusted so long if it is trusted by the OS.
  - **its certificate name is in the trusted certificate list** (default) – Select the radio button beside it so that only applications with certificate name listed in the trusted certificate list will be trusted. (Refer to **Section 7.2.3 – Trusted Certificate**)
  - **its certificate name and thumbprint is in the trusted certificate list** – Select the radio button beside it so that only applications with certificate name and thumbprint listed in the trusted certificate list will be trusted. (Refer to **Section 7.2.3 – Trusted Certificate**)

- **Learning mode** – Check on the checkbox beside it to turn on learning mode so that all the applications which are supposed to be blocked by Application Whitelisting will be written to a log file instead.



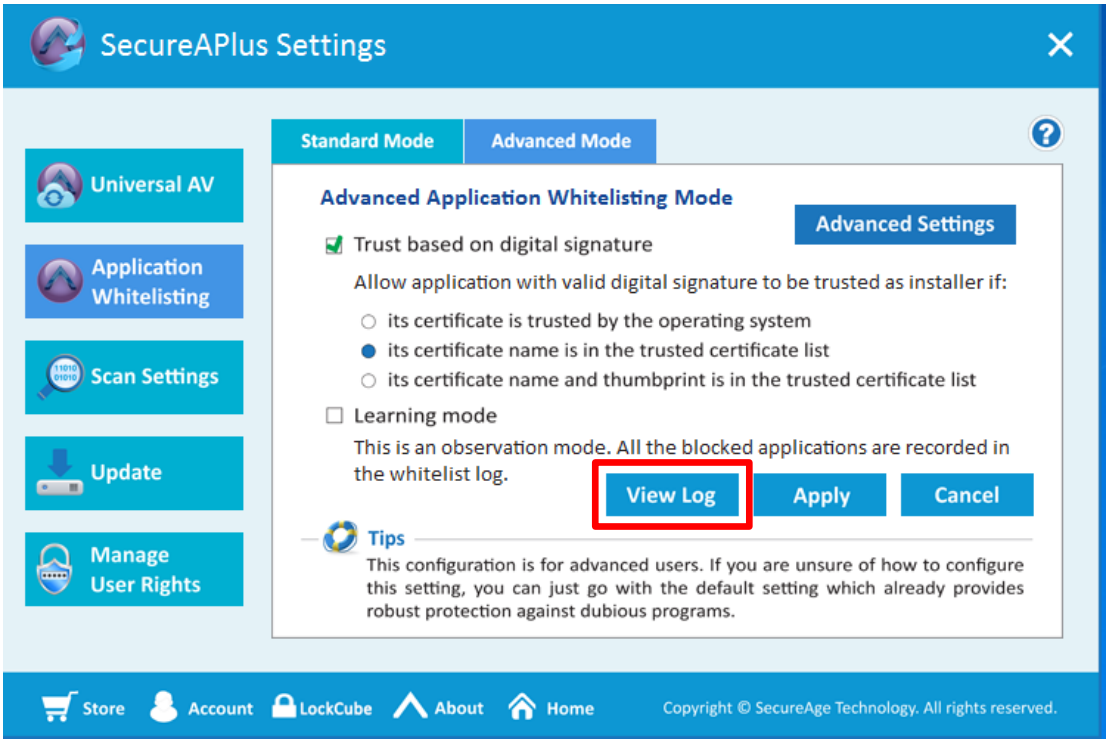
- Click on **Apply** button to apply the changes made.

Note:

- During initial installation, Application Whitelisting will do a whitelisting on the system to whitelist the files and creates a whitelist database file at the end. It will use this whitelist file to check whether the files are trusted or not.
- The Application Whitelisting feature will immediately kicks in right after installation, so even while it is still doing the initial whitelist creation, Application Whitelisting will start to prompt when a new file or application is being executed.
- By default, if the file is not in the whitelist, it will be trusted using its digital signature instead but only if it is under the trusted certificate list.
- Normally, learning mode is being used for testing purposes or for learning the behaviour of Application Whitelisting.

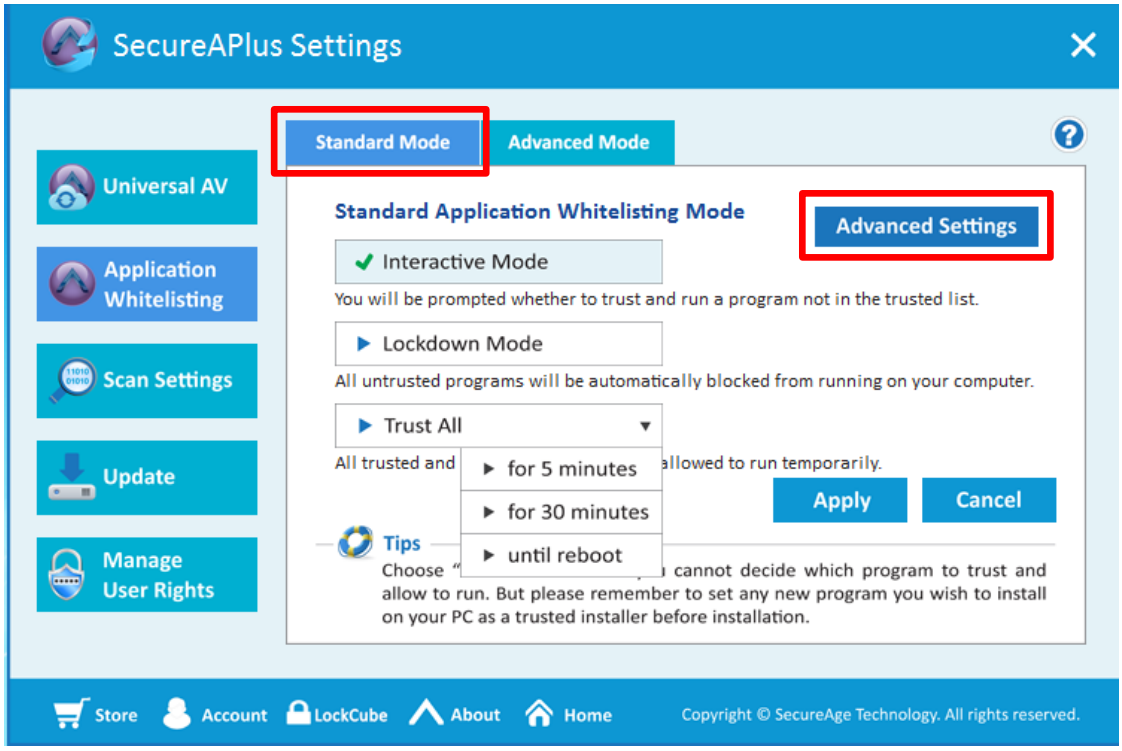
To view the application whitelisting log, follow the step below:

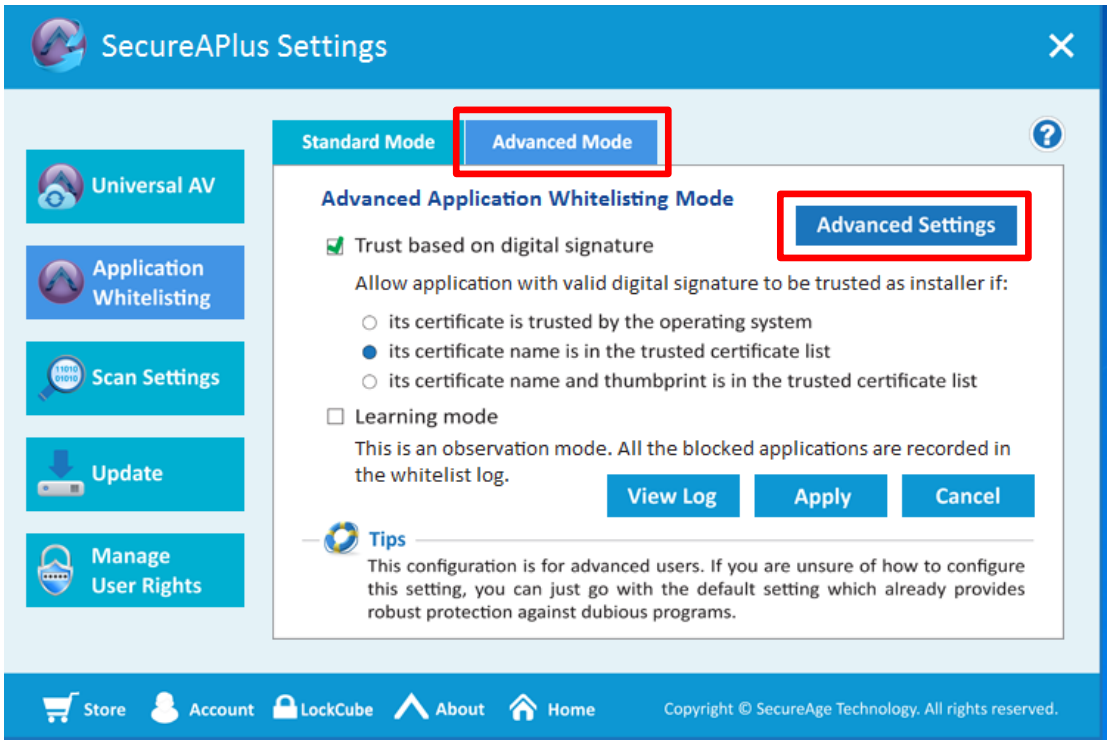
- Click on **View Log** button, it will launch the log using the notepad.



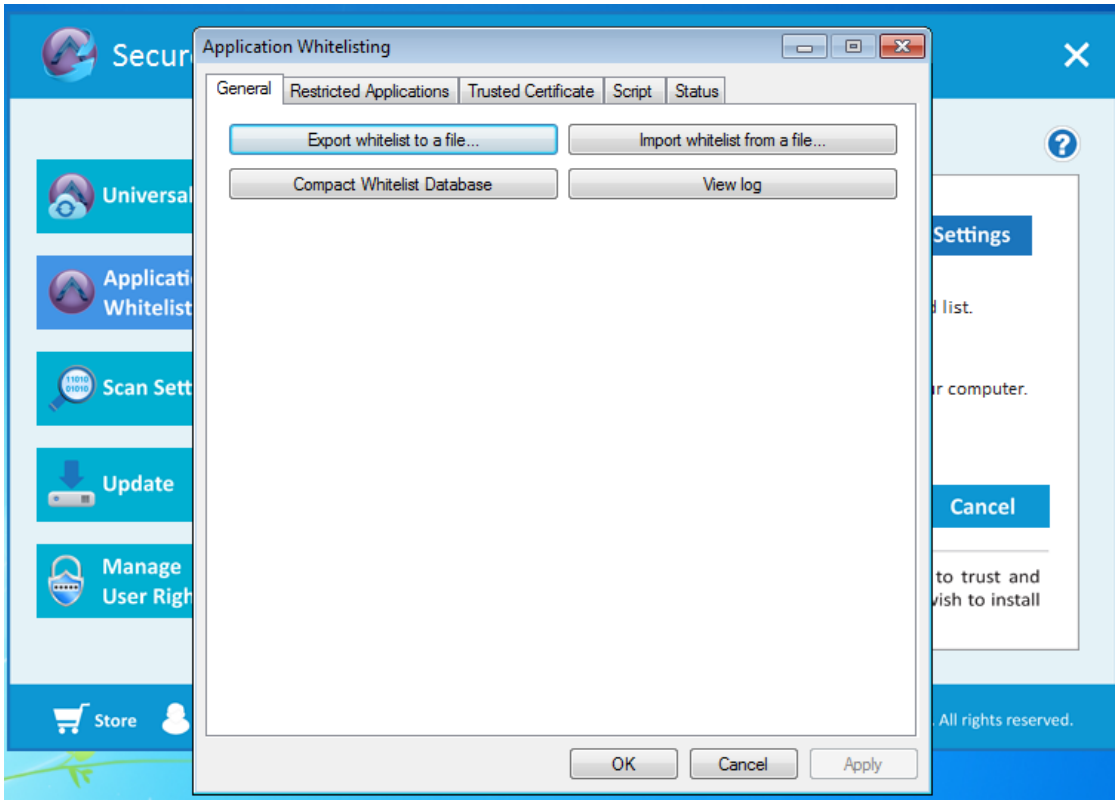
To view the advanced settings for Application Whitelisting, follow the steps below:

- Click on the **Advanced Settings** button within either the **Standard Mode** tab or **Advanced Mode** tab under **Application Whitelisting** on the left menu. The **Application Whitelisting** window will launch.

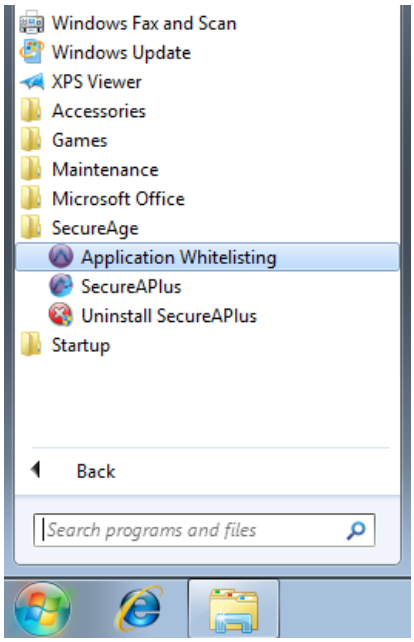




- The **Application Whitelisting** window will launch.



- Alternatively to navigate to this **Application Whitelisting Settings** window directly, you can click **Start**, point to **All Programs**. Click on **SecureAge** and click on **Application Whitelisting**.



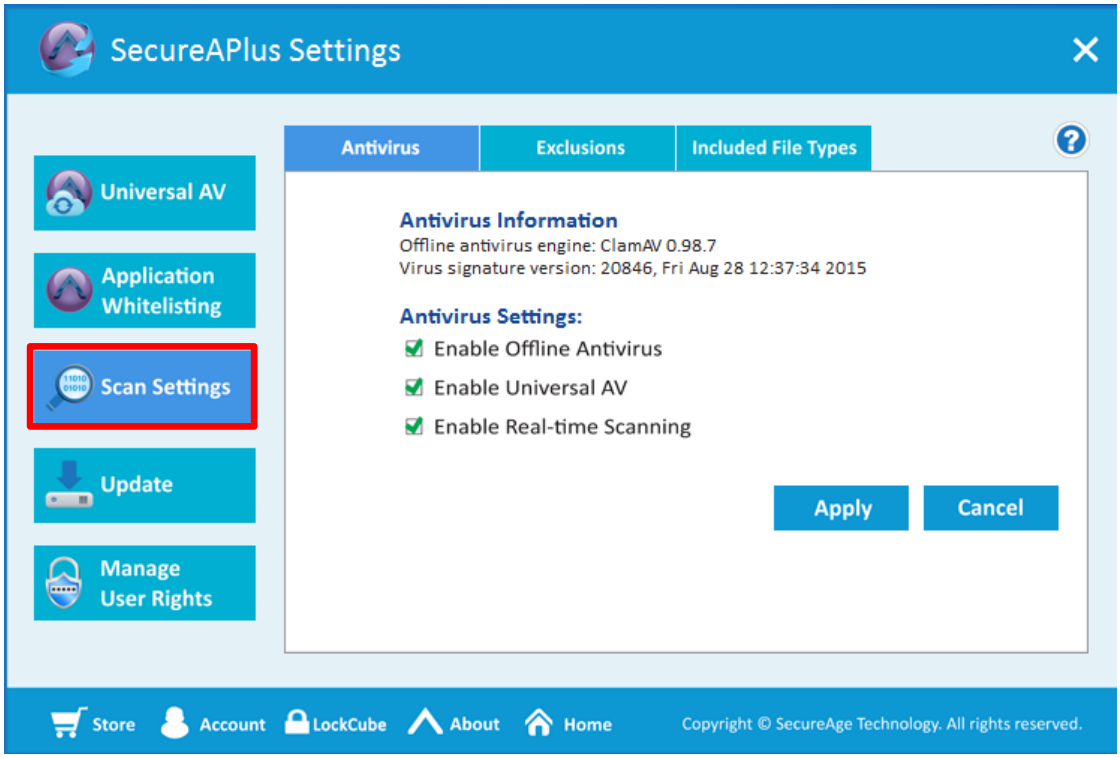
Note:

- Refer to **Section 7.2** for the detailed advanced settings of Application Whitelisting.

4.3 Scan Settings

Users can disable the real-time scanning if they wish to by following the steps below:

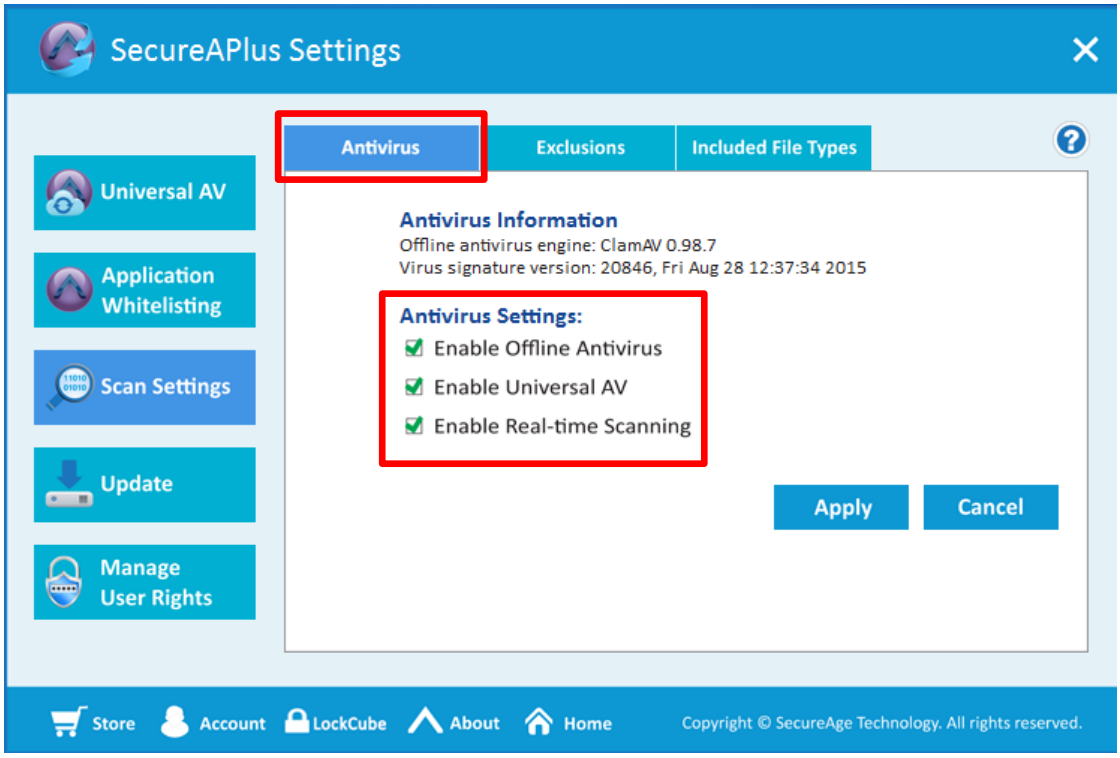
- Start SecureAPlus. Please refer to **Section 2.1** for the steps to start SecureAPlus.
- In **SecureAPlus** window, click on the **Settings** icon to view the settings.
- In the SecureAPlus Settings window, click on **Scan Settings** on the left menu.



4.3.1 Antivirus

To setup your antivirus settings, follow the steps below:

- Start SecureAPlus. Please refer to **Section 2.1** for the steps to start SecureAPlus.
- In **SecureAPlus** window, click on the **Settings** icon to view the settings.
- In the **SecureAPlus Settings** window, click on **Scan Settings** on the left menu and click on the **Antivirus** tab.
- By default, **Offline Antivirus**, **Universal AV** and **Real-time Scanning** are enabled.

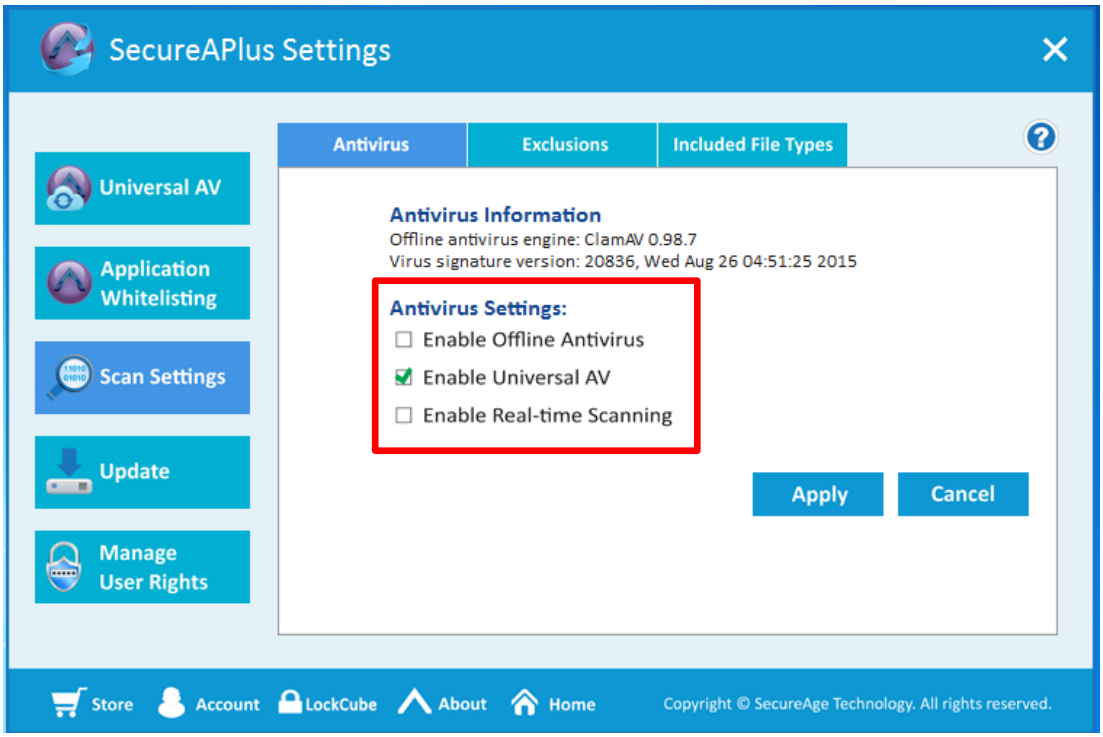


Note:

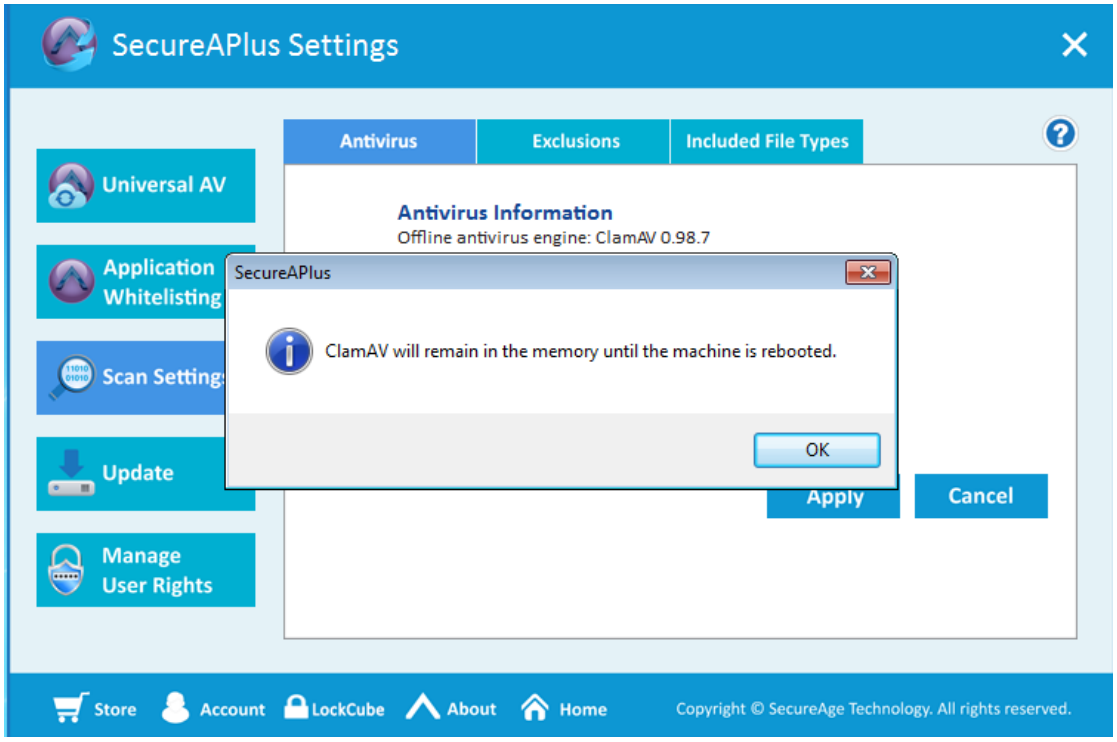
- **Universal AV with no real-time protection** will scan all the executable files on user's machine continuously in the cloud.
- **Universal AV with real-time protection** will scan all the executable files on user's machine continuously in the cloud. It also immediately scans any newly installed or created executable files and when an untrusted application is being executed.
- **Universal AV** and **Offline Antivirus** are both used for real-time scanning.
- For Universal AV, it requires to have online internet connection to connect to the cloud. But to also stay protected even without internet connection, the **Offline Antivirus** (ClamAV) will kick in which requires no internet connection and still able to protect user's machine.

4.3.1.1 Universal AV without real-time protection

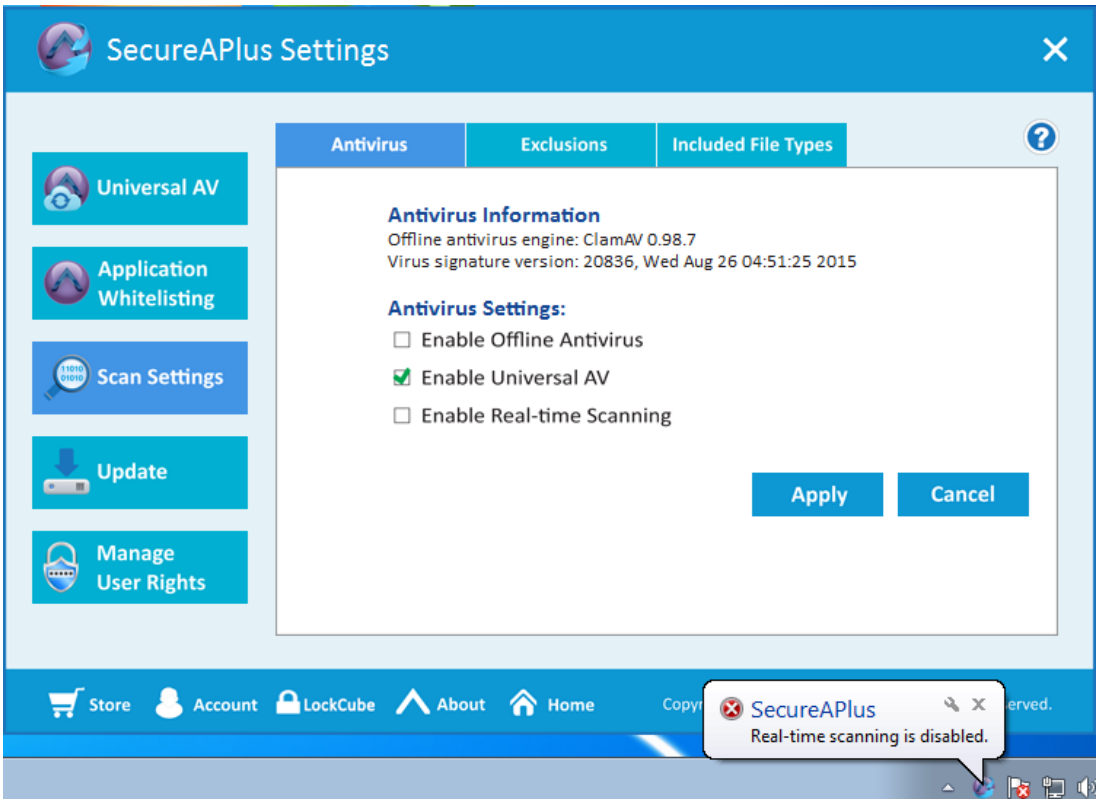
- For only protection from Universal AV, select the option as shown below.



- Click on **Apply** button to apply the changes made.
- A message will pop up saying that the ClamAV will still remain in the memory until the machine is rebooted. (Note: The message will only appear when user switches from **Enable Offline Antivirus** to disable.)

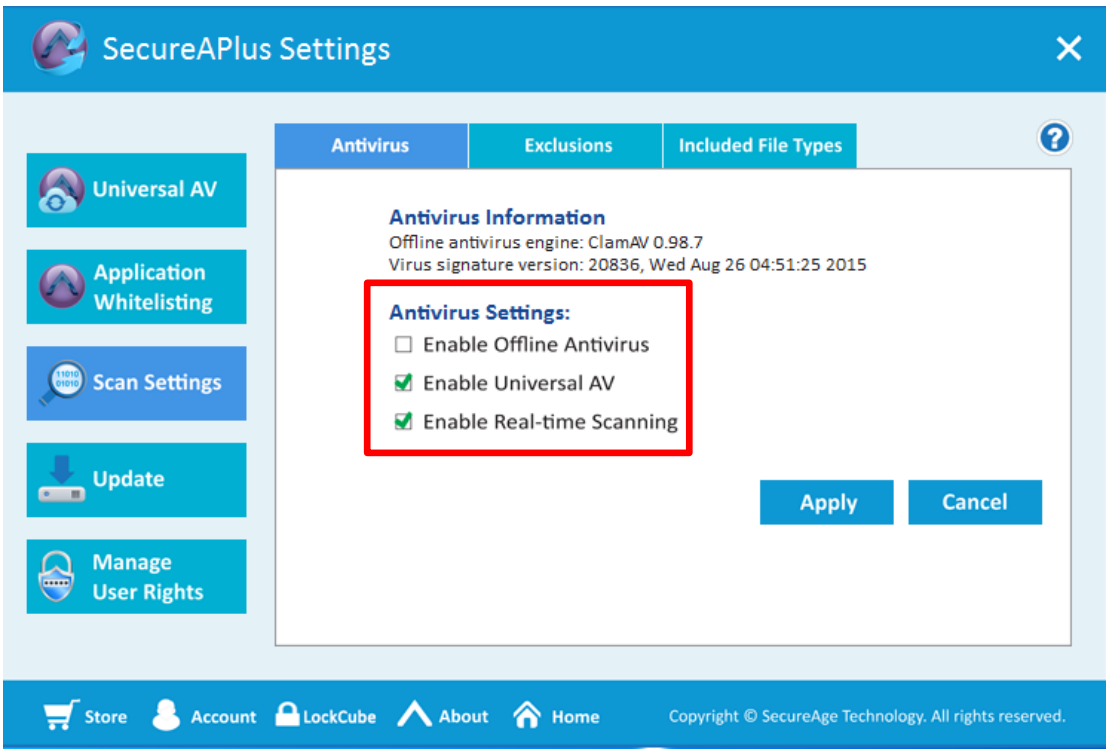


- The SecureAPlus tray icon will also display a message saying that the real-time scanning is disabled.

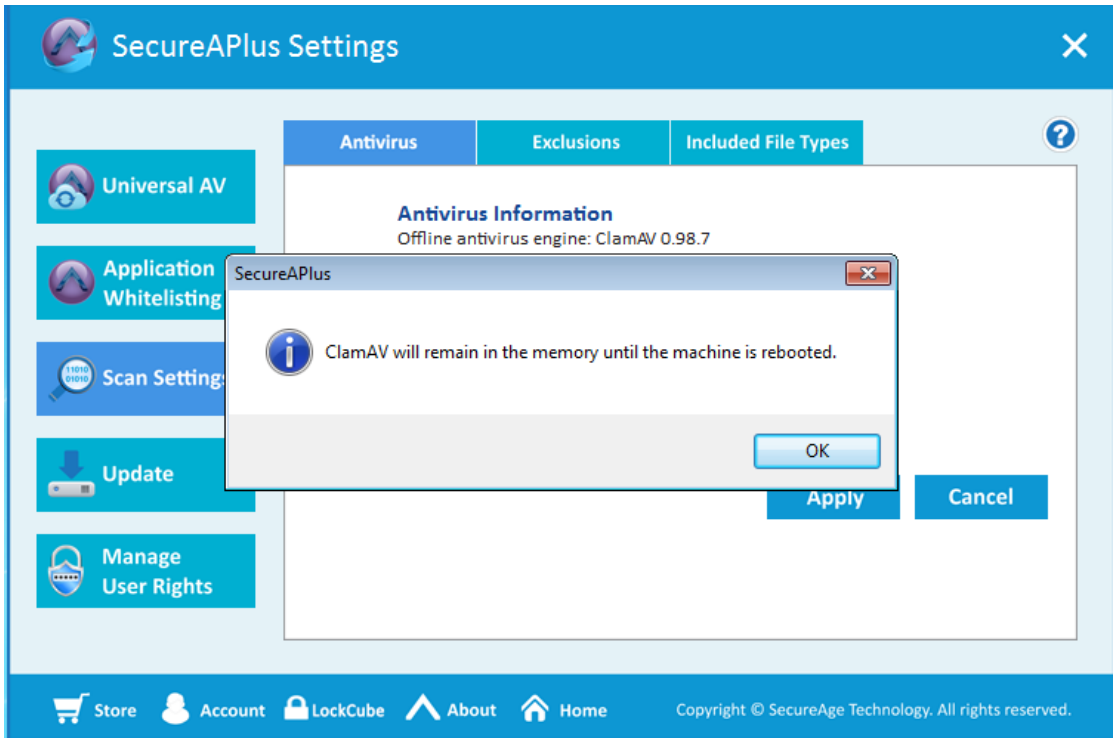


4.3.1.2 Universal AV with real-time protection

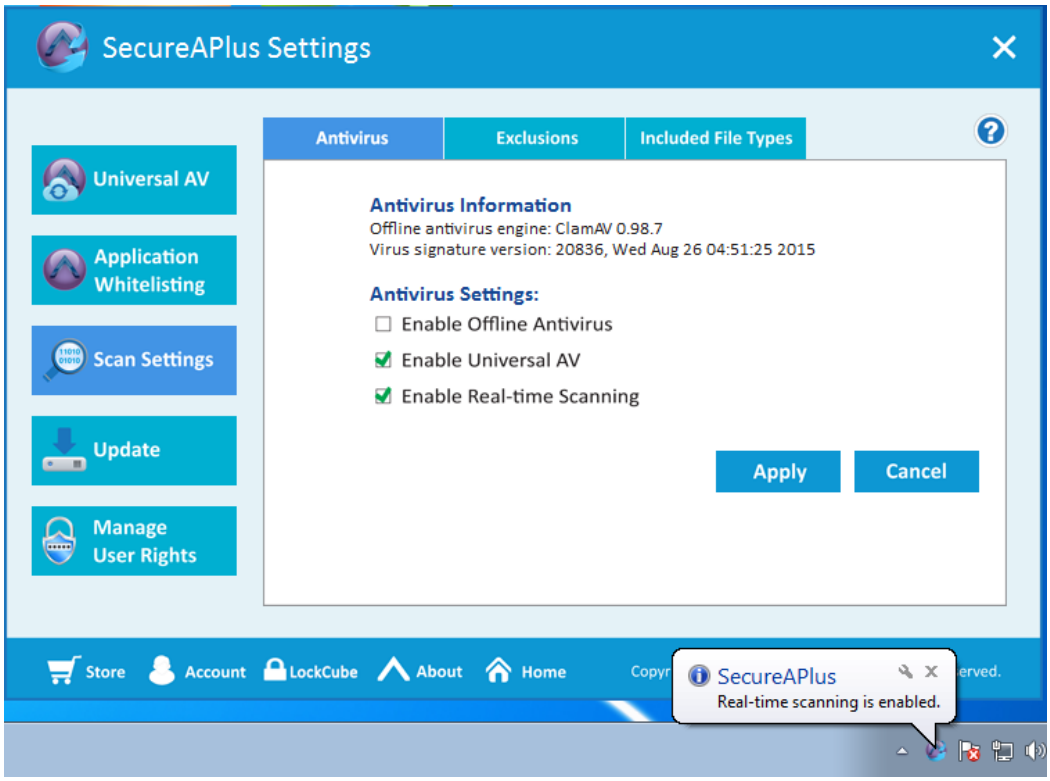
- For protection from Universal AV and real-time scanning by Universal AV, select the options as shown below.



- Click on **Apply** button to apply the changes made.
- A message will pop up saying that the ClamAV will still remain in the memory until the machine is rebooted. (Note: The message will only appear when user switches from **Enable Offline Antivirus** to disable.)

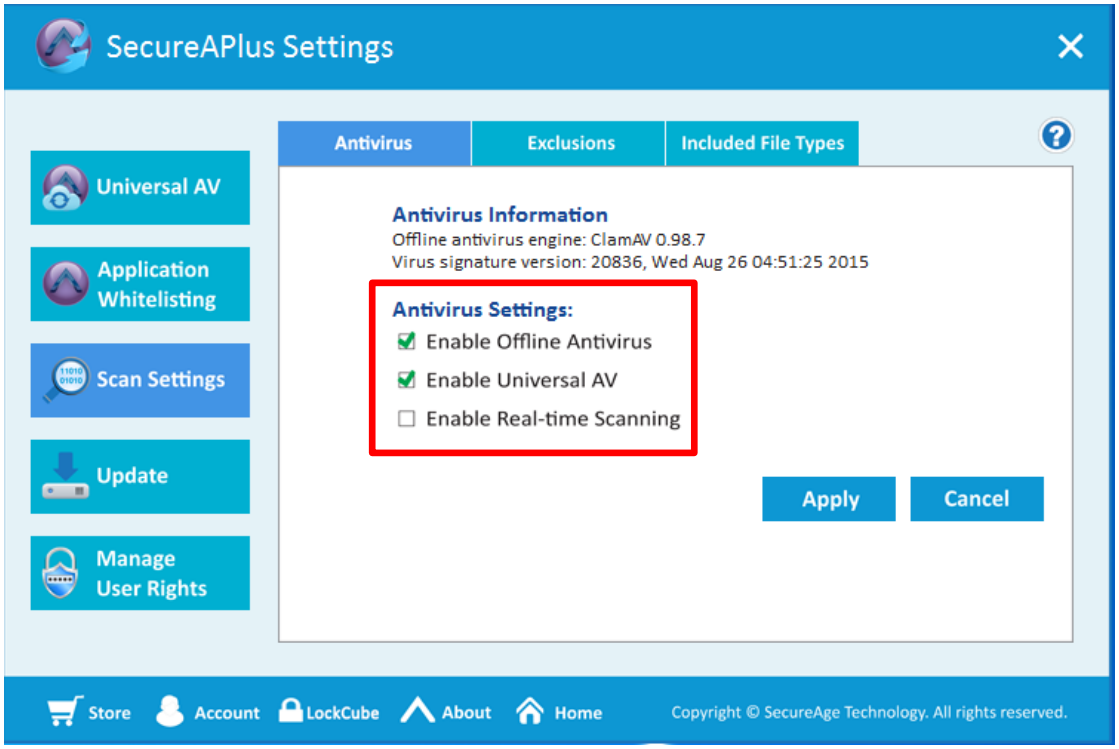


- The SecureAPlus tray icon will display a message saying that the real-time scanning is enabled.

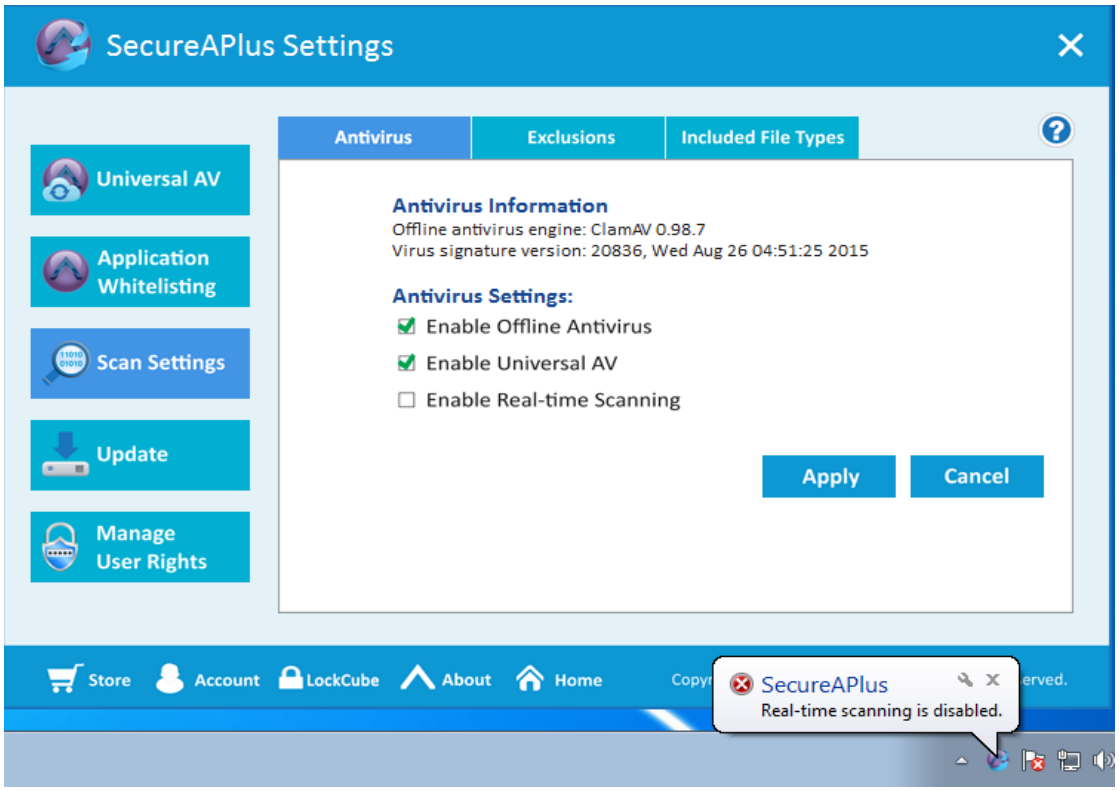


4.3.1.3 Universal AV and Offline Antivirus without real-time protection

- For both engines to be used for manual scanning (Eg: Right click to scan a file using Windows Explorer) and Universal AV to still do scanning at the background, select the options as shown below.

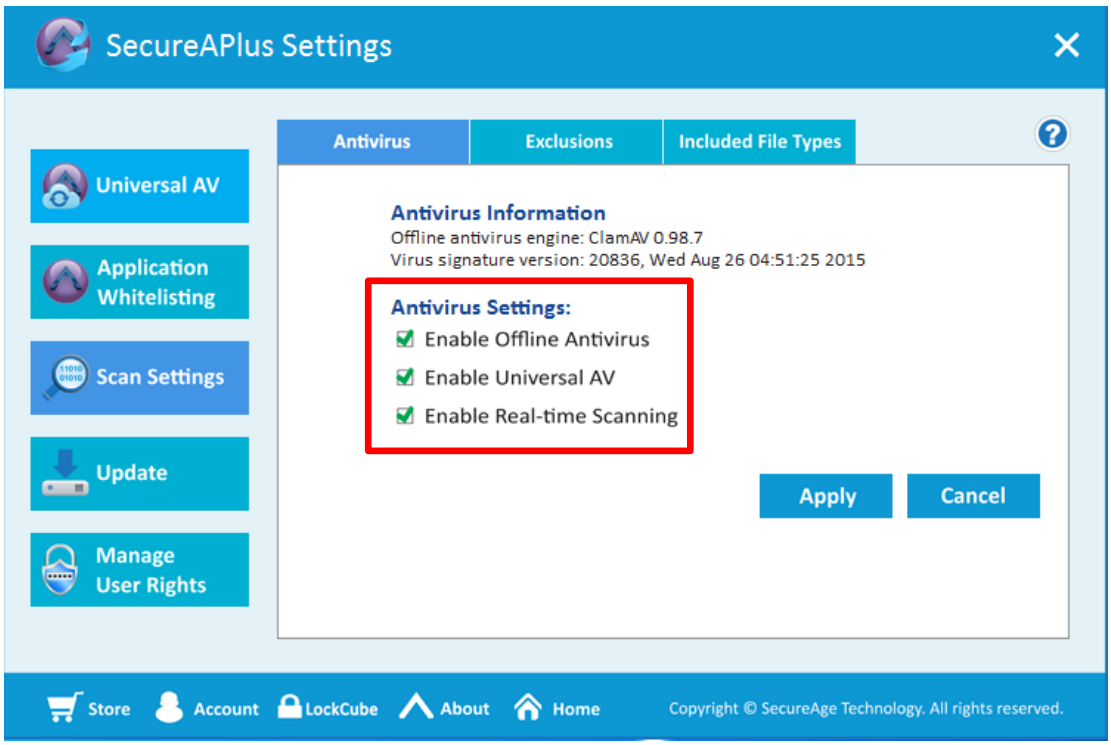


- Click on **Apply** button to apply the changes made.
- The SecureAPlus tray icon will display a message saying that the real-time scanning is disabled.

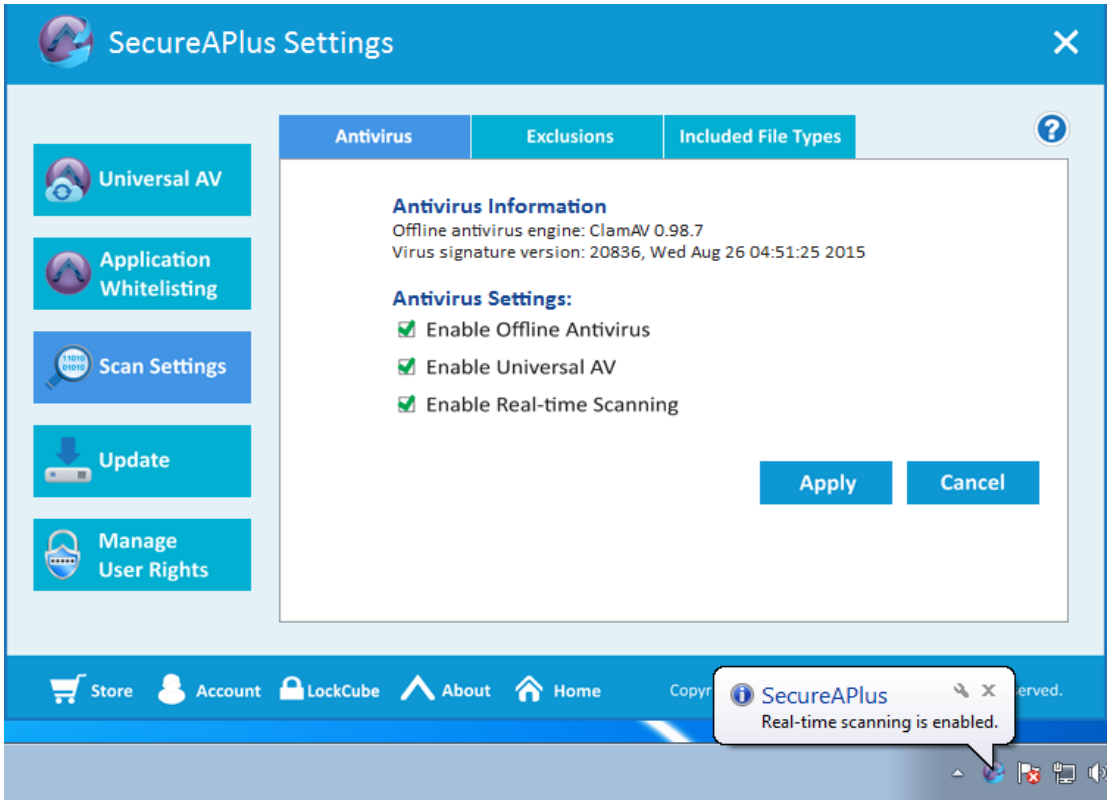


4.3.1.4 Universal AV with Offline Antivirus with real-time protection

- For full protection of Offline Antivirus and Universal AV with real-time scanning, select the options as shown below.

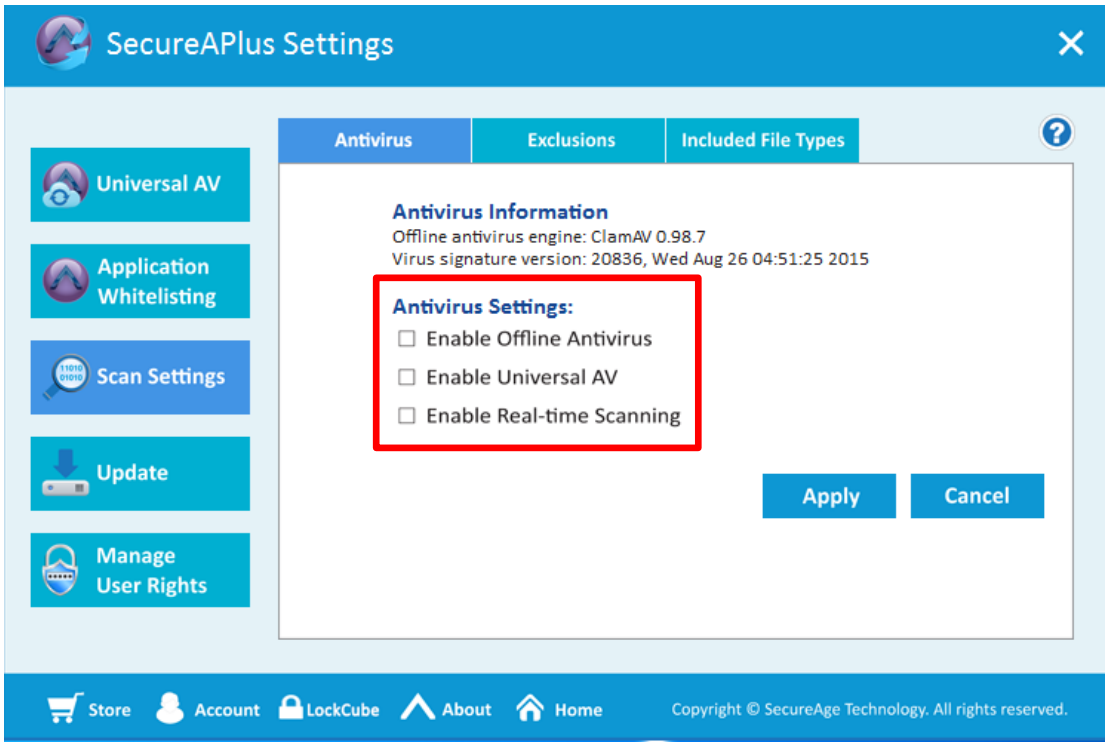


- Click on **Apply** button to apply the changes made.
- The SecureAPlus tray icon will display a message saying that the real-time scanning is enabled.

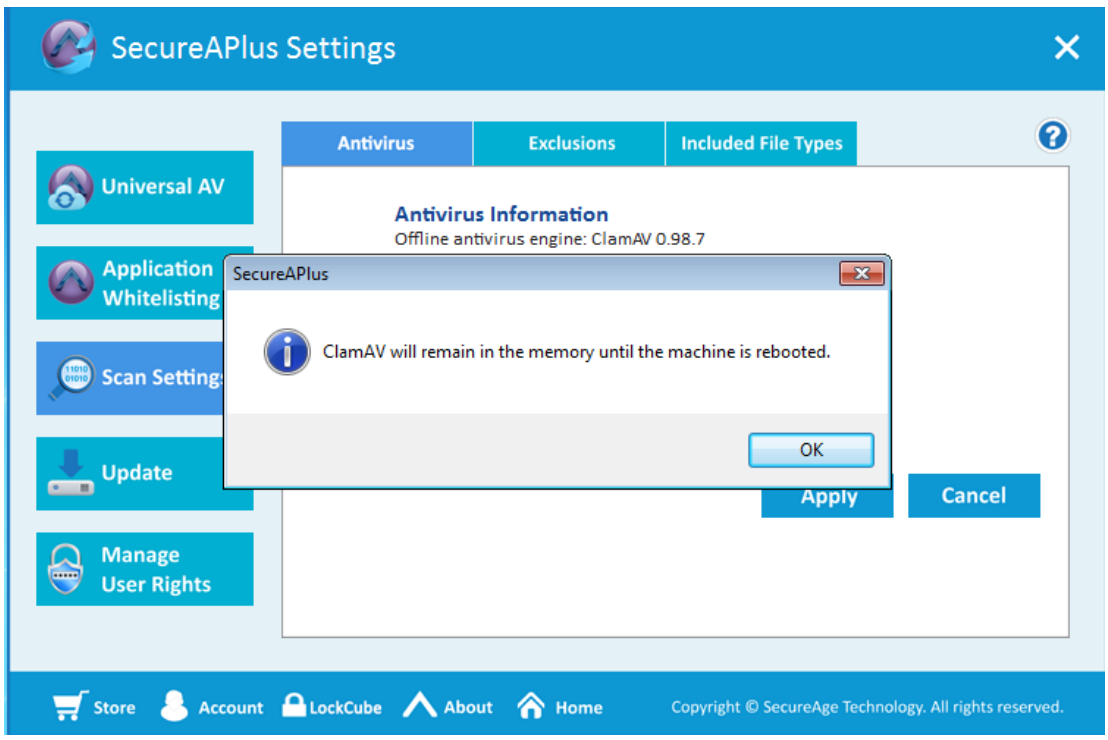


4.3.1.5 Application Whitelisting only

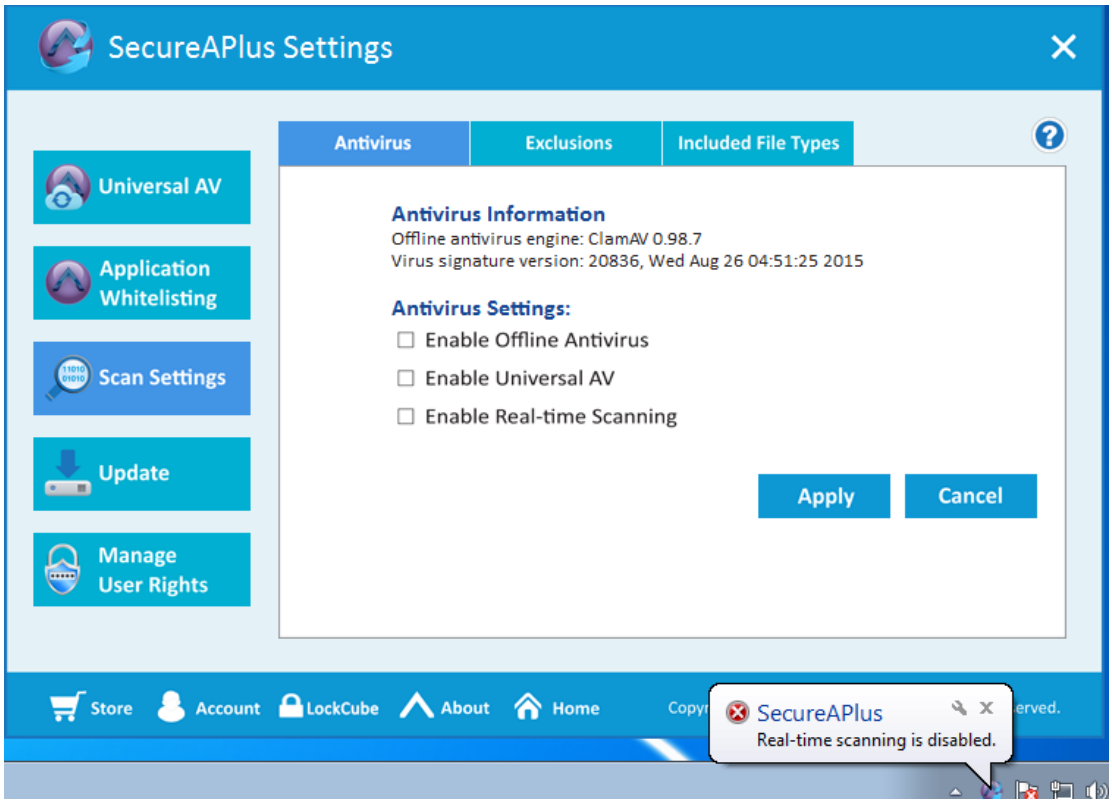
- For only protection from Application Whitelisting, do not enable any settings as shown below.



- Click on **Apply** button to apply the changes made.
- A message will pop up saying that the ClamAV will still remain in the memory until the machine is rebooted. (Note: The message will only appear when user switches from **Enable Offline Antivirus** to disable.)

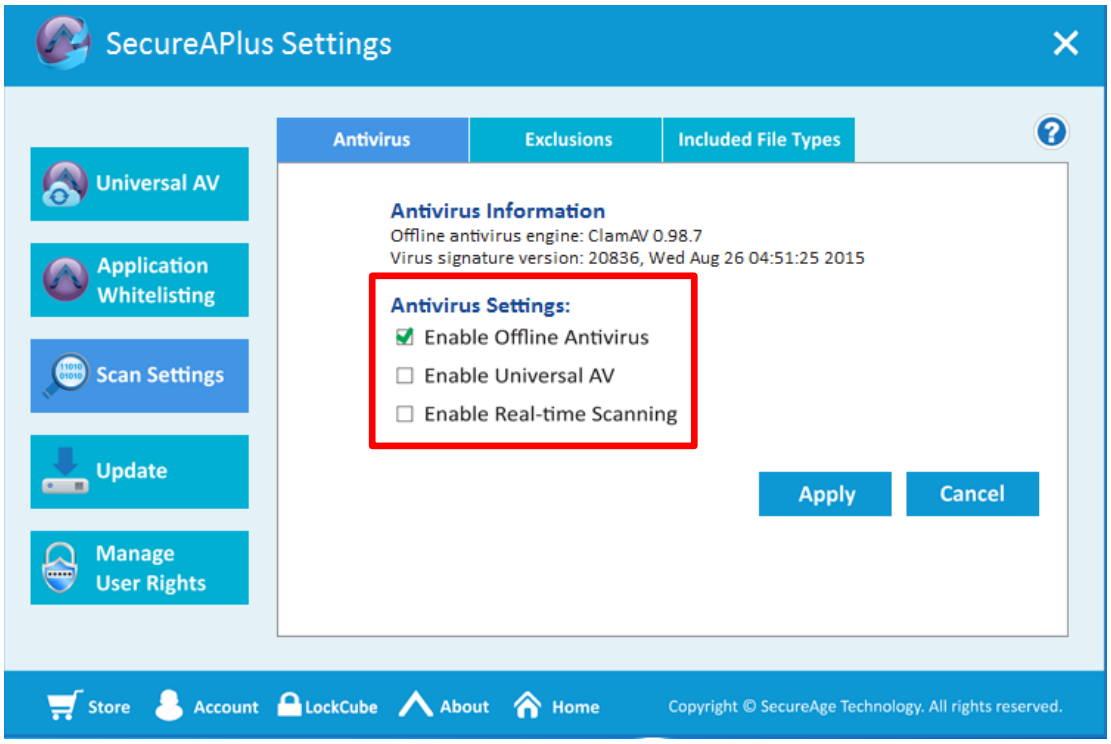


- The SecureAPlus tray icon will also display a message saying that the real-time scanning is disabled.

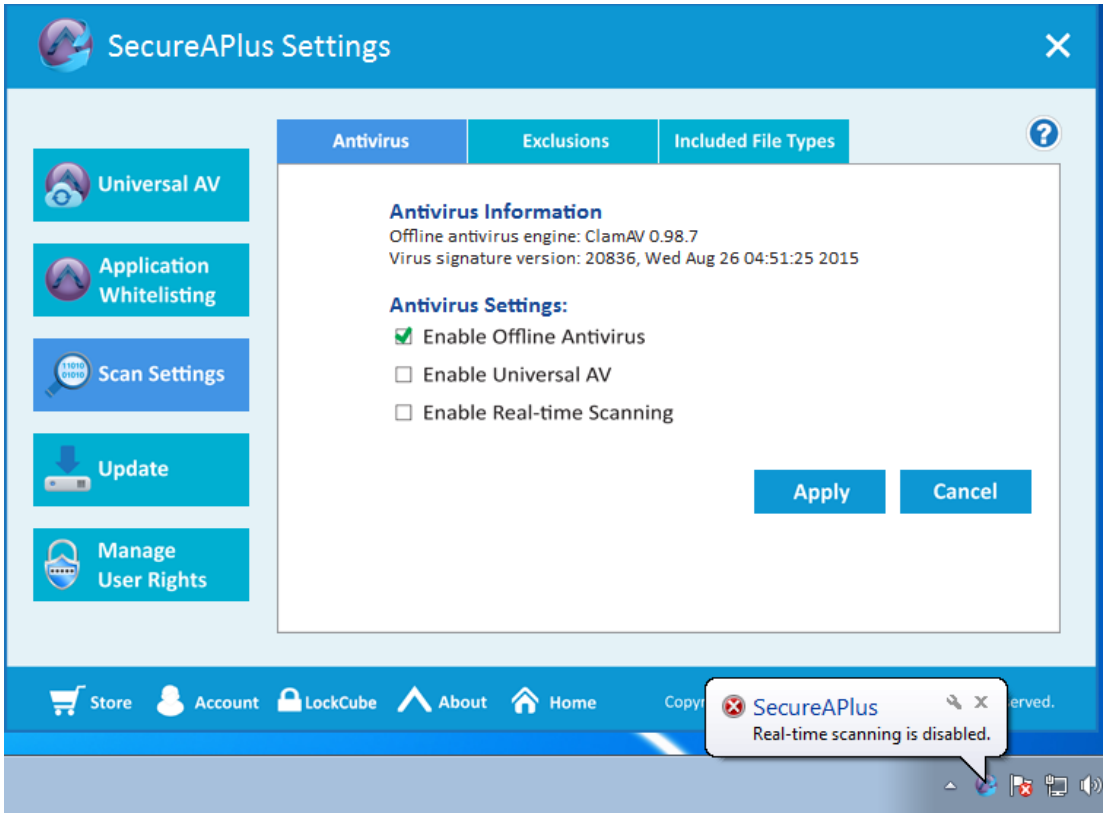


4.3.1.6 Offline Antivirus without real-time protection

- For only protection from Offline Antivirus only without any real-time scanning as shown below.

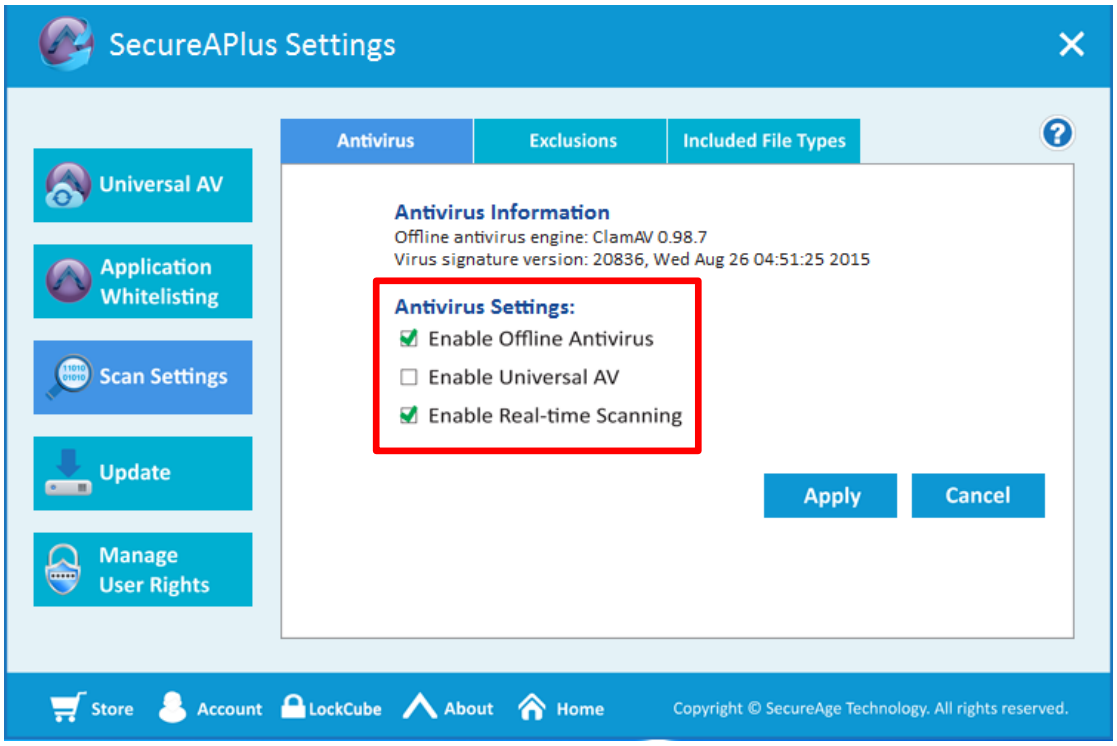


- The SecureAPlus tray icon will also display a message saying that the real-time scanning is disabled.

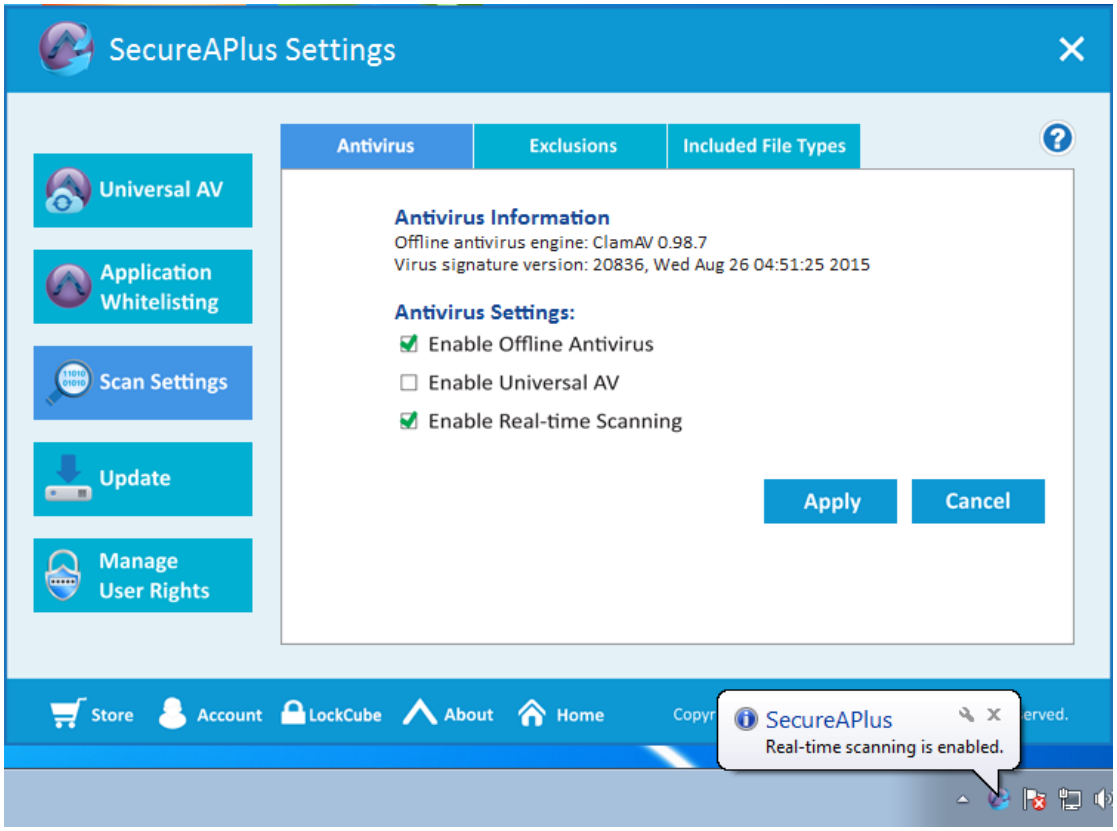


4.3.1.7 Offline Antivirus with real-time protection

- For only protection from Offline Antivirus only with real-time scanning as shown below.



- The SecureAPlus tray icon will also display a message saying that the real-time scanning is enabled.

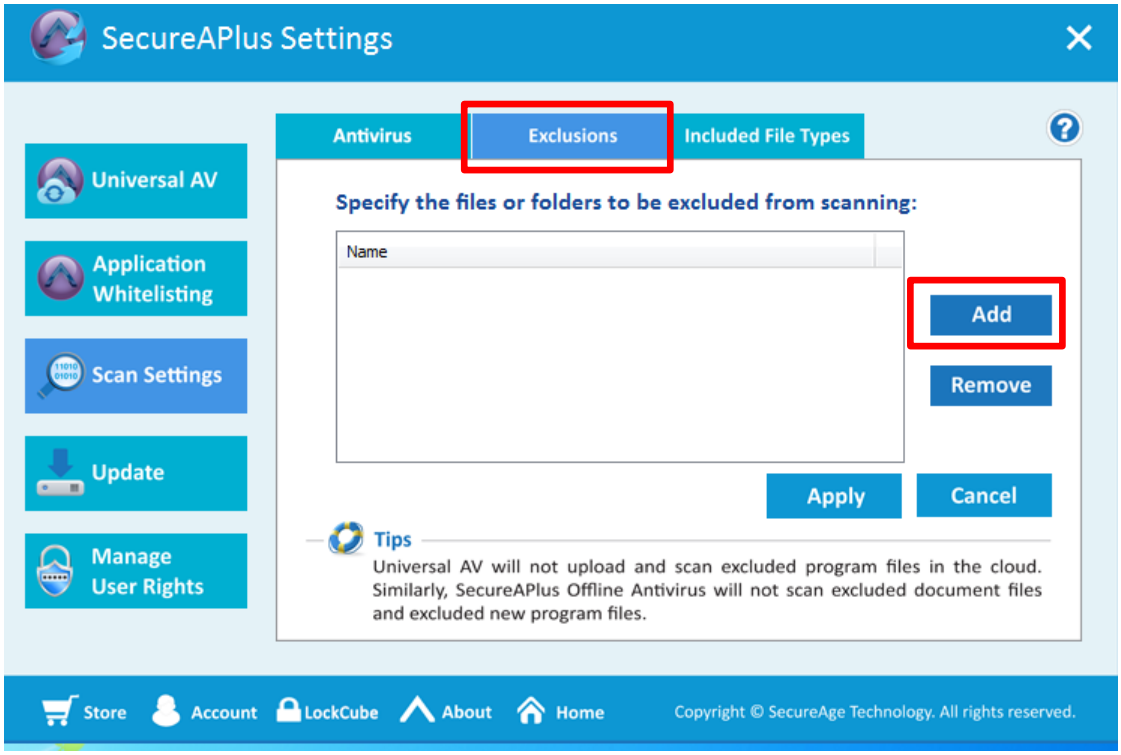


4.3.2 Files/Folders Exclusions

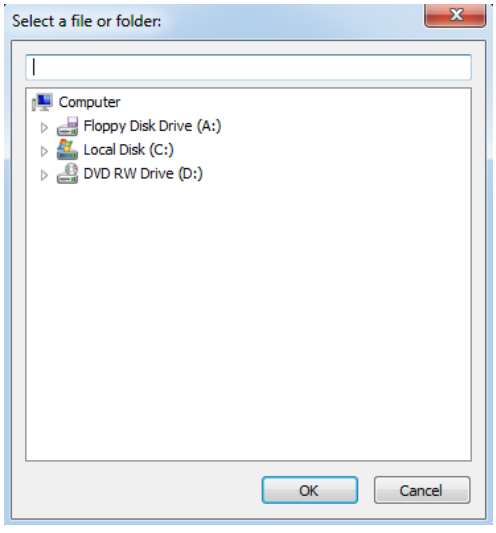
Certain folders or files can be specified under the list of exclusions in order for it to be excluded from scanning.

To setup your exclusions settings, follow the steps below:

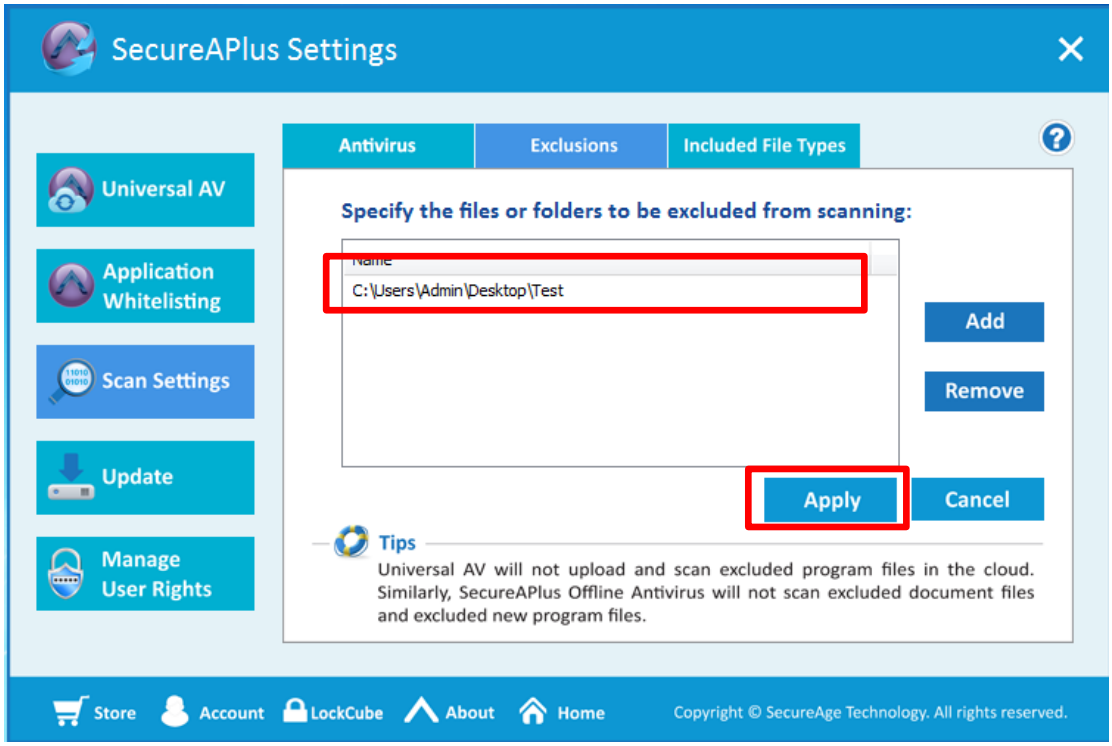
- Start SecureAPlus. Please refer to **Section 2.1** for the steps to start SecureAPlus.
- In **SecureAPlus** window, click on the **Settings** icon to view the settings.
- In the **SecureAPlus Settings** window, click on **Scan Settings** on the left menu and click on the **Exclusions** tab.
- Click on **Add** button to add folders or files to be excluded from scanning.



- Select the folder or file to be excluded on scanning and click on **OK** button.



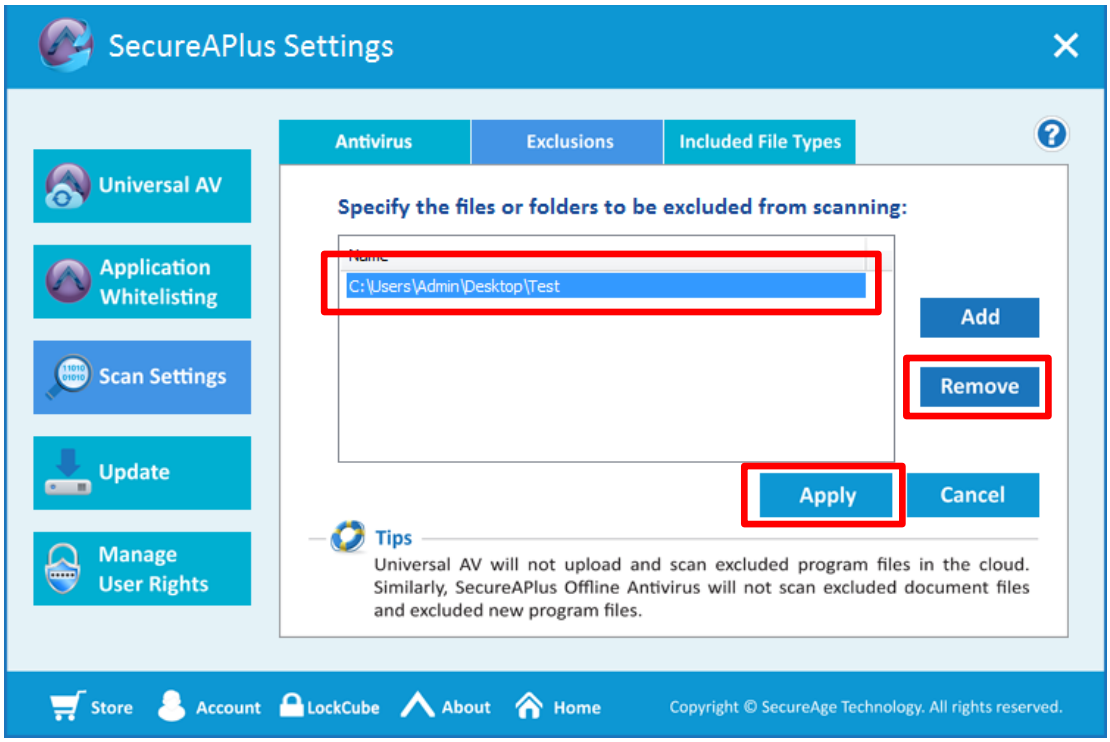
- It will be displayed under the list of exclusions.



- The newly added folders or files to be excluded on scanning will be added to the list of exclusions. Then click on **Apply** button to apply the changes made.

To remove folders or files that are excluded on scanning, follow the steps below to remove:

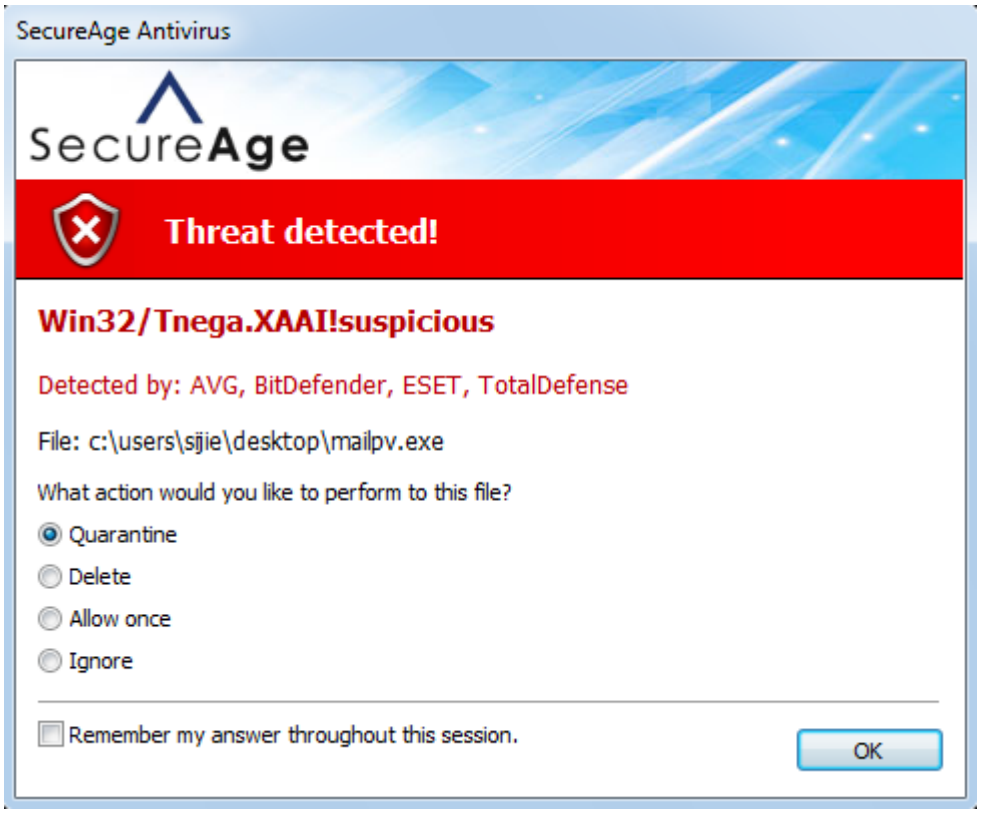
- Select the folders or files under the list and click on **Remove** button.



- The selected folders or files will be removed from the list of exclusions and will be included on scanning. Then click on **Apply** button to apply the changes made.

File exclusion during real-time scanning

SecureAPlus will prompt user when there is a threat detected. When user is sure that it is not a threat, select **Ignore** and click on the **OK** button. This will put the file into the list of exclusions which will be excluded from real-time scanning. User will not be prompted for further action on the file anymore.



However, to get prompted again for the same file, user has to manually remove it from the list of exclusions.

Note:

- Quarantine: Moves the infected file to an isolated area to prevent it from causing any issues or harm to the machine.
- Delete: Totally remove the infected file from the machine.
- Allow: Gives the infected file the permission to execute one time only. User will be prompted again when the infected file is being accessed the next time.
- Ignored permanently: Disregard the file totally even if it is an infected file and goes under the Ignored and Exclusion lists.

4.3.3 Included File Types

Certain file types can be specified under the list of extension in order for it to be included for real-time scanning.

By default the Antivirus client always includes the following extensions for real-time scanning:

New program files, .pdf, .docx, .doc, .xlsx, .xls, .pptx, .ppt

And all the executable files regardless of its file extension are also included.


Note:

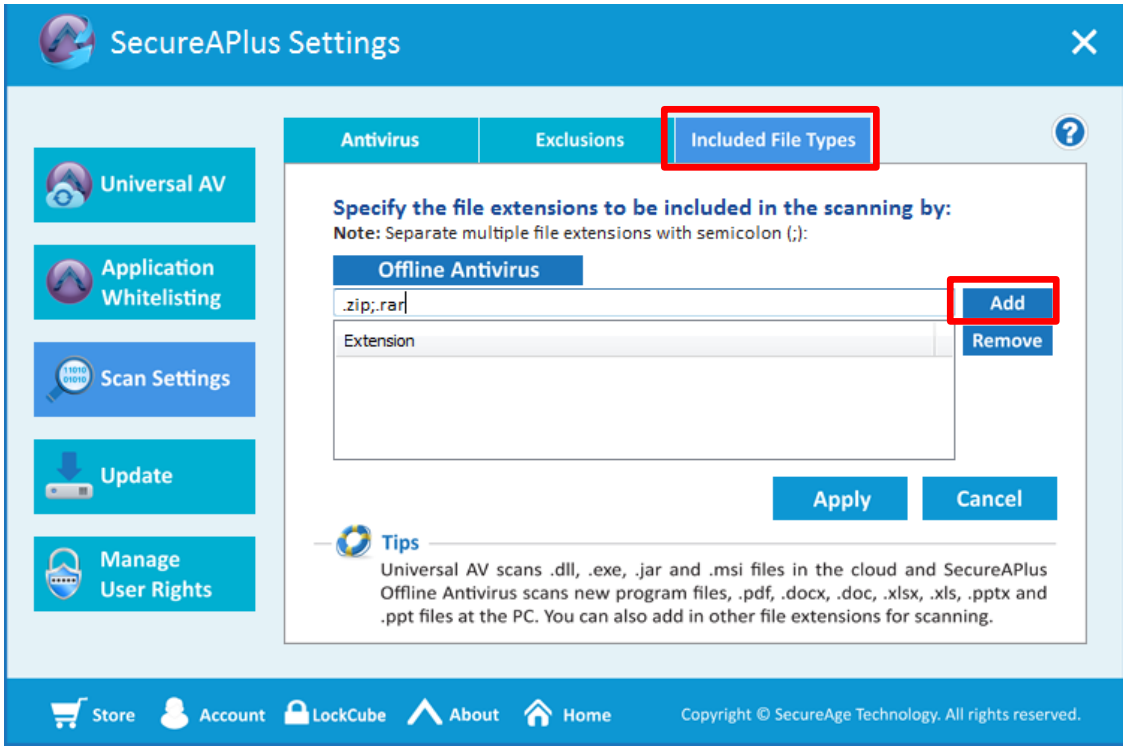
- With Universal AV installed and enabled, only new executable files will be scanned. Those executable files that has already been trusted and run will not go through the real-time scanning anymore. As continuous scanning is being done by the Universal AV server, there is no need to scan the same executable files on the local machine. Therefore with Universal AV, the speed will be improved tremendously.

To setup the file types to be included on real-time scanning settings, follow the steps below:

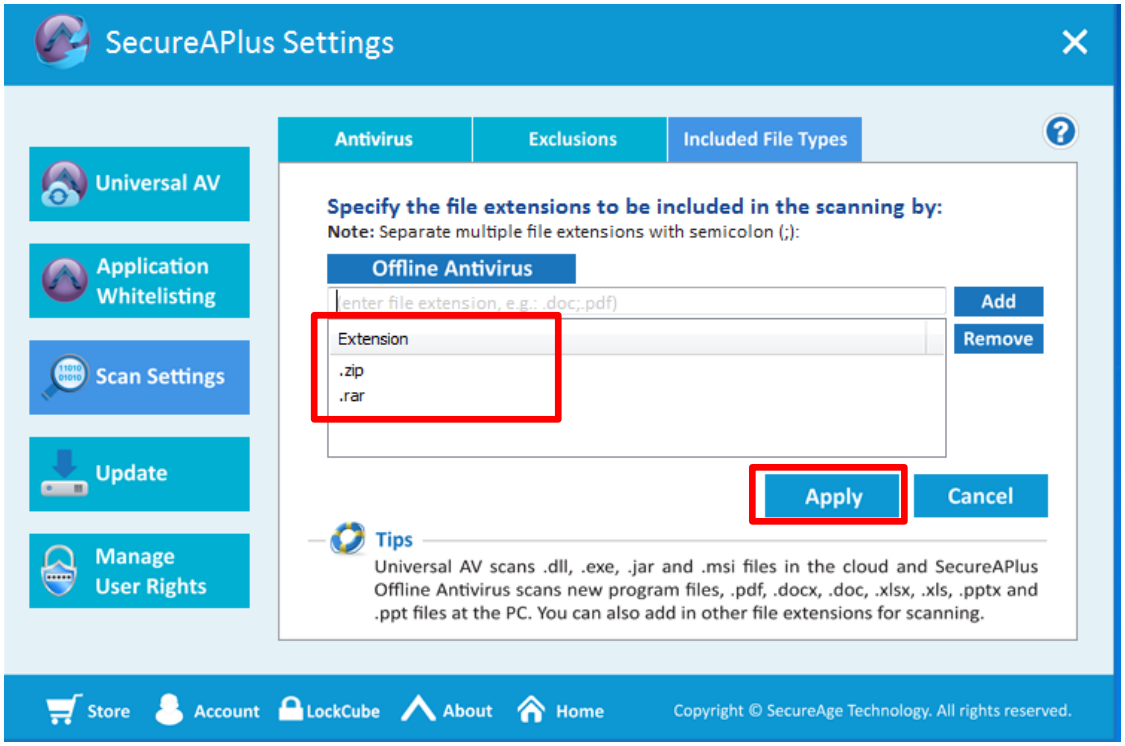
- Start SecureAPlus. Please refer to **Section 2.1** for the steps to start SecureAPlus.
- In **SecureAPlus** window, click on the **Settings** icon to view the settings.
- In the **SecureAPlus Settings** window, click on **Scan Settings** on the left menu and click on the **Included File Types** tab.

To add files to be included during real-time scanning, follow the steps below to add:

- Under **File extensions**, enter the extensions and click on **Add** button.

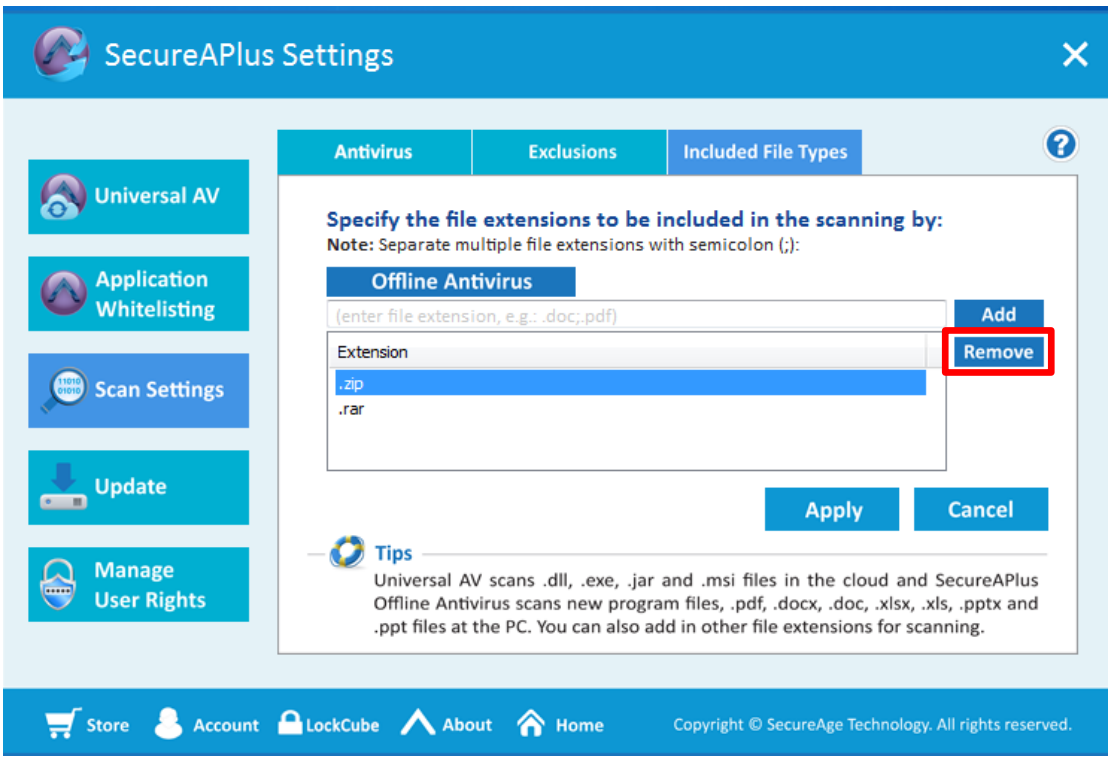


- The newly added file extension will be added to the list of extensions and will be included during real-time scanning. Then click on **Apply** button to apply the changes made.

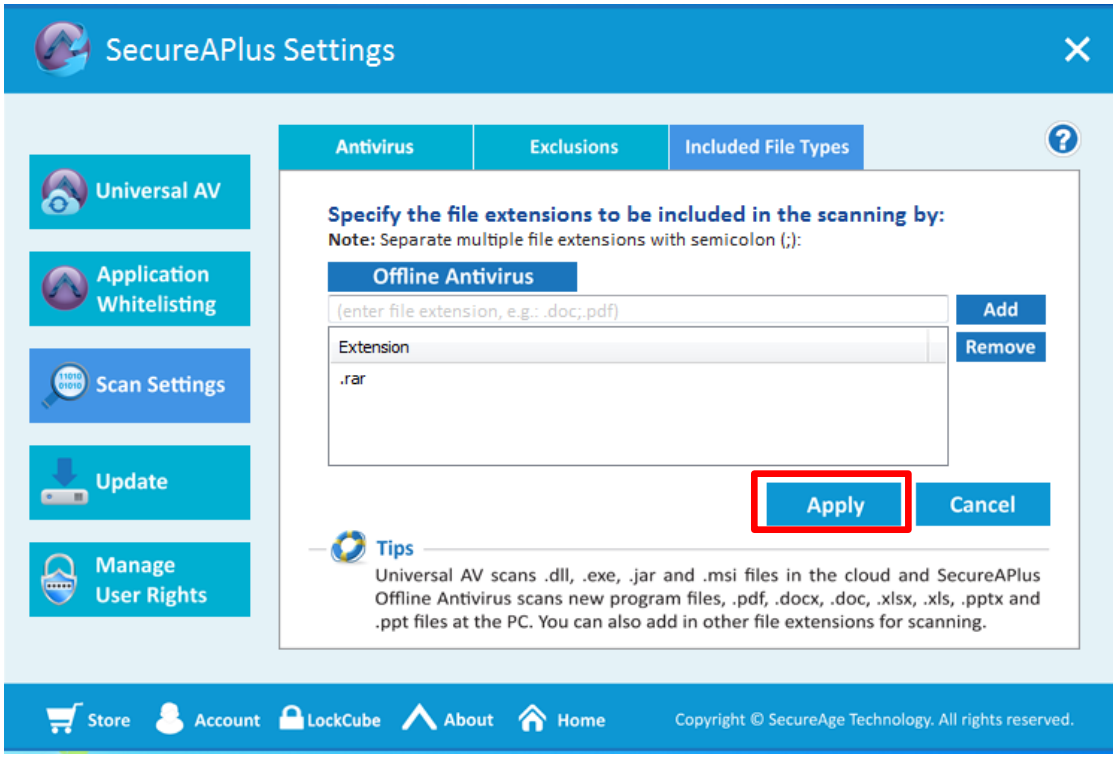


To remove files so that are included during real-time scanning, follow the steps below to remove:

- Under the list of extensions, select the extension and click on **Remove** button.



- The selected file extension will be removed from the list of extensions and will be excluded on real-time scanning. Then click on **Apply** button to apply the changes made.

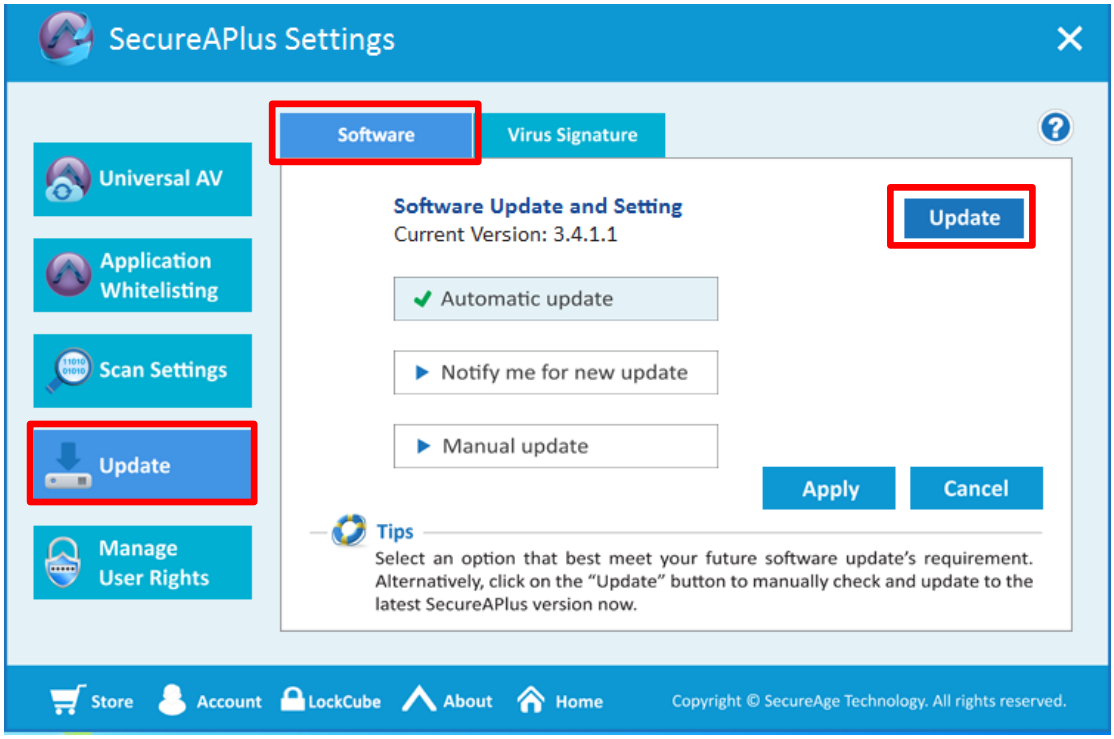


4.4 Update

4.4.1 Software

To setup your software update settings, follow the steps below:

- Start SecureAPlus. Please refer to **Section 2.1** for the steps to start SecureAPlus.
- In **SecureAPlus** window, click on the **Settings** icon to view the settings.
- In the **SecureAPlus Settings** window, click on **Update** on the left menu and click on the **Software** tab.
- To update the SecureAPlus software, click on the **Update** button, SecureAPlus will check if there's any new version updates.



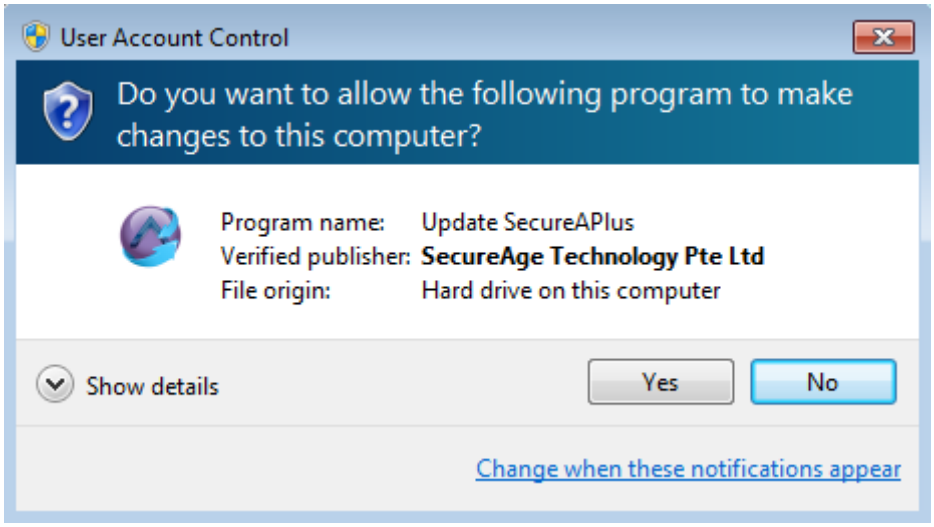
Under **Software Update** Options, you can select any of the listed options:

- **Automatic update.** – SecureAPlus will automatically update when there is a new software update. (This is the default selected option)
- **Notify me when an update is available.** – When new updates are available, SecureAPlus will notify user about it.
- **Manual update.** – SecureAPlus will not automatically check for any new updates.
- Click on **Apply** button to apply any changes made.

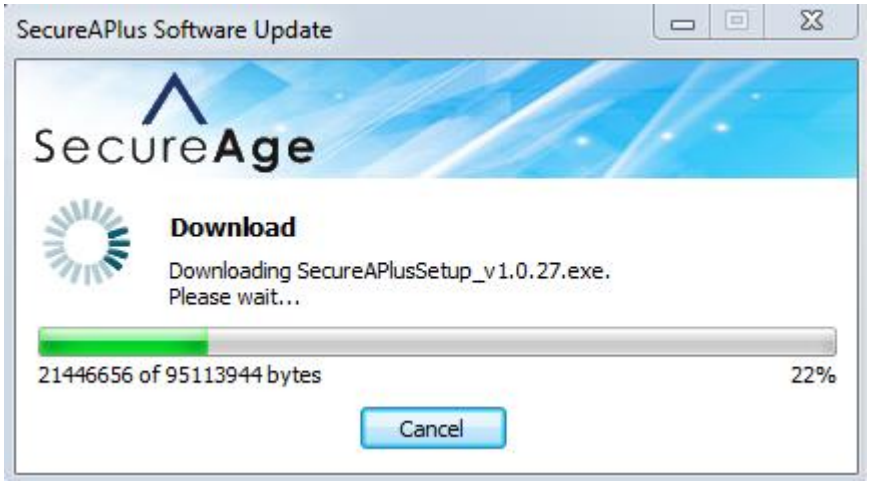
4.4.1.1 Automatic update

When there is a new software update, SecureAPlus will automatically update the software.

- Certain operating systems will require allowing **User Account Control** for updating SecureAge software. Click **Yes** to run update for SecureAPlus software, otherwise click **No**.



- It will start to download the new update.

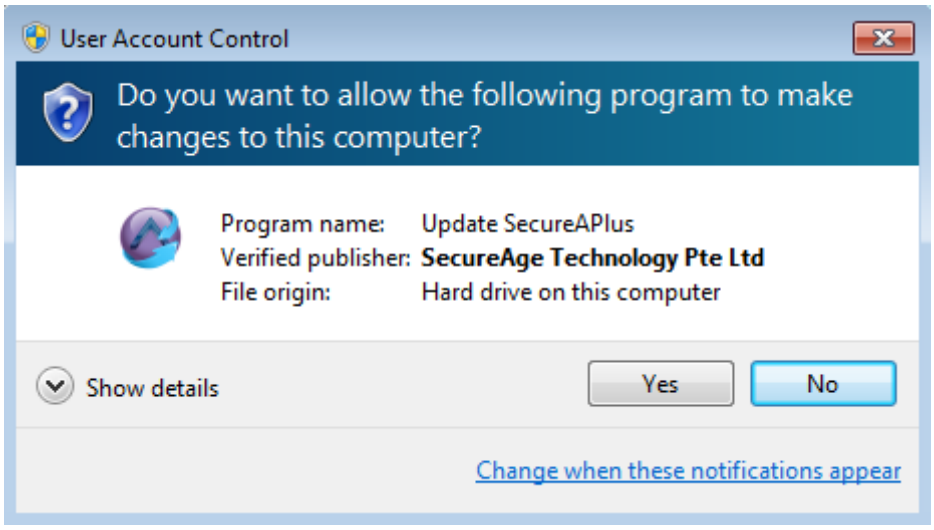


- Upon completion of the downloading, follow the installation steps to complete updating SecureAPlus.

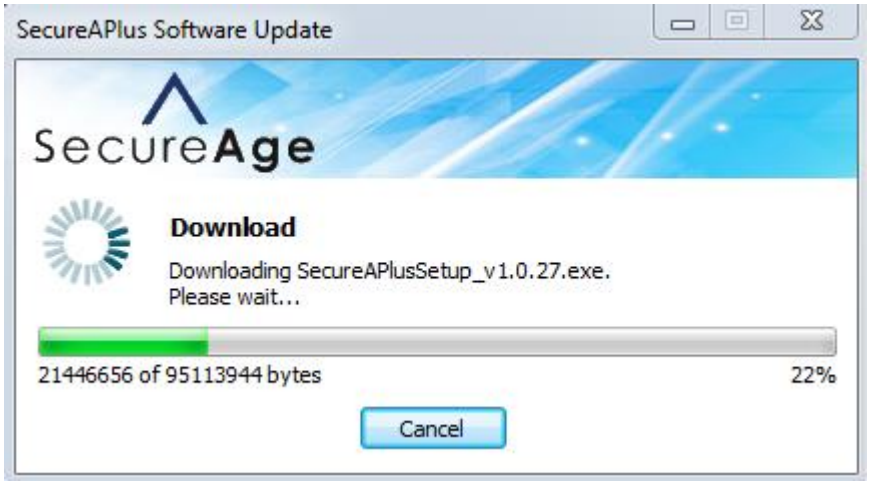
4.4.1.2 Notify me for new update

If user chooses the **Notify me when an update is available** option for **Software Update** Options, when there is a new software update, it will prompt user that there is an update available. Click on **Download & Install** to update, otherwise click **Cancel**.

- Certain operating systems will require allowing **User Account Control** for updating SecureAge software. Click **Yes** to run update for SecureAPlus software, otherwise click **No**.



- It will start to download the new update.

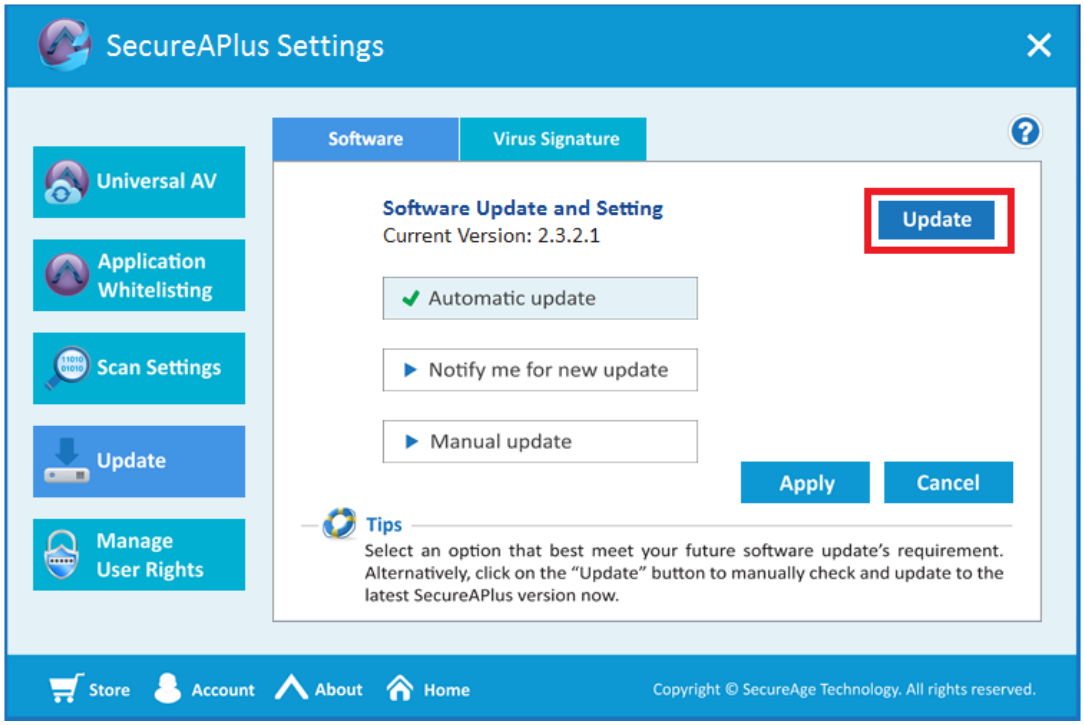


- Upon completion of the downloading, follow the installation steps to complete updating SecureAPlus.

4.4.1.3 Manual update

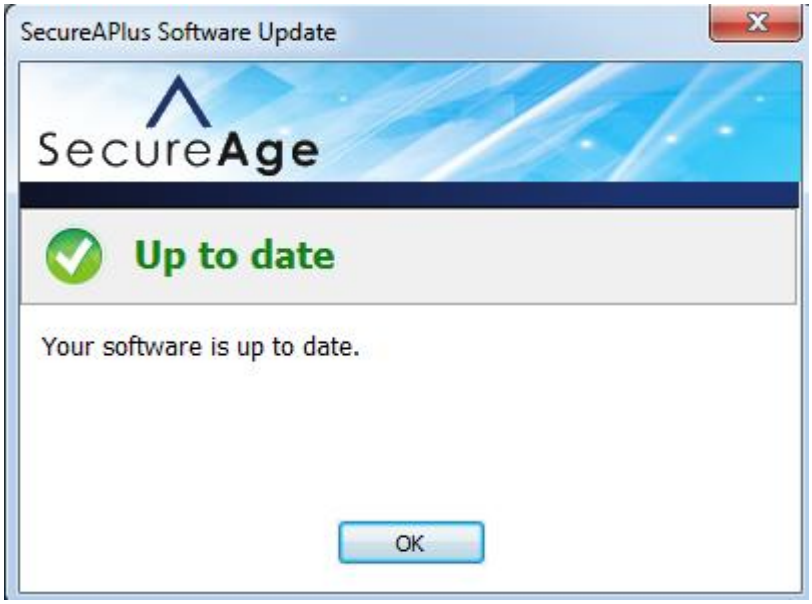
To check the SecureAPlus software update manually, follow the steps below:

- Click on the **Check Update** button.



- The **SecureAPlus Software Update** window will appear and start to check for new updates.

Upon completion of checking new updates, if the SecureAPlus is up to date, it will display a message saying that the software is up to date.

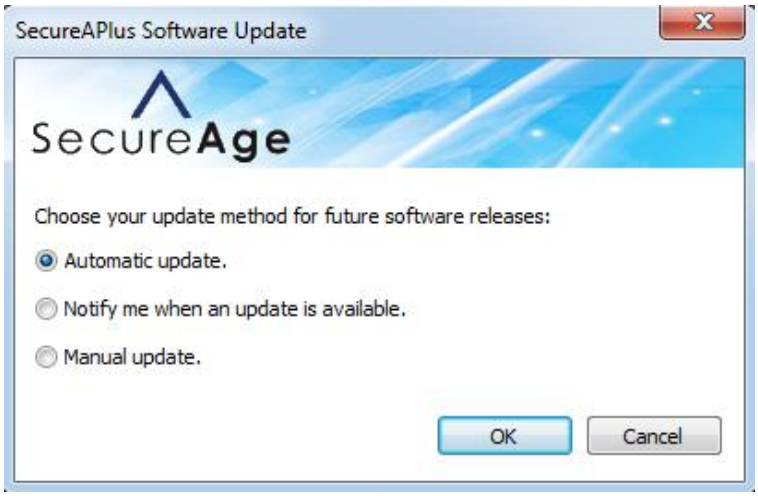


- Else if there is a new software update, it will prompt user that there is an update available. Click on **Download & Install** to update, otherwise click **Cancel**.

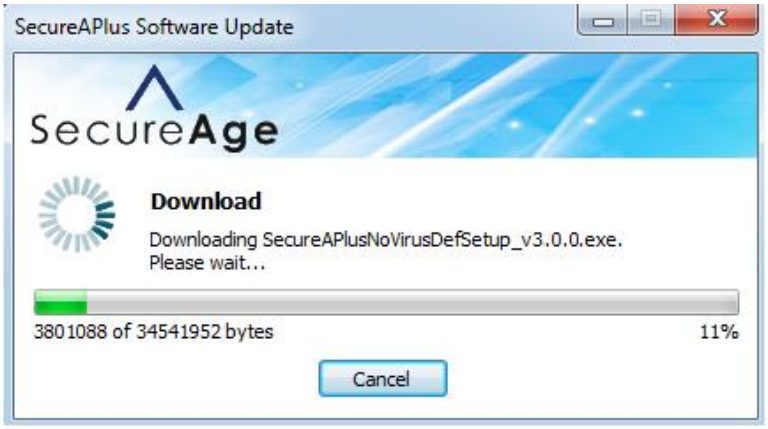
Note:

- To change the options for software updates, click on **Options…** button, a new window will appear to allow you to make changes to the update method.

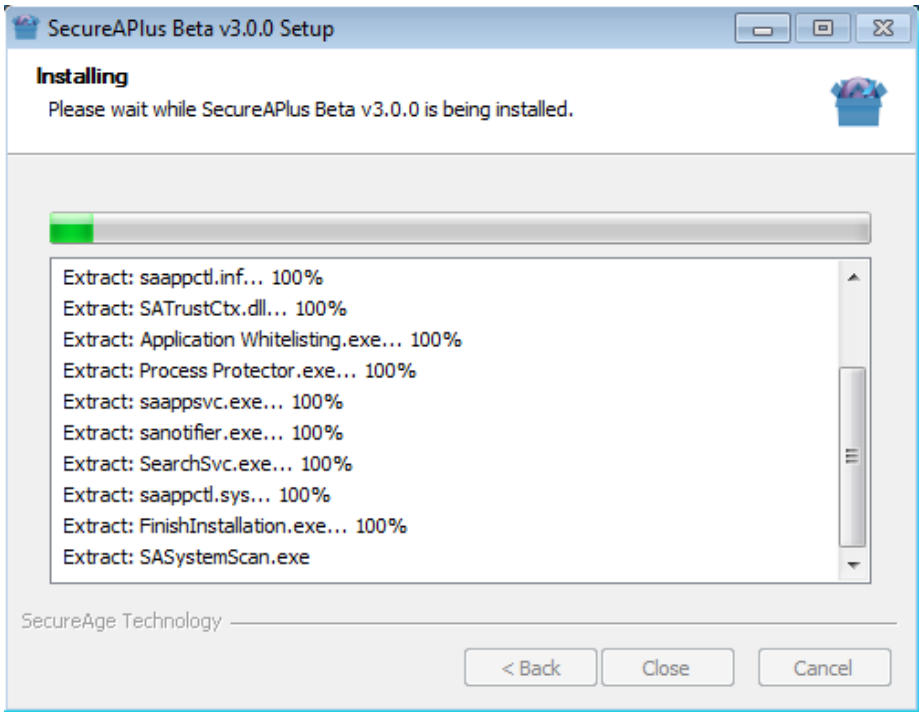
- After making the selection, click on **OK** button to proceed.



- Click on **Download & Install** and it will start to download the new update.



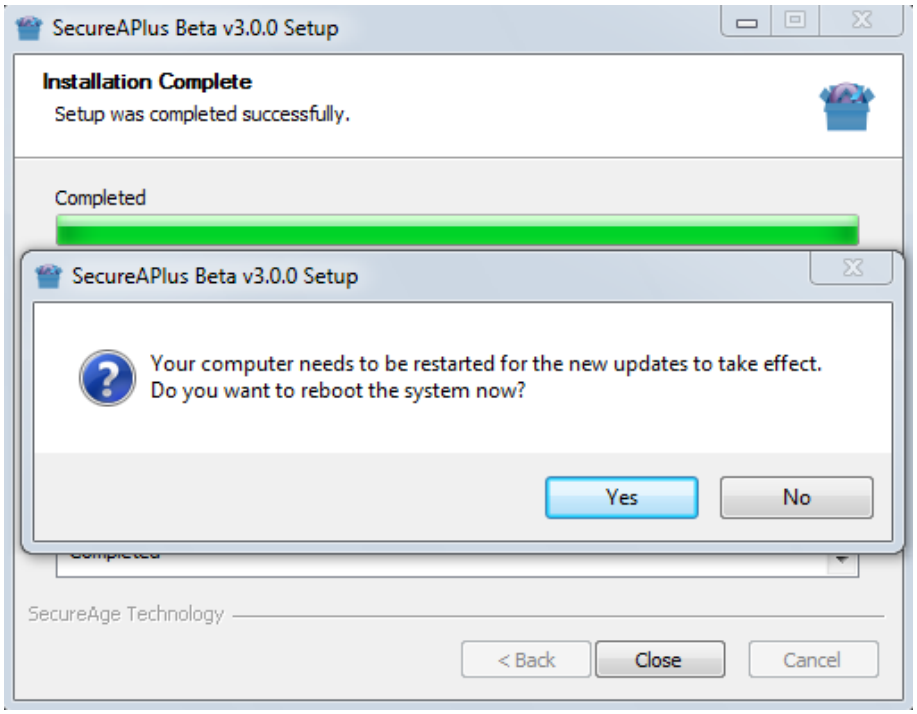
- Upon completion of the download of new update, SecureAPlus installation will start.



- It will prompt to reboot when installation completes, select **Yes** to restart your computer. Otherwise, select **No** and reboot later.

Note:

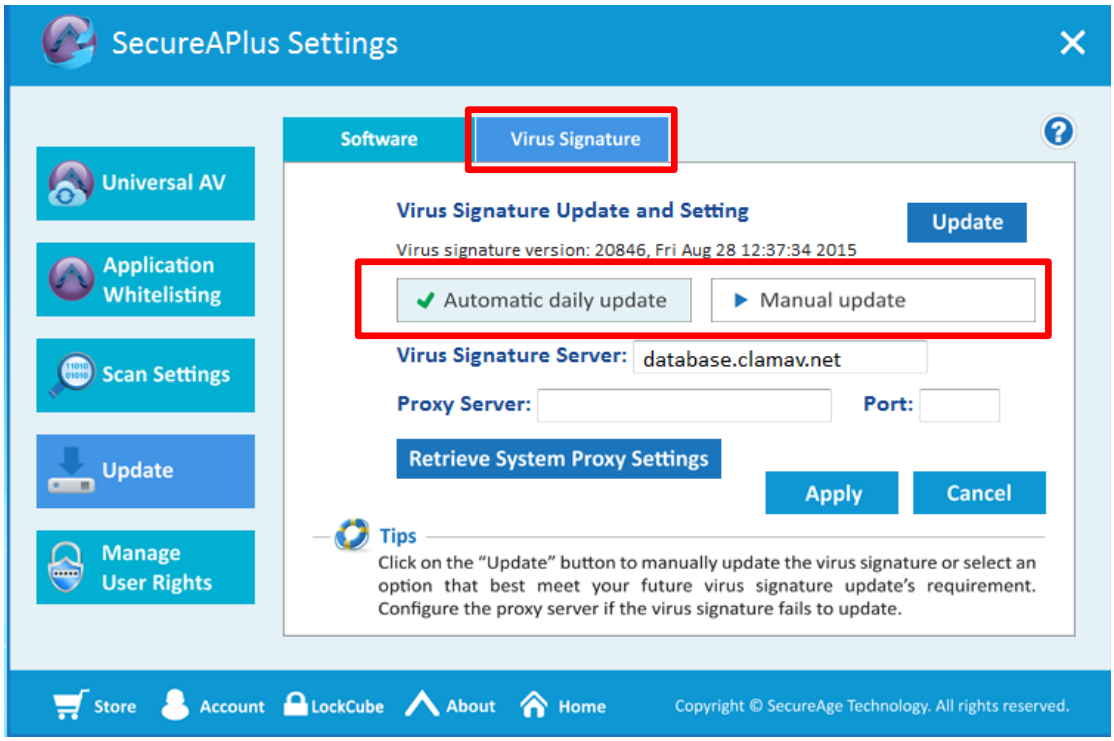
It is recommended that you reboot the machine at the end of installation process in order to have all the features working properly.



4.4.2 Virus Signature

To setup your software update settings, follow the steps below:

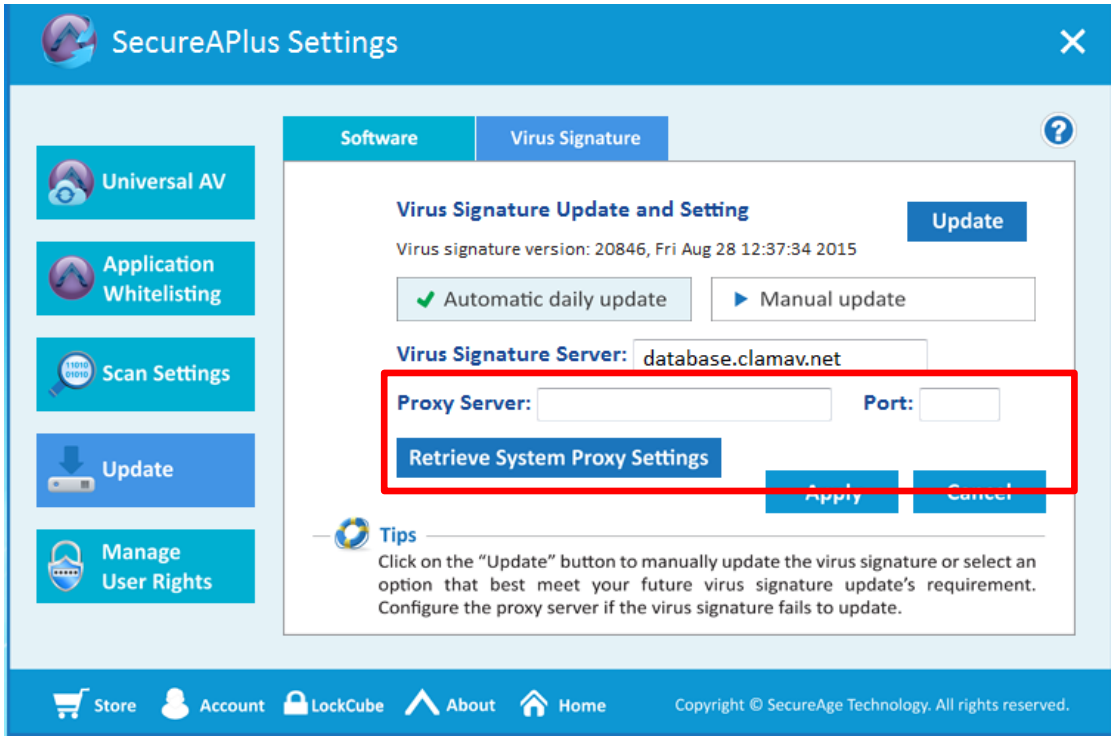
- Start SecureAPlus. Please refer to **Section 2.1** for the steps to start SecureAPlus.
- In **SecureAPlus** window, click on the **Settings** icon to view the settings.
- In the **SecureAPlus Settings** window, click on **Update** on the left menu and click on the **Virus Signature** tab.



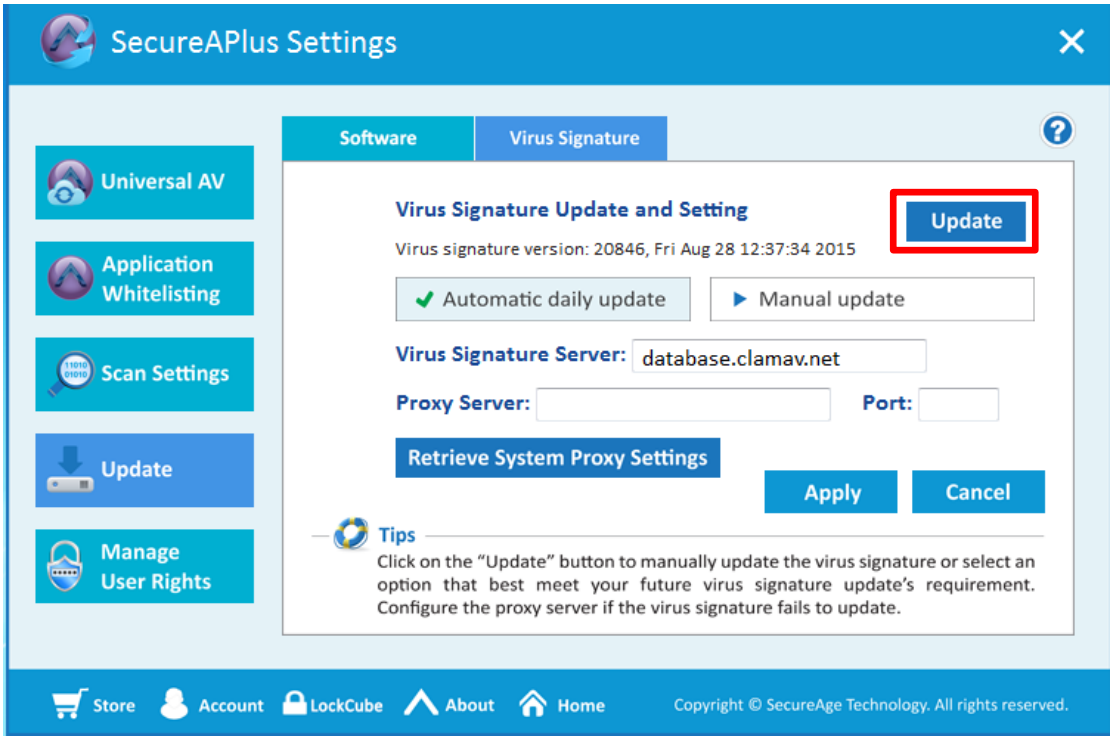
Under **Virus Signatures Update** Options, you can select any of the listed options:

- **Automatic daily update** – SecureAPlus will automatically update the antivirus data daily. (This is the default selected option)
- **Manual update** – User have to manually update the antivirus database in order to update it. Click on the **Update Virus Signature** button to manually update it.
- Click on **Apply** button to apply any changes made.

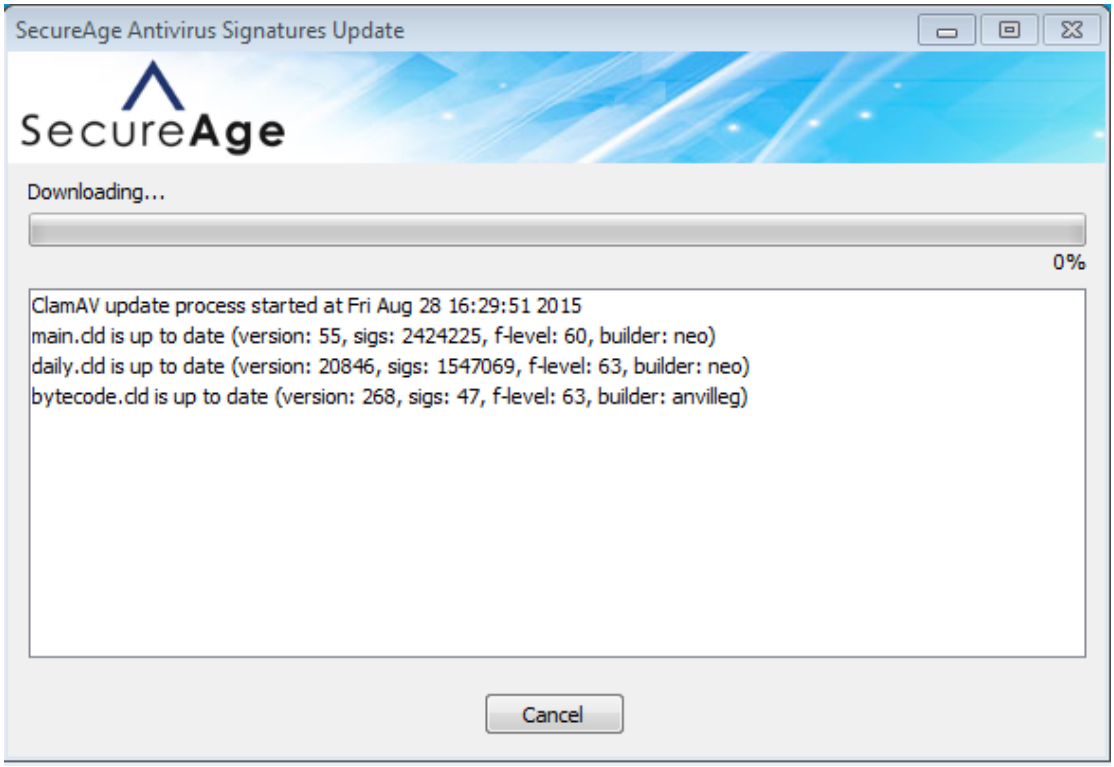
Proxy Server – Users can manually set their own proxy server and port number to retrieve their system proxy settings via their Internet Explorer browser which will be used by ClamAV to update their virus signature.



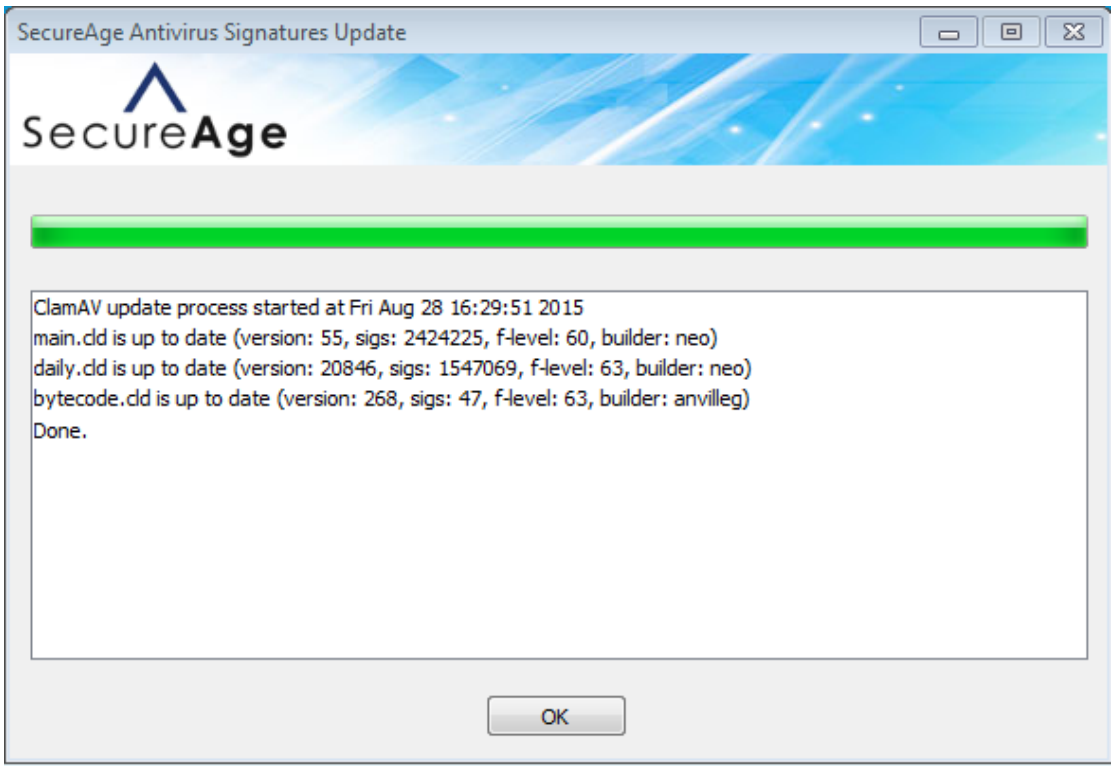
To update the virus signature, click on the **Update** button.



- It will download and update the latest virus definitions.



- When it shows that it is done, click on **OK** button to return back to the **SecureAPlus Settings** window.



Note:

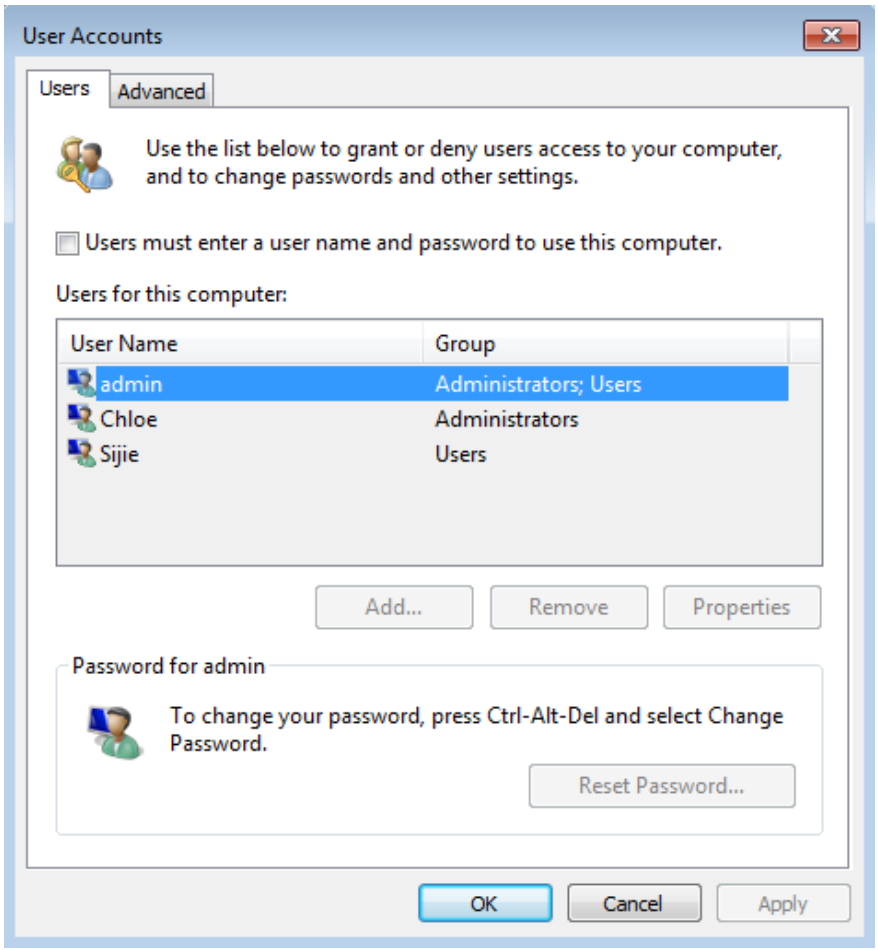
- **Automatic update** settings are good whereby once it detects that there is a new version, it will update automatically in the background and does not require any actions from the user. User will be automatically protected by the latest security updates.
- However, sometimes it may add on more traffic loads on a user whom already has a heavy traffic load which in turn causes the system to run very slow due to the heavy use of system resources. Also, some users would like to have a control over what is being downloaded and installed into their systems. For such cases, users are recommended to opt for the **manual update** options.

4.5 Manage User Rights

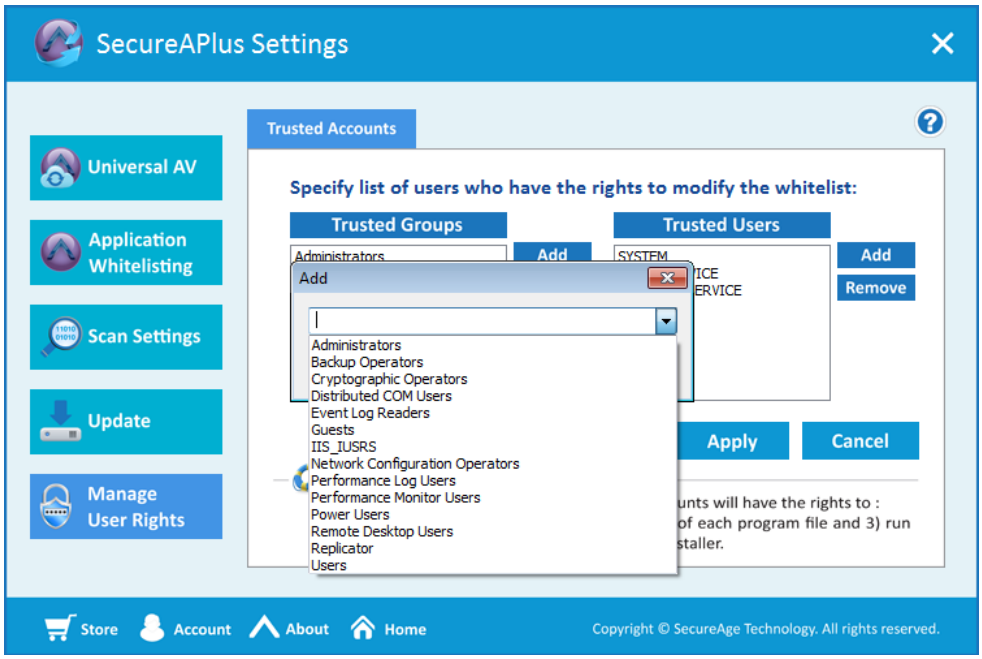
4.5.1 Manage Groups/Users in Windows

4.5.1.1 Difference between Trusted Groups and Trusted Users

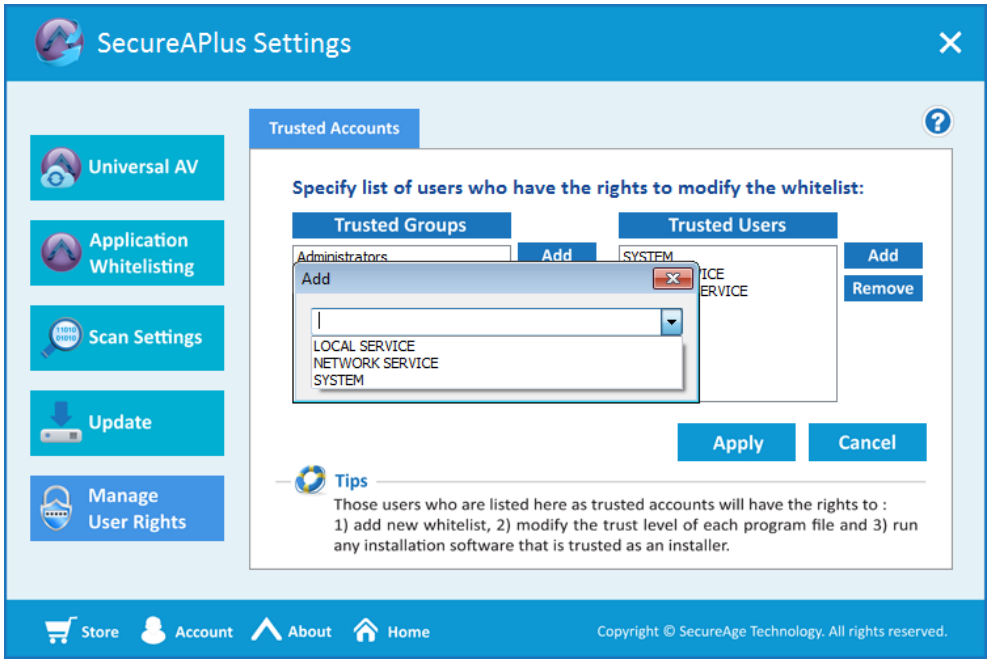
- One user can belong to a certain group or it can belong to multiple groups.
- For example, admin belongs to Administrators and Users group. Chloe and Sijie each belong to Administrators and Users group respectively.



- As shown under the groups list, these are the default groups created by Windows.



- As shown under the users list, these are the default system accounts created by Windows. (By default, these accounts are not visible to end users.)



- For Windows to boot up and run all the operating system files, it will log on as the **System** account in the background to do these. Same for **Local Service** and **Network Service** accounts, Windows use these accounts to perform some operating system task such as Windows Update. Therefore, all this 3 accounts have to be in the **Trusted Users** list in order to allow Windows to add new whitelist and perform their tasks as per normal without being blocked by Application Whitelisting.

4.6 To create your own group in Windows, refer to Section 4.5.1.2Manage User Rights

4.6.1 Manage Groups/Users in Windows

4.6.1.1 Difference between Trusted Groups and Trusted Users

- **- Create Group in Windows**
- .

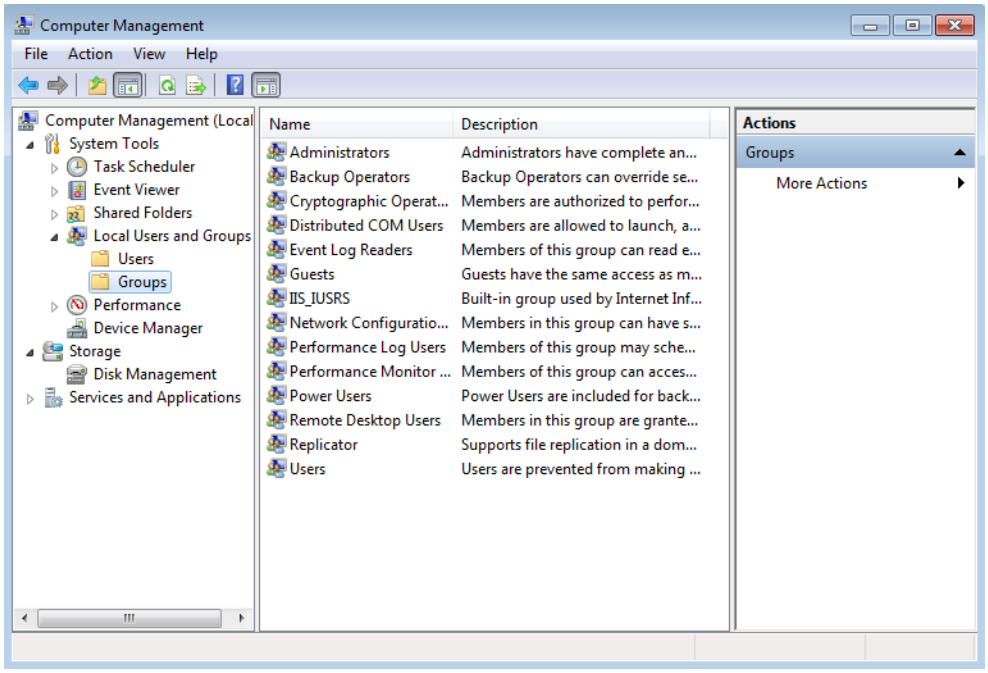
Note:

- For Application Whitelisting, SecureAPlus make use of Trusted Groups and Users to decide who are allowed to modify (Eg: add a new file or adjust the trust level).
- By default, **Administrators** is the default trusted group that is allowed to do everything on Windows. This is the same as for SecureAPlus which will work on every Windows machine.
- For enterprise who have several administrators, they can add the specific administrators' to the **Trusted Users** and remove **Administrators** from the **Trusted Groups**. This is to only give the rights to specific administrators instead of all the administrators.

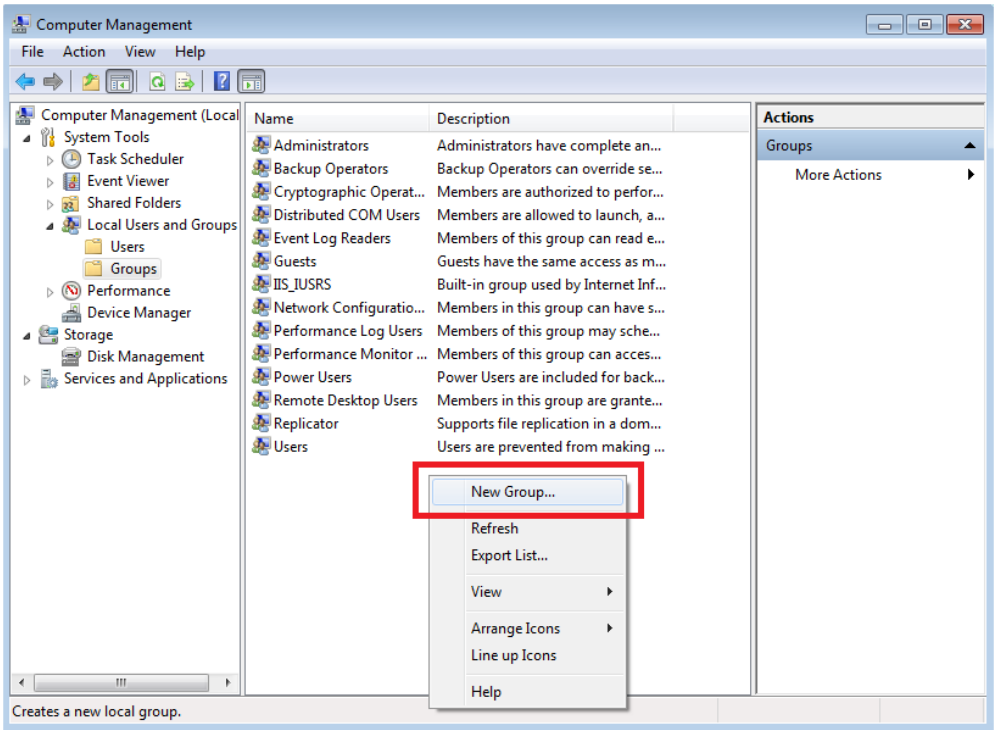
4.6.1.2 Create Group in Windows

To create new group in Windows, follow the steps below:

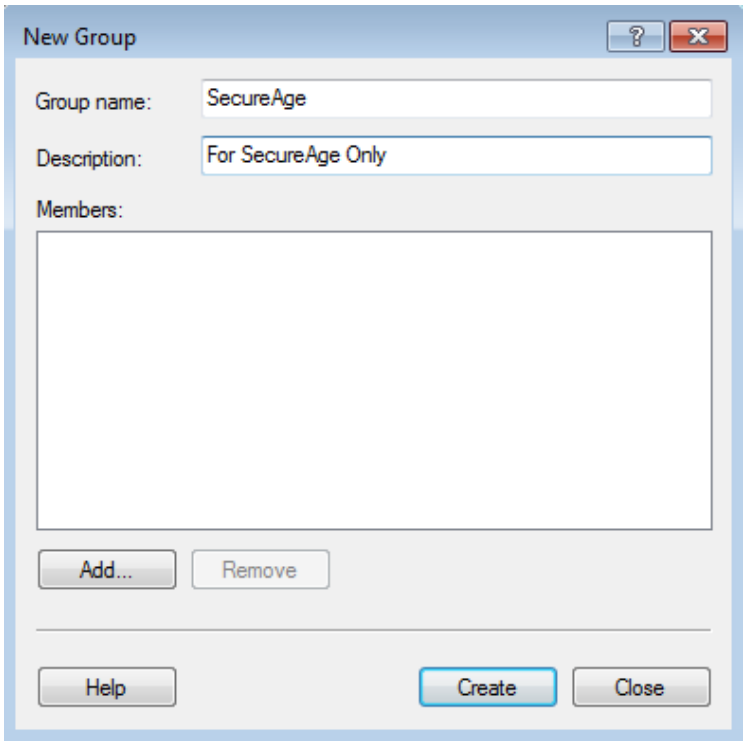
- Go to **Control Panel → Administrative Tools → Computer Management**
- Navigate to **Local Users and Groups** under **Computer Management** on the left panel. Click on **Groups**.



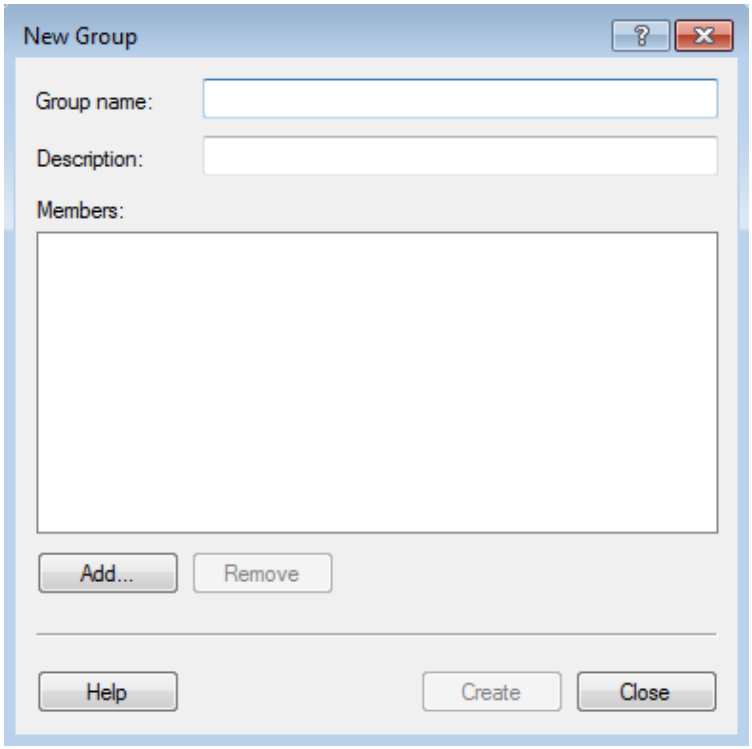
- Right click in the middle panel and click on **New Group…** when the right click menu appears.



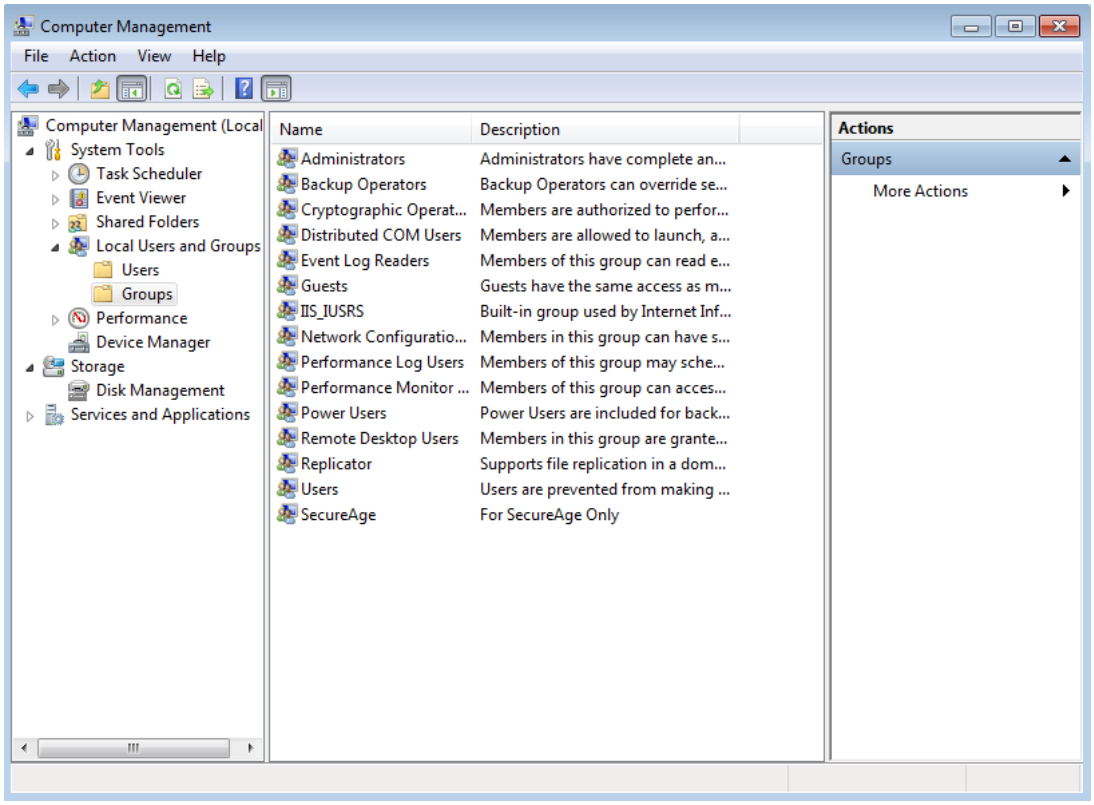
- The **New Group** creation window will appear. Enter the group details and click on **Create** button.



- The window will be cleared once the group is being created successfully, repeat the previous steps to create more groups else click on **Close** button to exit the **New Group** creation window.



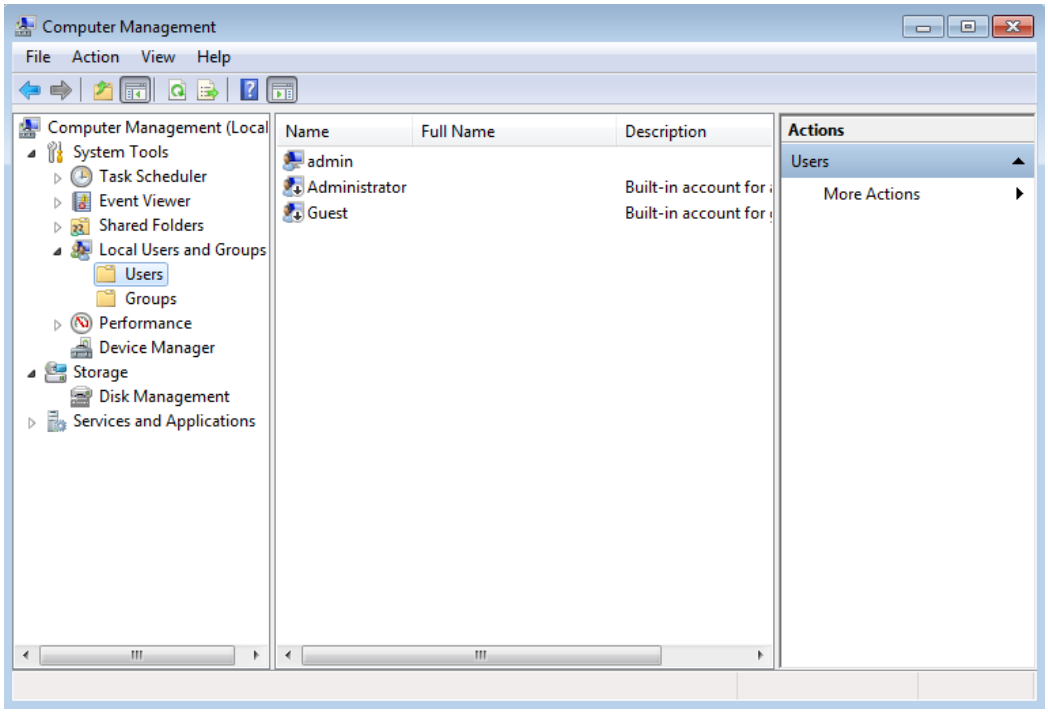
- The newly created group will appear under the Groups list.



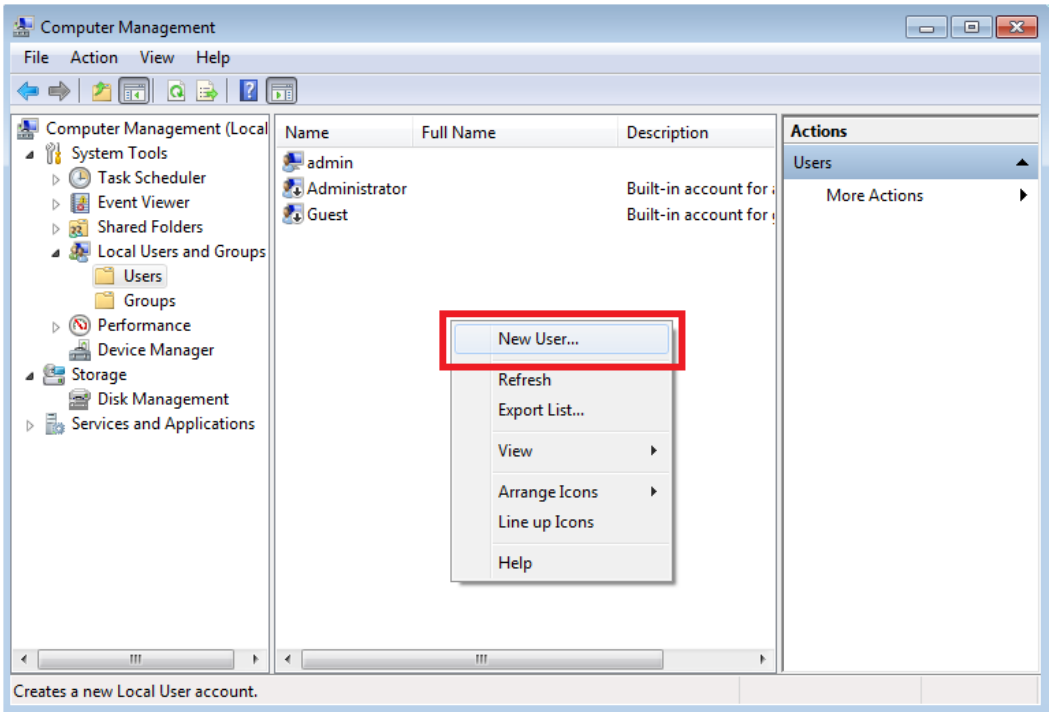
4.6.1.3 Create User in Windows

To create new user in Windows, follow the steps below:

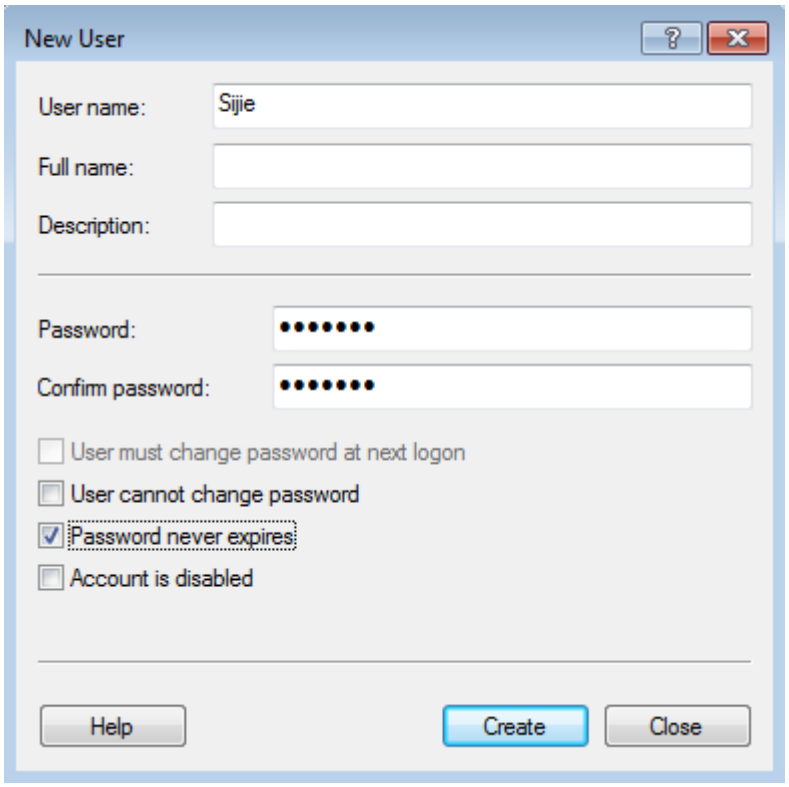
- Go to **Control Panel → Administrative Tools → Computer Management**
- Navigate to **Local Users and Groups** under **Computer Management** on the left panel. Click on **Users**.



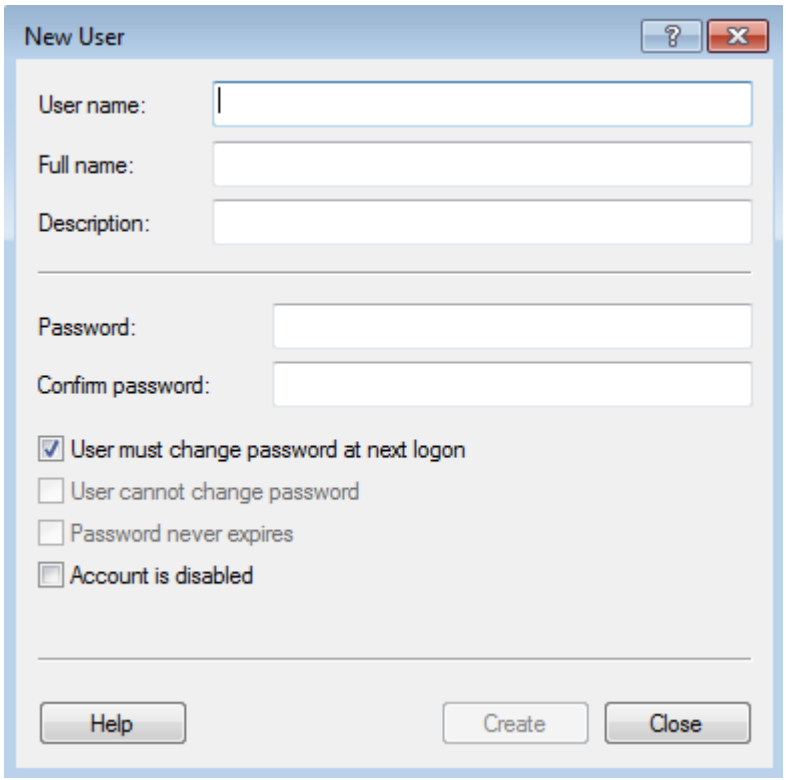
- Right click in the middle panel and click on **New User…** when the right click menu appears.



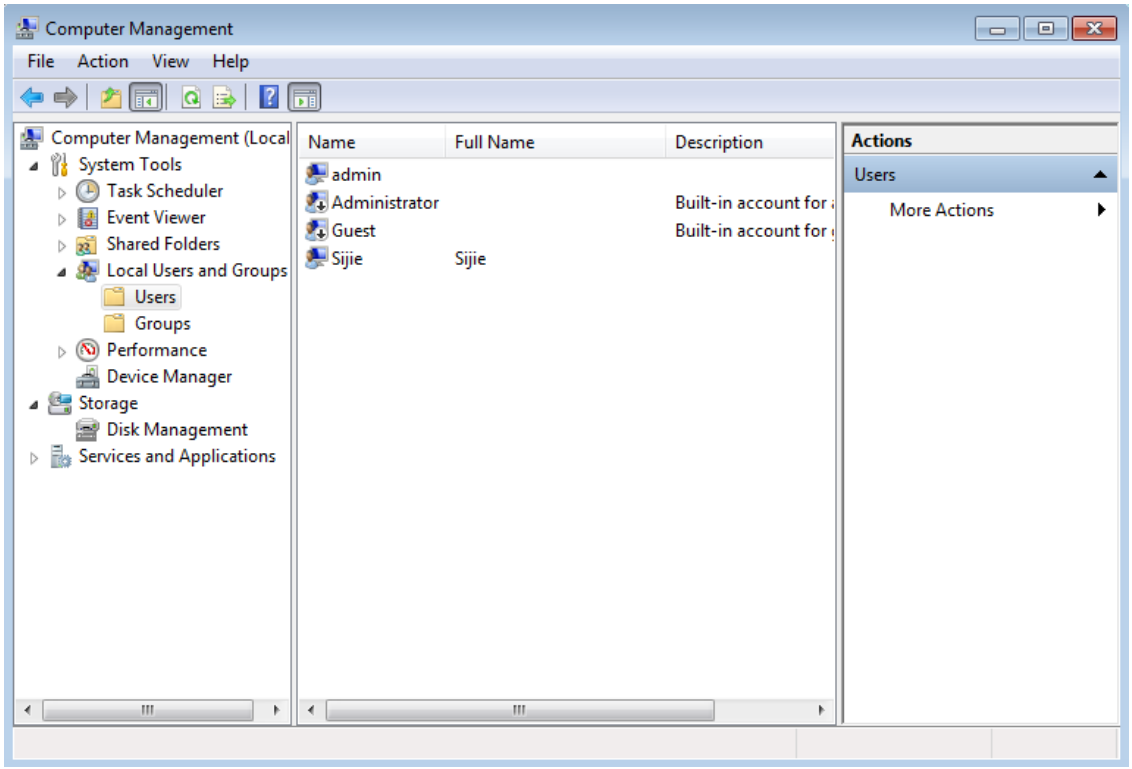
- The **New User** creation window will appear. Enter the user details and click on **Create** button.



- The window will be cleared once the user is being created successfully, repeat the previous steps to create more users else click on **Close** button to exit the **New User** creation window.



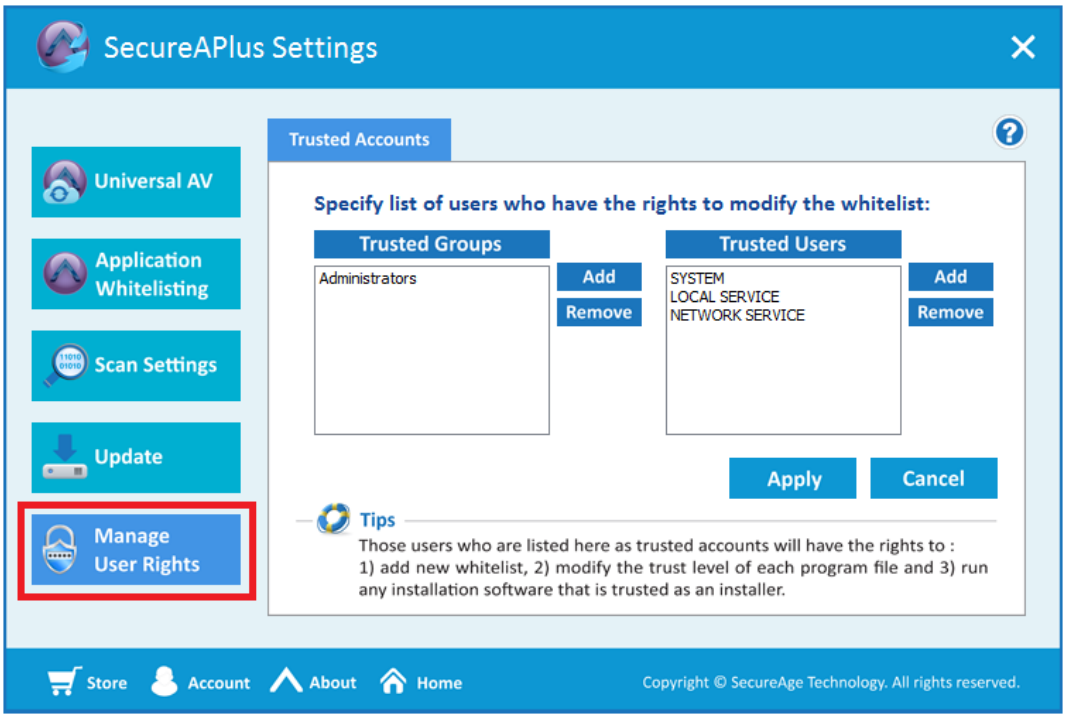
- The newly created user will appear under the Users list.



4.6.1.4 *Managed Trusted Groups and Users in SecureAPlus*

You can setup the user rights of trusted accounts by following the steps as below:

- Start SecureAPlus. Please refer to **Section 2.1** for the steps to start SecureAPlus.
- In **SecureAPlus** window, click on the **Settings** icon to view the settings.
- In the **SecureAPlus Settings** window, click on **Manage User Rights** on the left menu.



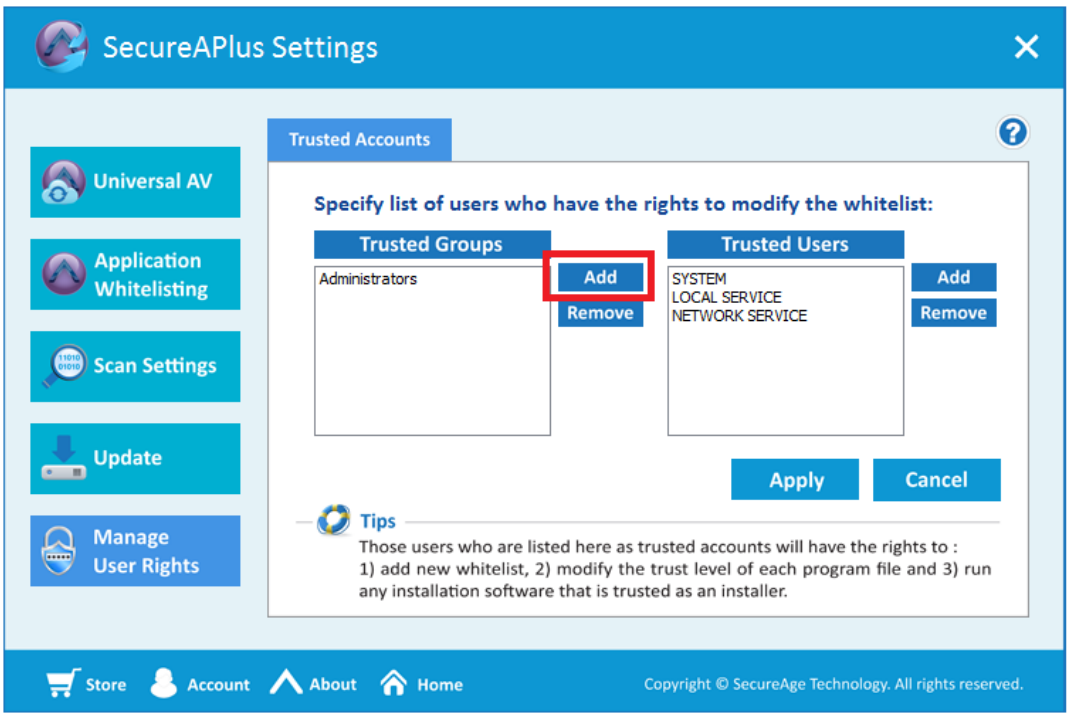
- In the **Trusted Accounts** tab, users can choose to edit the Trusted Groups and Trusted Users.

Note:

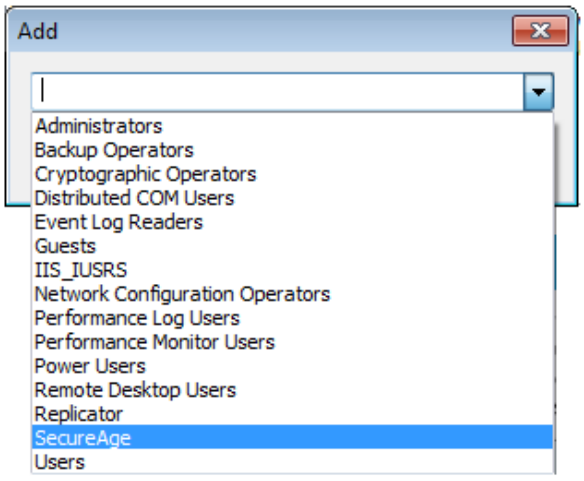
- Only trusted accounts are allowed to install new trusted applications by launching a “Trusted Installer” application. Normal users are allowed to execute trusted installer, but the trusted level will be downgraded as trusted application only. This is to prevent a normal user to install any unwanted applications.
- Only trusted accounts can modify the trust level of a file. Normal user will get access denied if they are trying to modify the trust level of a file.

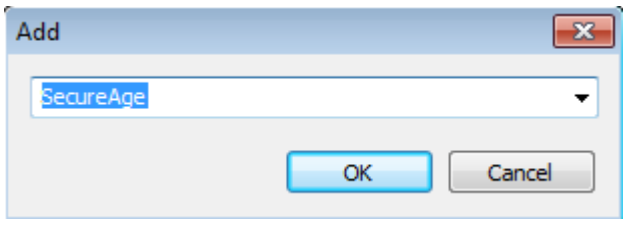
To add Trusted Groups, follow the steps below to add:

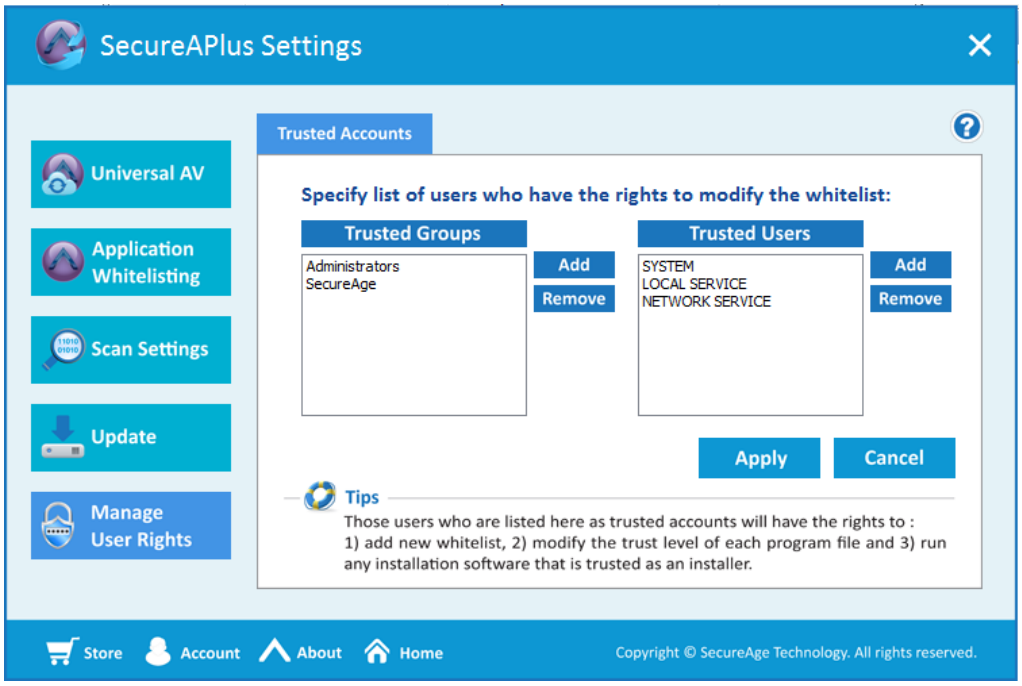
- Under **Trusted Groups**, click on **Add** to add trusted groups.



- In **Add** window, from the dropdown box, select the group to be trusted for application whitelisting. Click **OK**. The newly added trusted group will appear in the Trusted Group list.



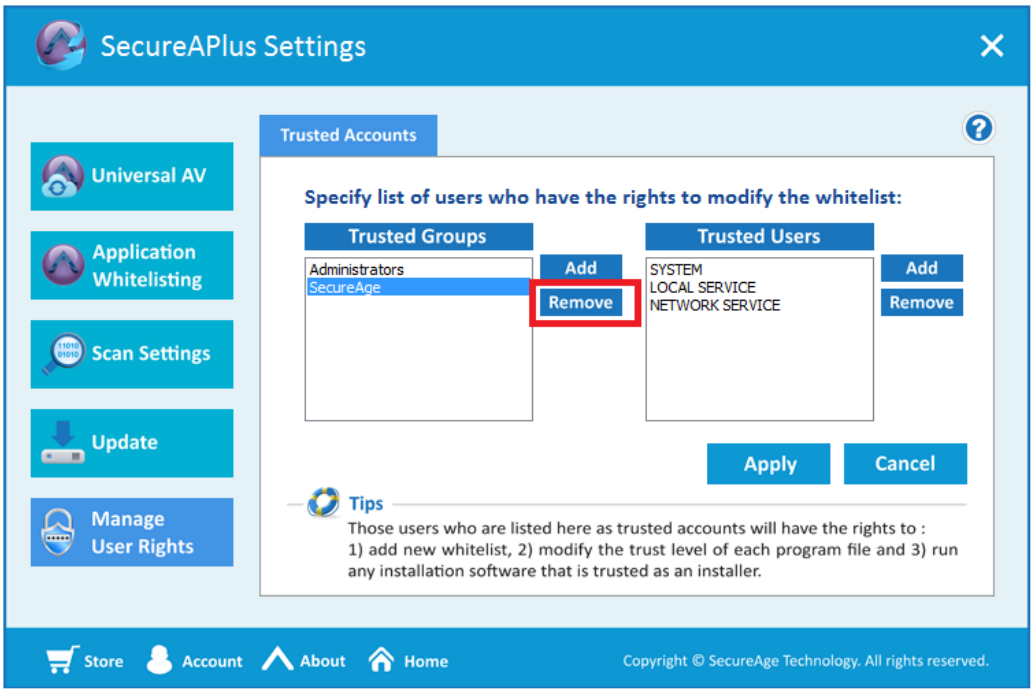




- The newly added trusted group will be added to the list. Then click on **Apply** button to apply the changes made.

To remove Trusted Groups, follow the steps below to remove:

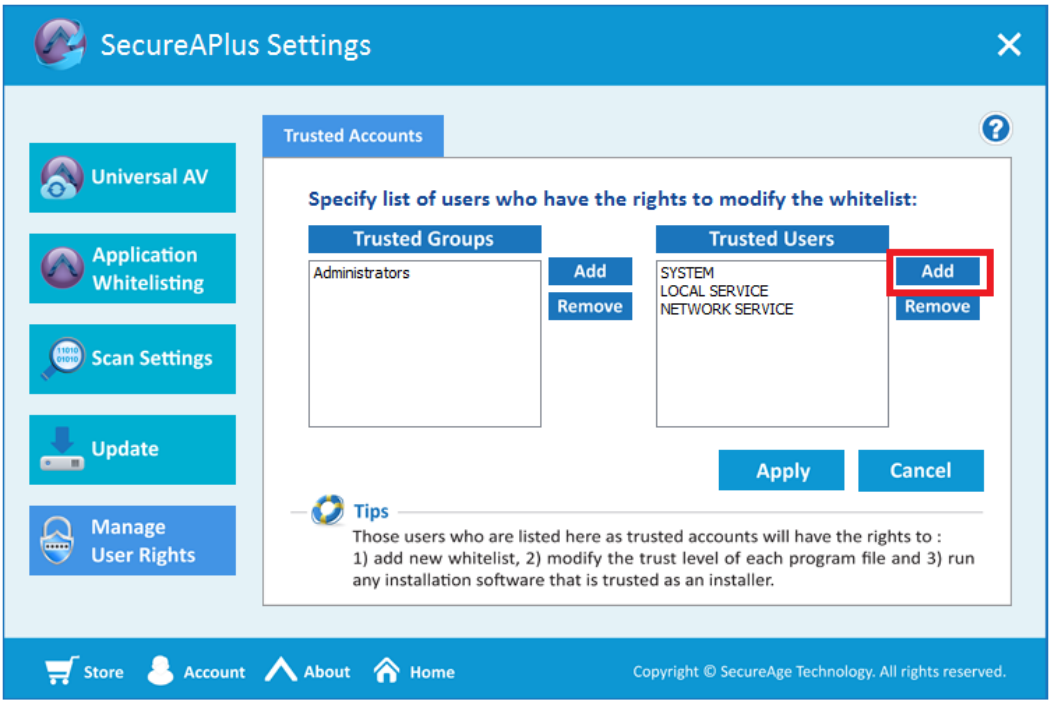
- Under **Trusted Groups**, select the trusted groups in the list and click on **Remove**.



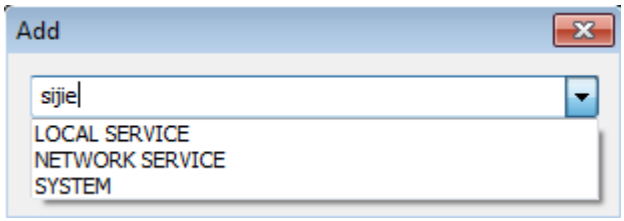
- The selected trusted group will be removed from the list. Then click on **Apply** button to apply the changes made.

To add Trusted Users, follow the steps below to add:

- Under **Trusted Users**, click on **Add** to add trusted users.



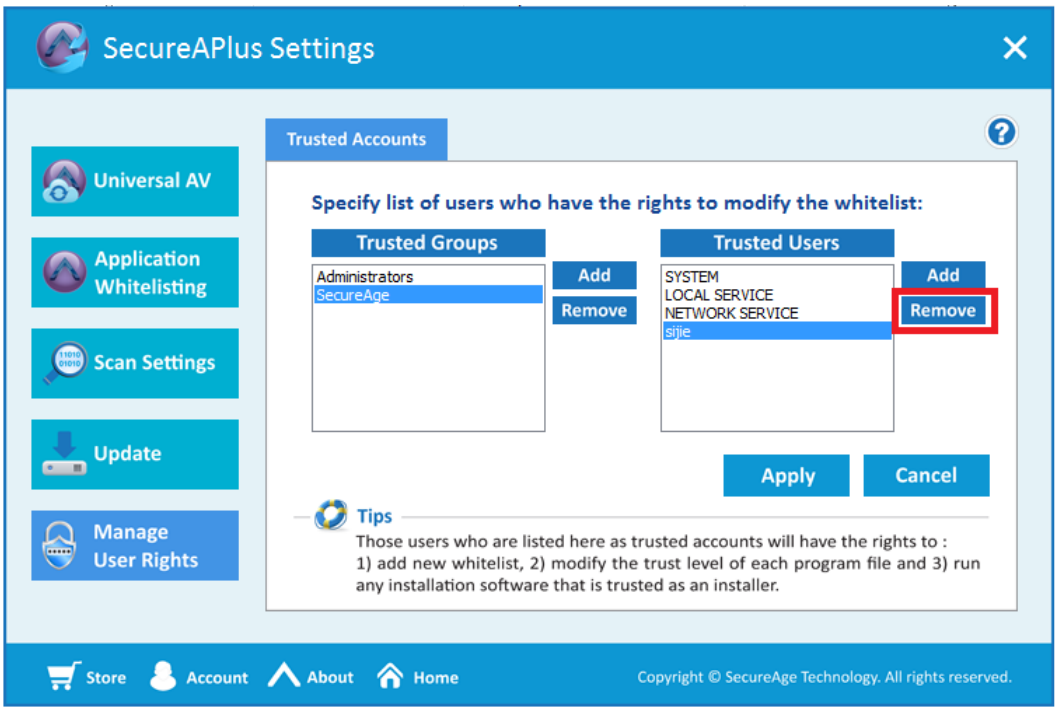
- In **Add** window, from the dropdown box, select the users or type the name of the users to be trusted for application whitelisting. Click **OK**.



- The newly added trusted users will be added to the list. Then click on **Apply** button to apply the changes made.

To remove Trusted Users, follow the steps below to remove:

- Under **Trusted Users**, select the trusted users in the list and click on **Remove**.



- The selected trusted user will be removed from the list. Then click on **Apply** button to apply the changes made.

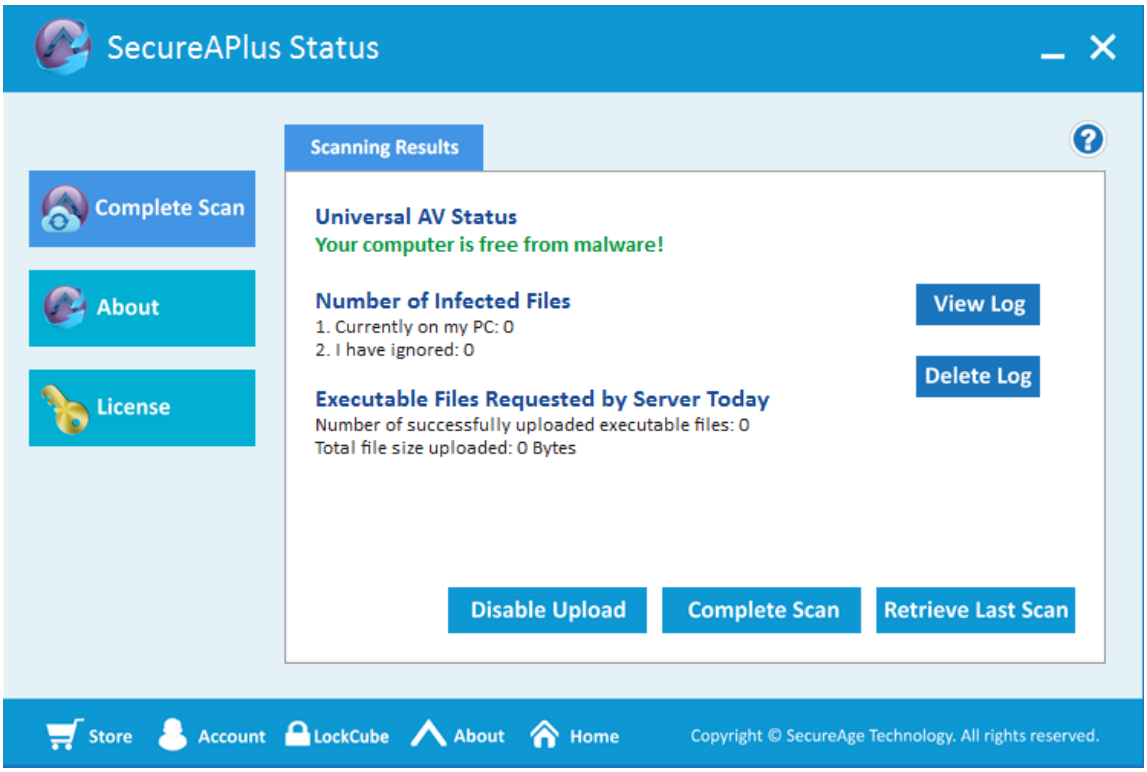
5 Universal AV

SecureAPlus Universal AV is to provide continuous scanning of the user's computer by multiples antivirus software in the cloud to achieve a more accurate scanning result by leveraging on stronger antivirus' scanning capabilities. It scans every executable files on the user's computer and does not use any heuristic rule to leave out any "safe" file which may later turn out to be sophisticated viruses.

To check details of the Universal AV, follow the steps below:

- Start SecureAPlus. Please refer to **Section 2.1** for the steps to start SecureAPlus.
- In the **SecureAPlus** window, click on the **Complete Scan** icon.

- The **SecureAPlus Status** window will appear, showing the current state of the Universal AV. The latest details of the Universal AV scan results will be displayed.

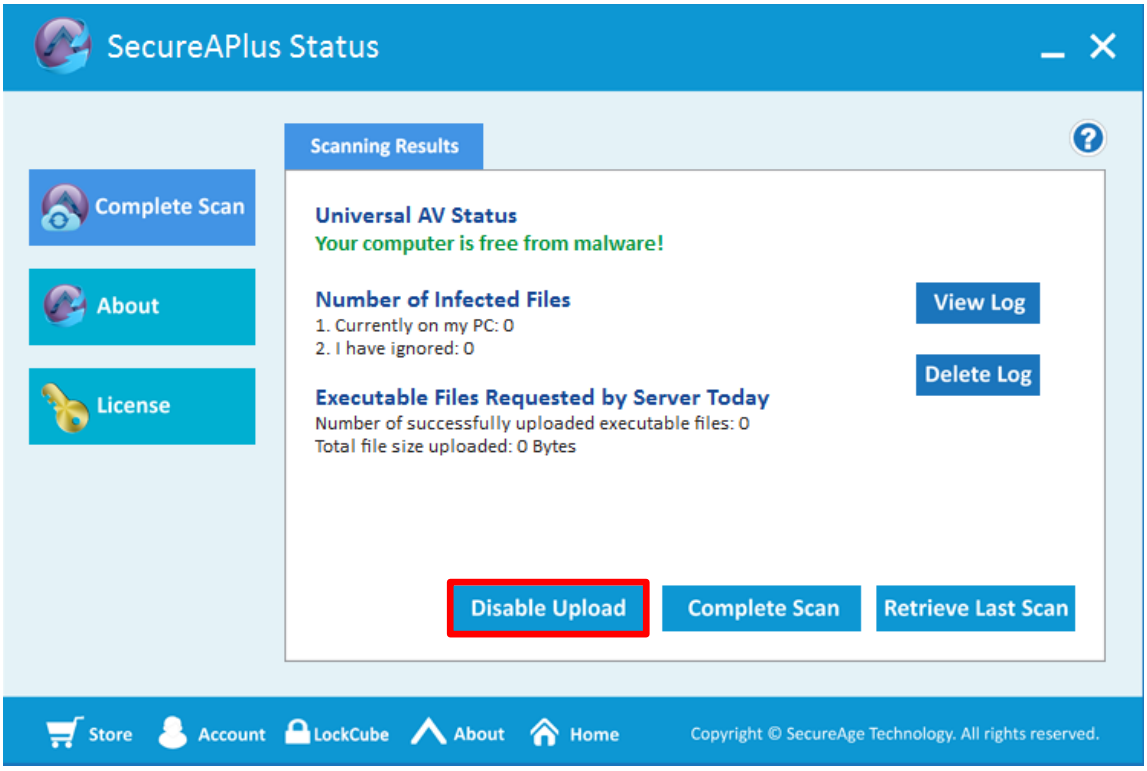


Universal AV	Description
Universal AV Status	
Universal AV Status	The current Universal AV status of the machine.
Number of Infected Files	
1. Currently on my PC	The number of infected files found on the local hard disks detected by the Universal AV.
2. I have ignored	The number of infected files which are being ignored.
Executable Files Requested by Server Today	
Number of successfully uploaded executable files	The number of executable files which are successfully uploaded to the server.
Total file size uploaded	The total file size uploaded to the server on the current day itself.

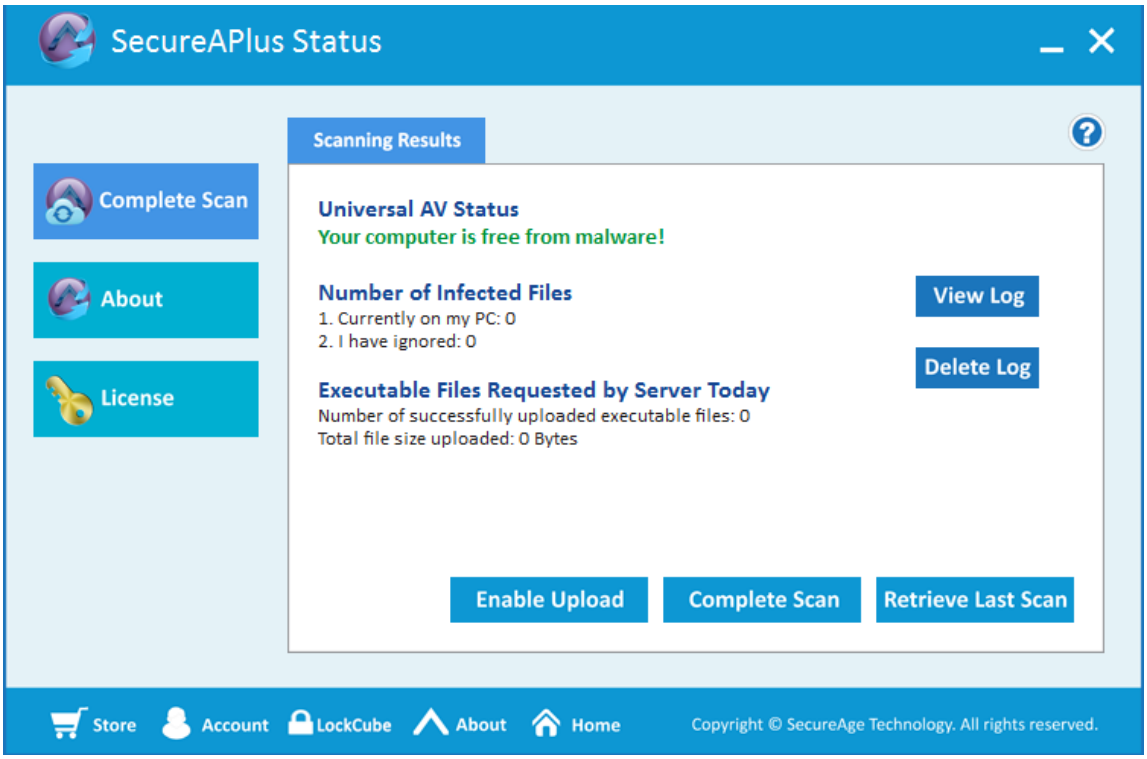
5.1 Disable/Enable Upload

To disable the upload of sample executable files, follow the steps below:

- Click on **Disable Upload** button.

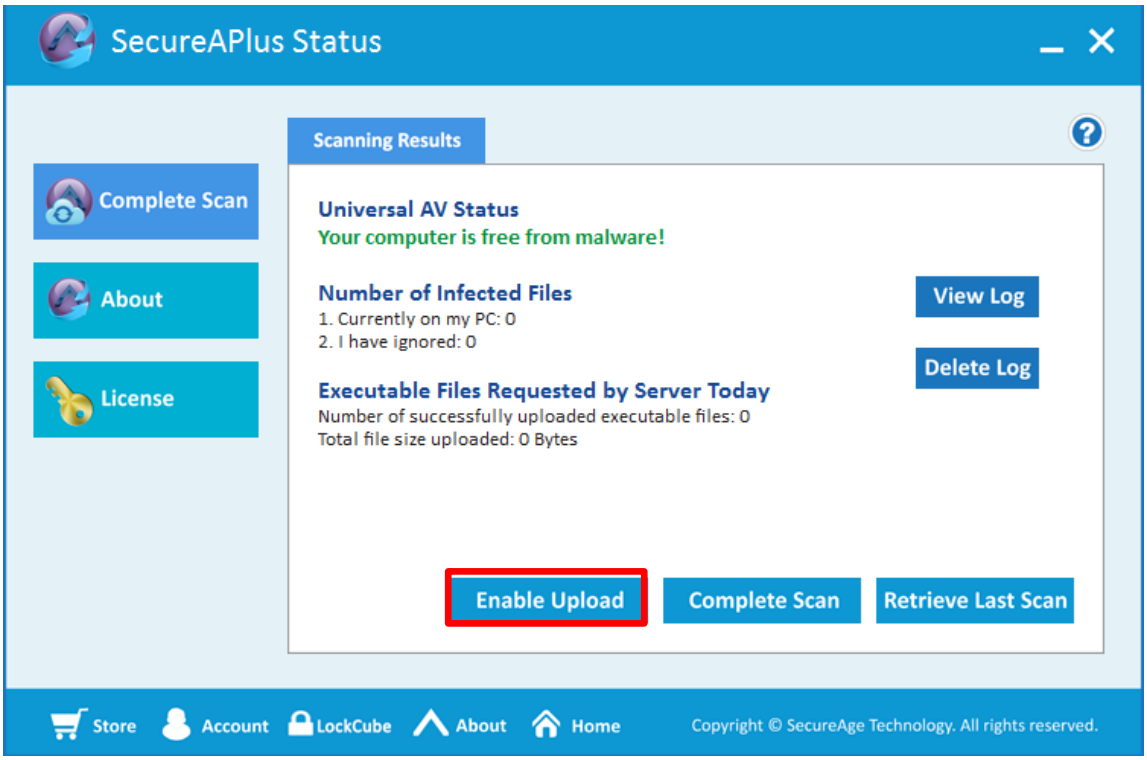


- The uploading will be disabled.

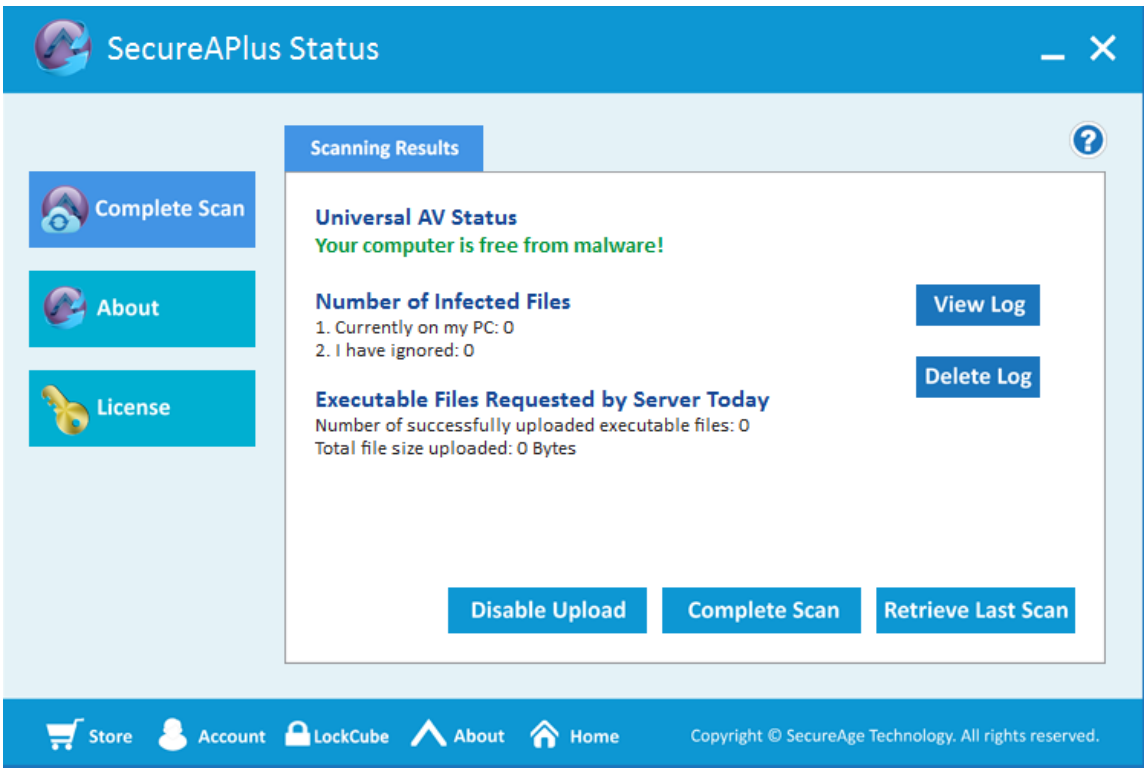


To enable the upload of sample executable files, follow the steps below:

- Click on **Enable Upload** button.



- The uploading will be enabled.



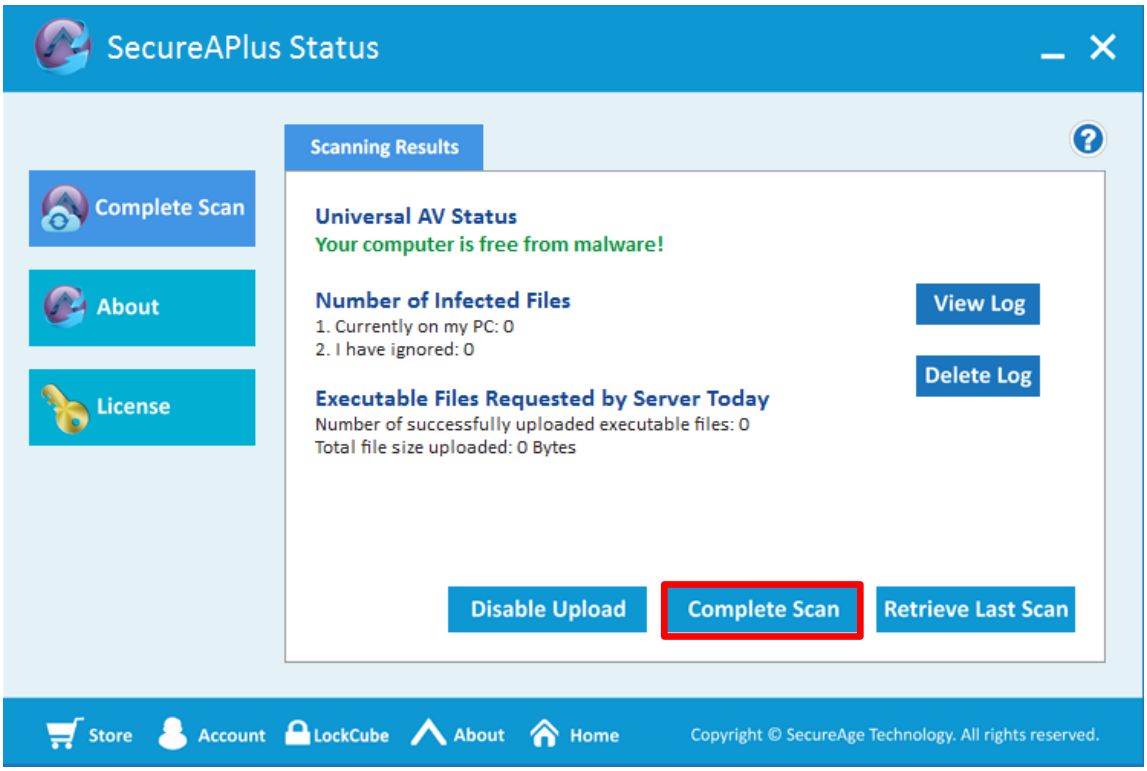
Note:

- This option is for users to disable/enable upload temporarily.
- For example users who are playing online games that require a large amount of internet bandwidth, they can choose to temporary disable the upload of sample executable files until they complete their games. However, if they forget to turn the upload back on, it will be still switched back on after they rebooted the machine.

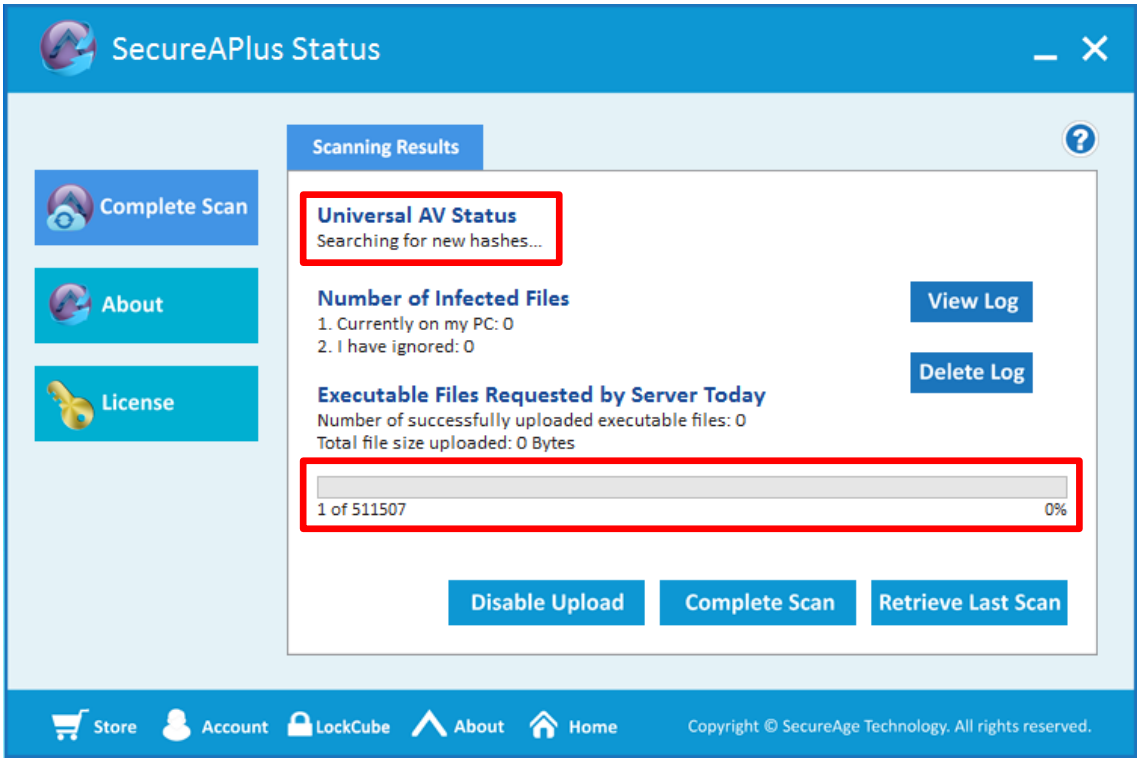
5.2 Complete Scan

To manually submit hashes for scanning or scan the full system, follow the steps below:

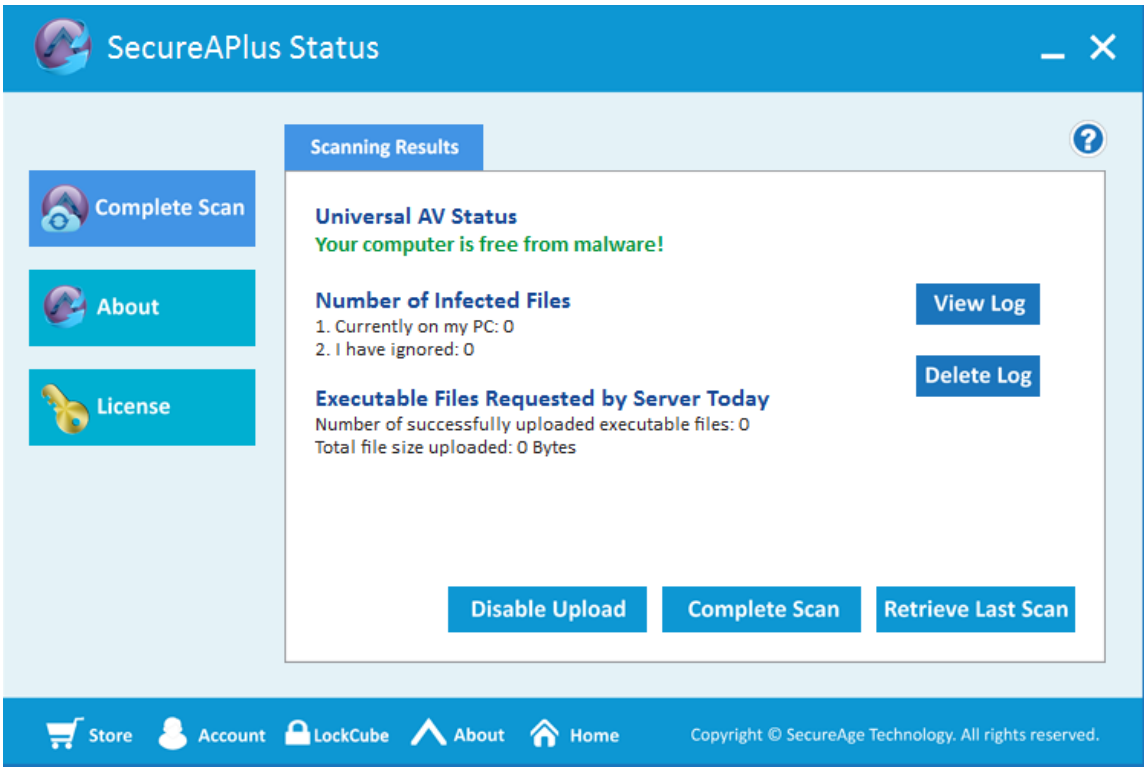
- Click on **Complete Scan** button within the **Scanning Results** tab.



- The progress of the scanning will be shown.



- When the full system scan completes, it will refresh and display the updated scan results.



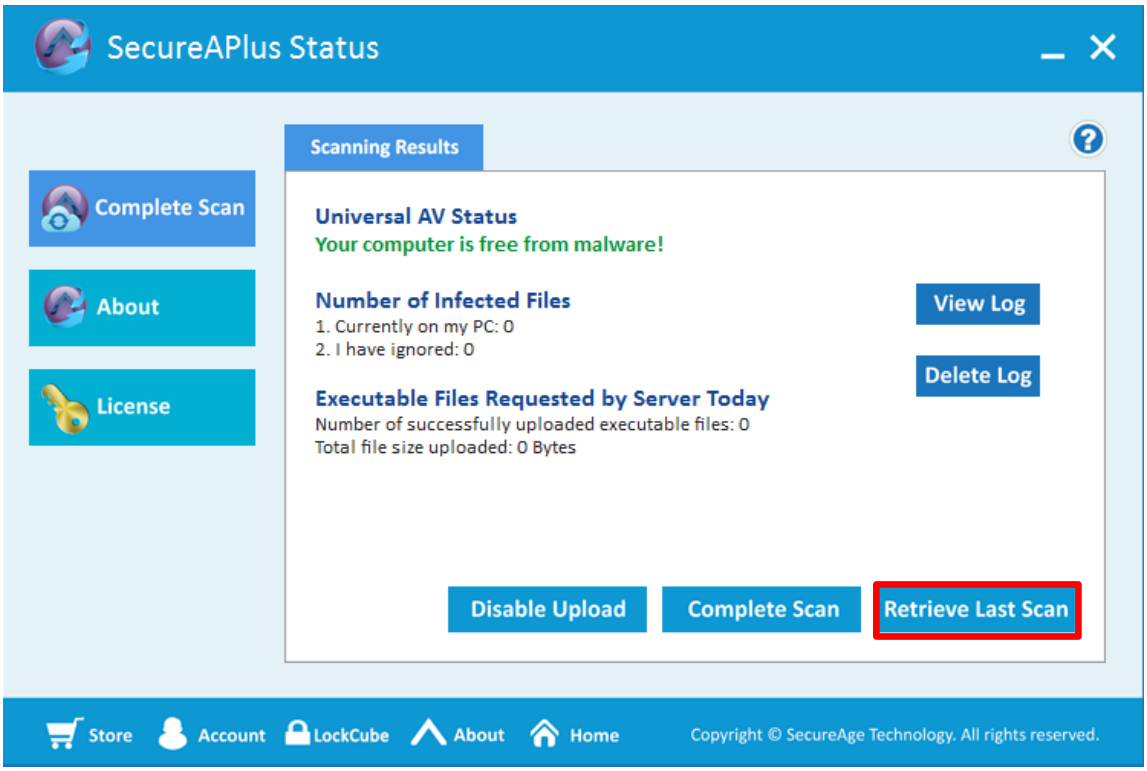
Note:

- The number of new hashes will be automatically submitted to the server every one hour or every time when the machine is rebooted.

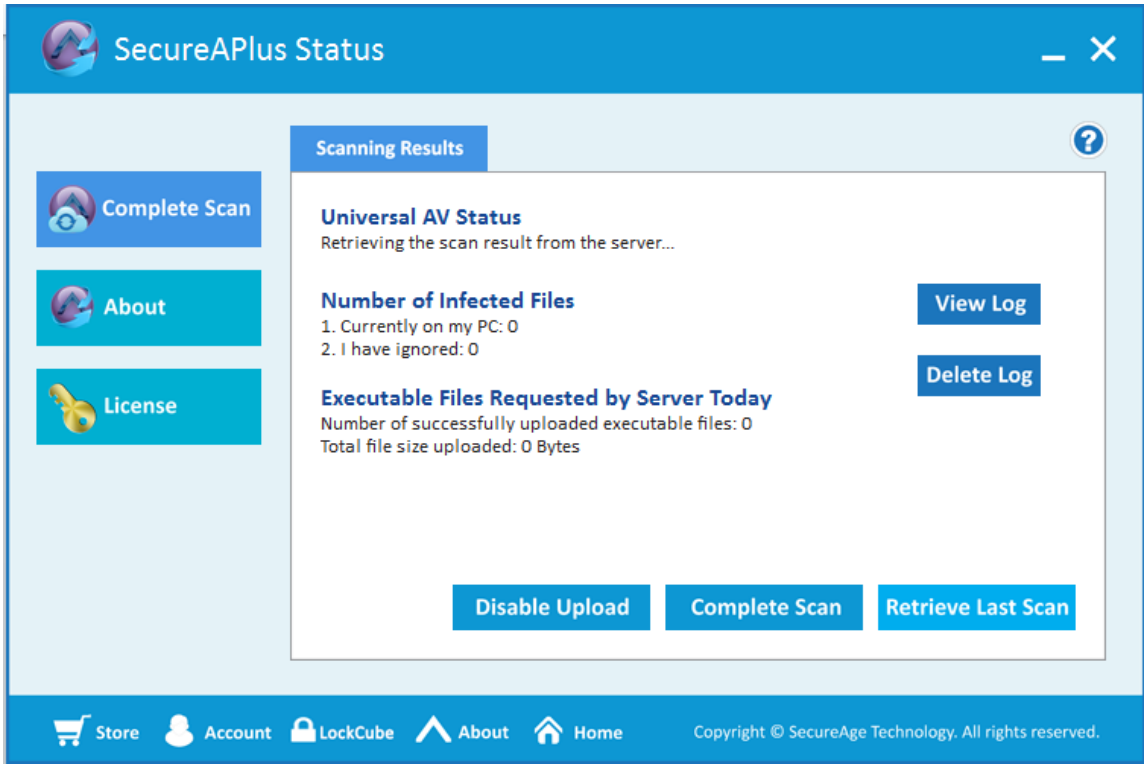
5.3 Retrieve Last Scan

To retrieve the last Universal AV's scan results, follow the steps below:

- Click on **Retrieve Last Scan** button.



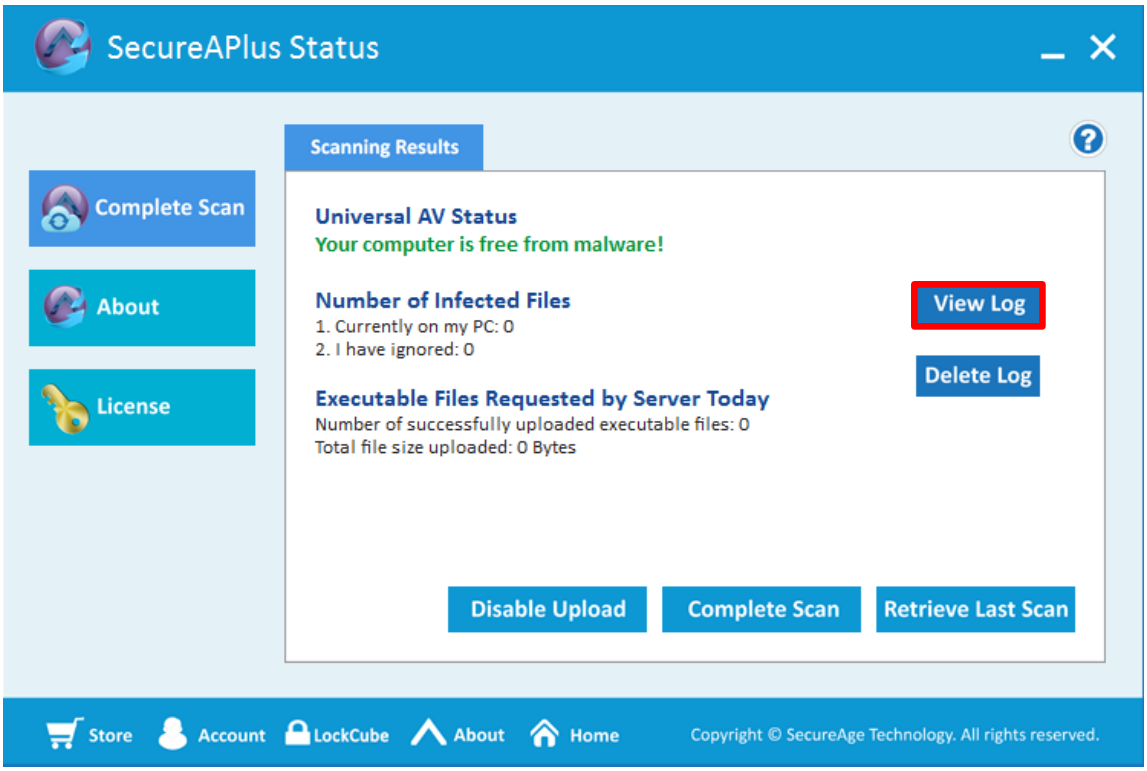
- The last scan result will be retrieved and displayed.



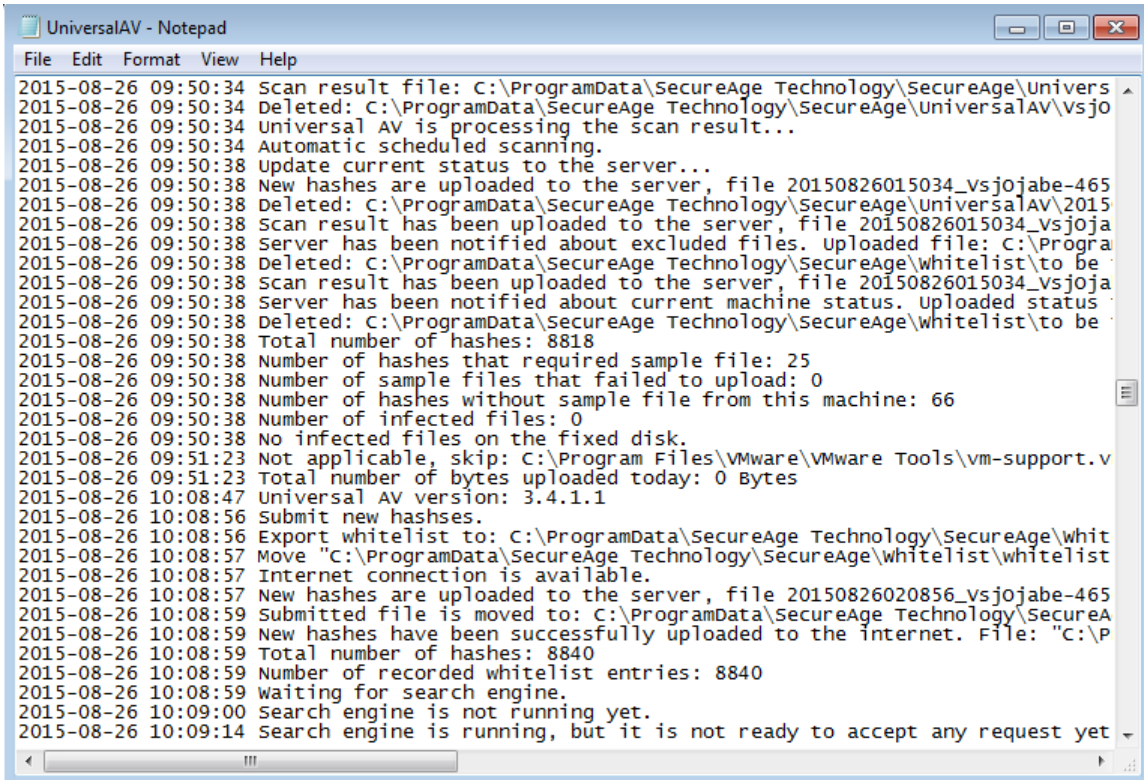
5.4 View Universal AV's Log

To view the Universal AV log, follow the steps below:

- Click on **View Log** button.



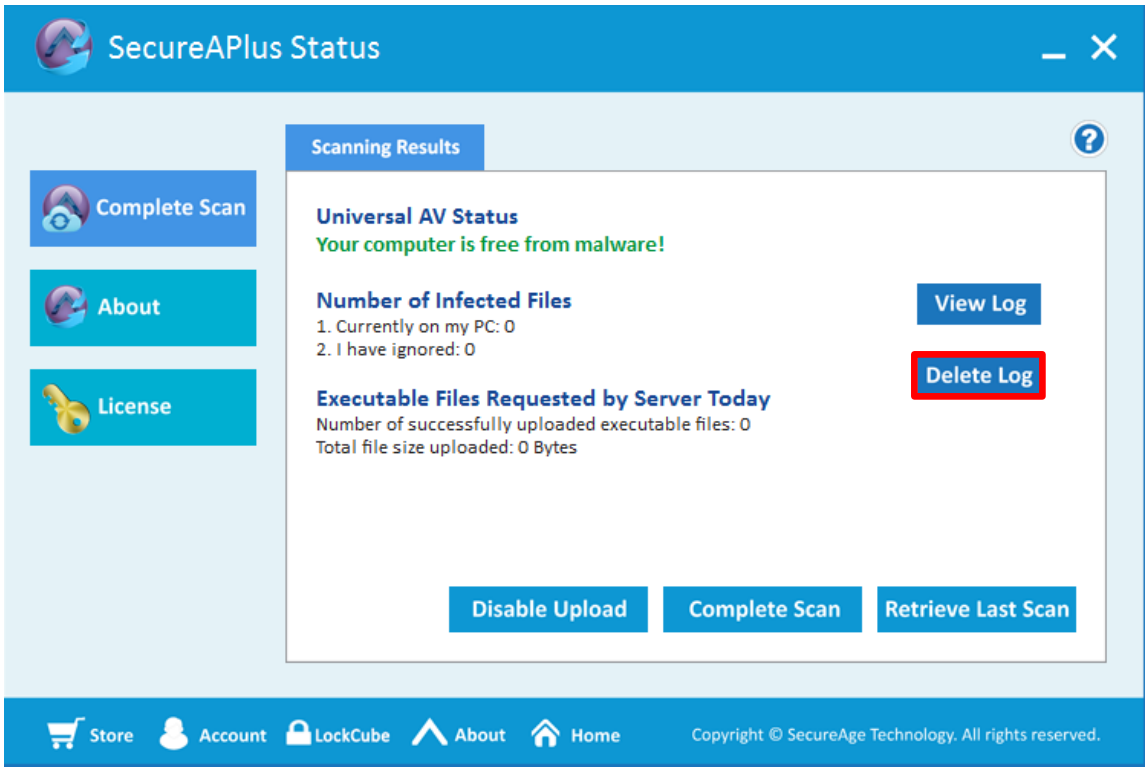
- The Universal AV log file will be opened using the default program.



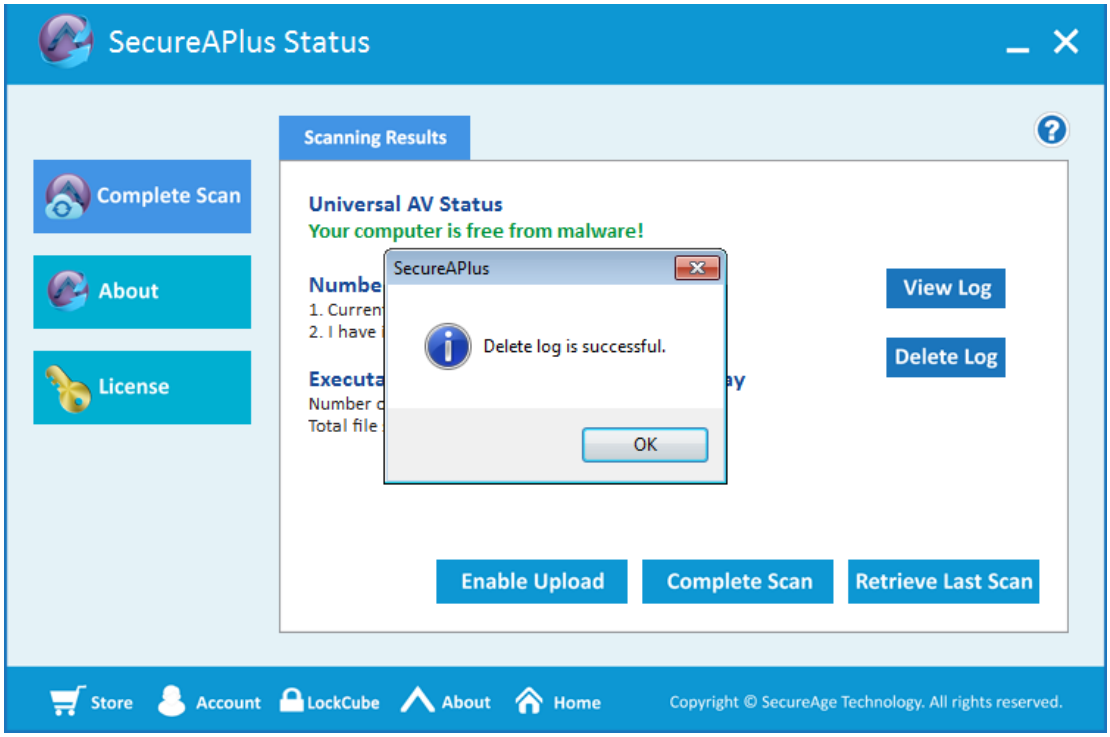
5.5 Delete Universal AV's Log

To purge the Universal AV log, follow the steps below:

- Click on **Delete Log** button.



- The Universal AV log file contents will be deleted.

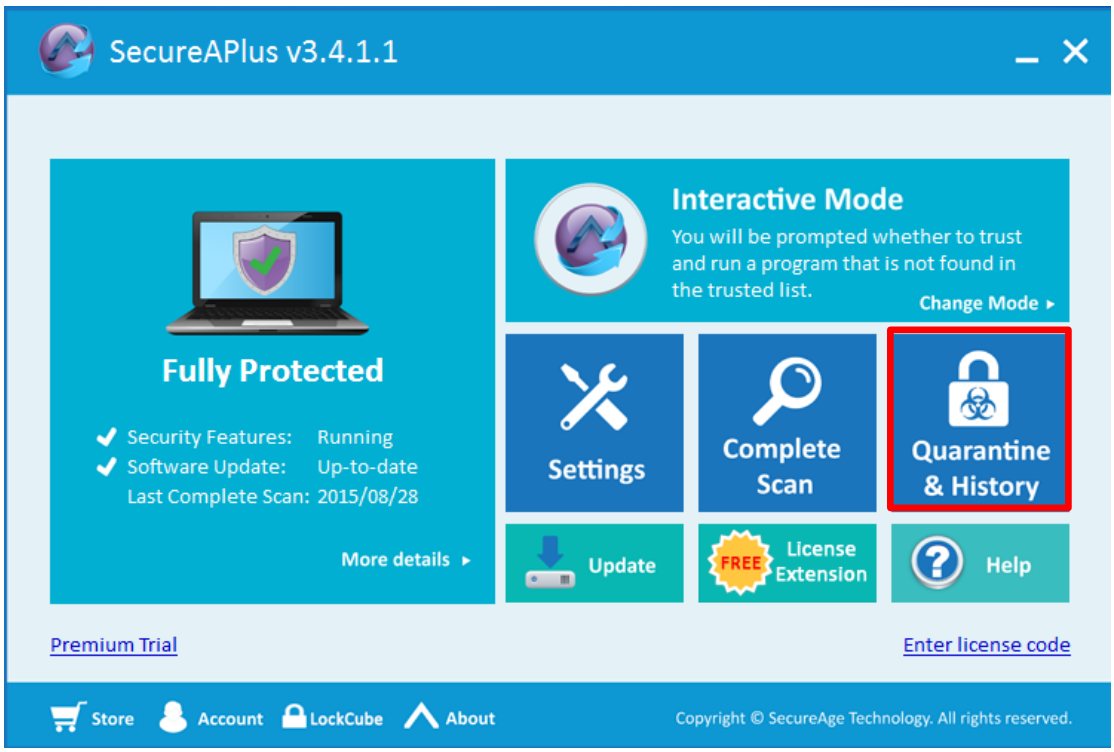


6 Quarantine & History

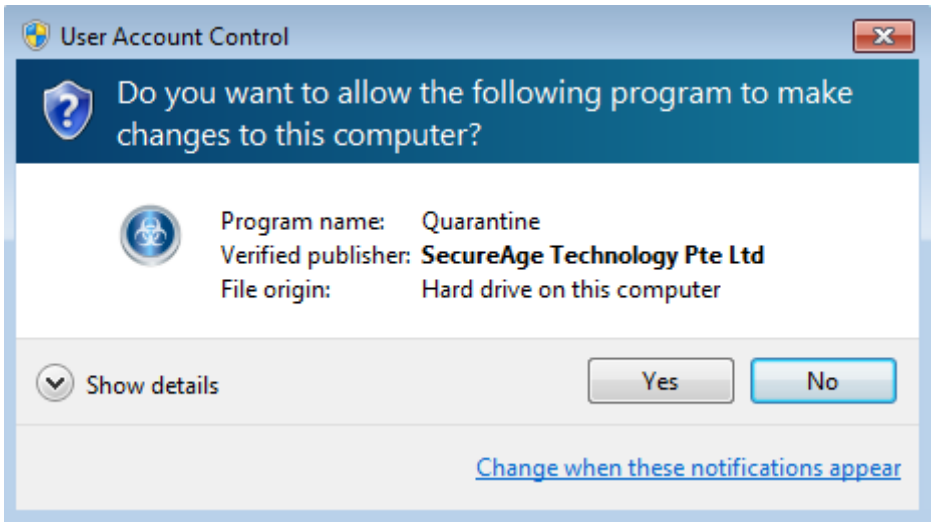
Items which are being detected as threats during scanning will prompt user if it should be quarantine or remove. If user selects the item to be quarantine, it will be quarantine and listed under the quarantine list.

To view the Quarantine & History, follow the steps below:

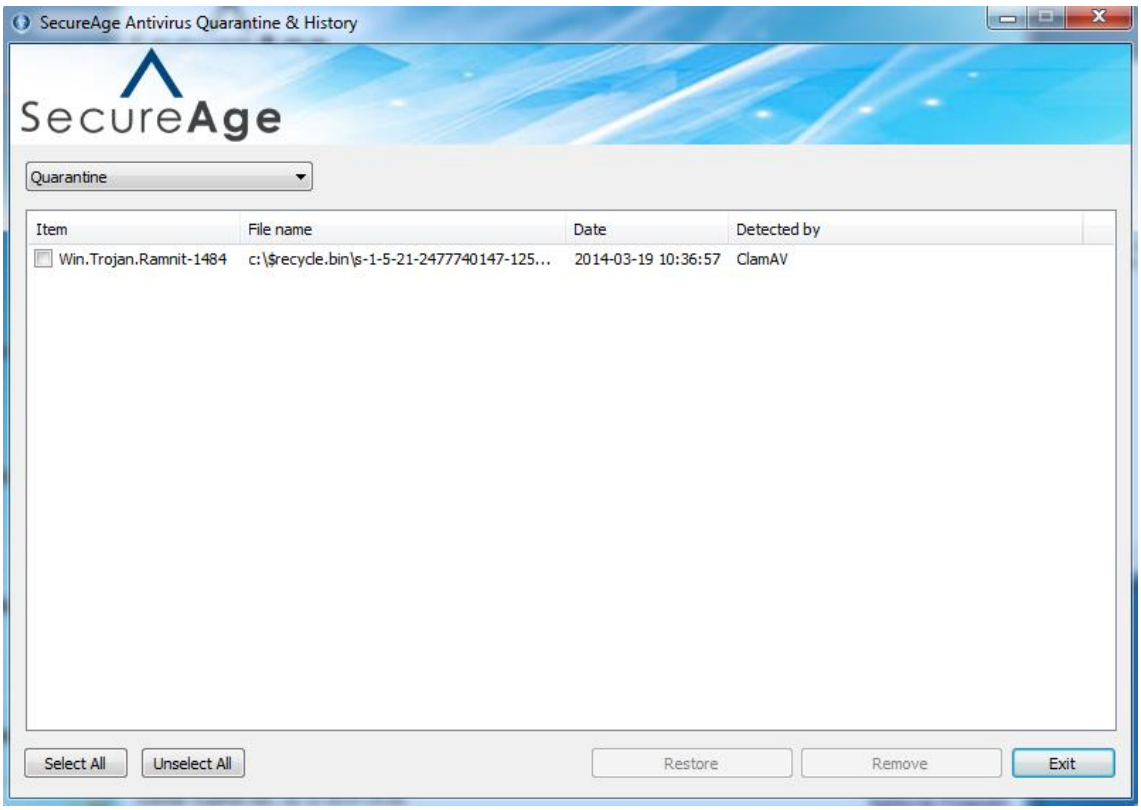
- Start SecureAPlus. Please refer to **Section 2.1** for the steps to start SecureAPlus.
- In the **SecureAPlus** window, click on the **Quarantine & History** icon.



- In **User Account Control** window, click **Yes** to allow Quarantine to run.



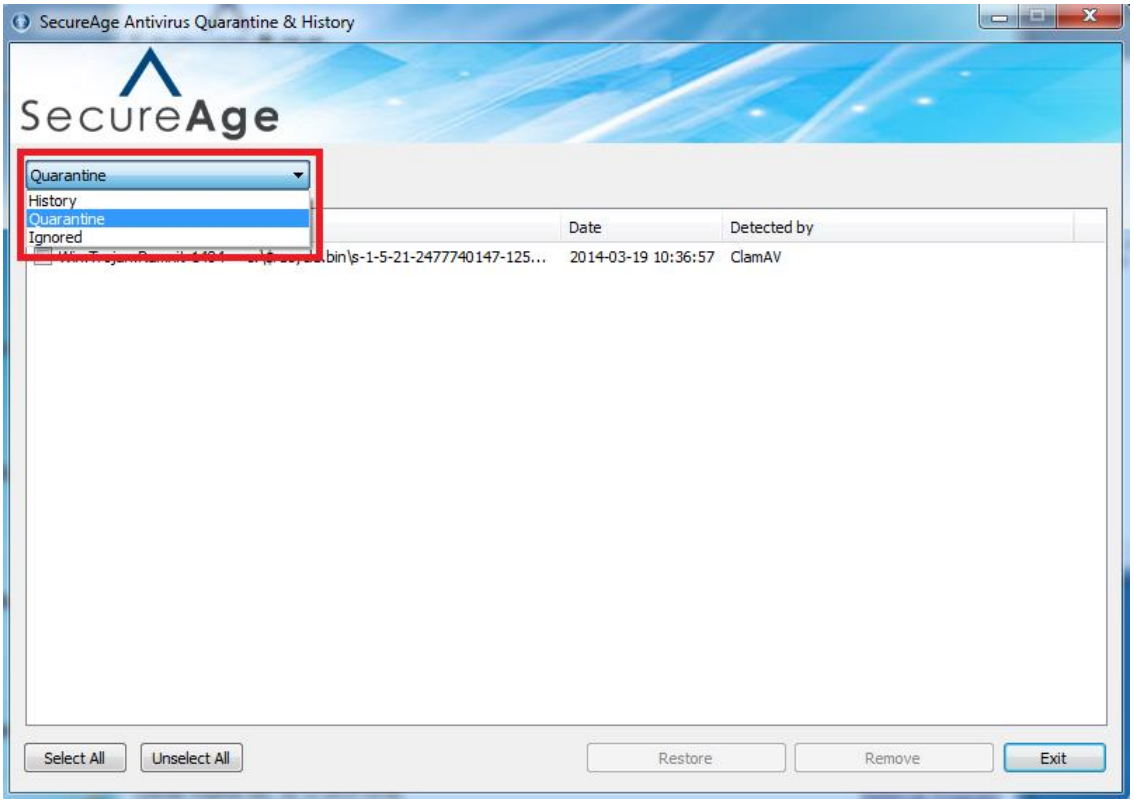
- The **SecureAge Antivirus Quarantine & History** window will launch.



6.1 Quarantine List

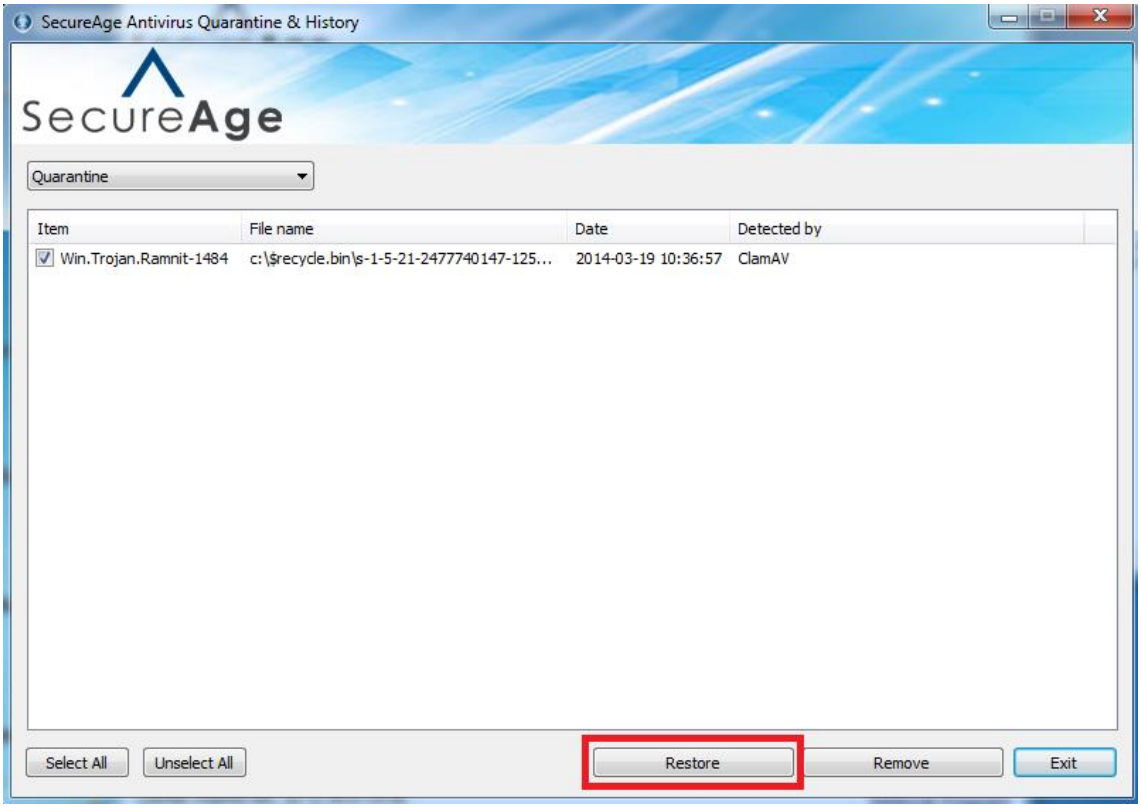
To view the quarantine list, follow the steps below:

- Start SecureAPlus. Please refer to **Section 2.1** for the steps to start SecureAPlus.
- In **SecureAPlus** window, click on **Quarantine & History** icon.
- In the **SecureAge Antivirus Quarantine & History** window, select **Quarantine** from the dropdown box.
- Items detected as threats from scanning which are being quarantined by the user will be listed in the quarantine list.

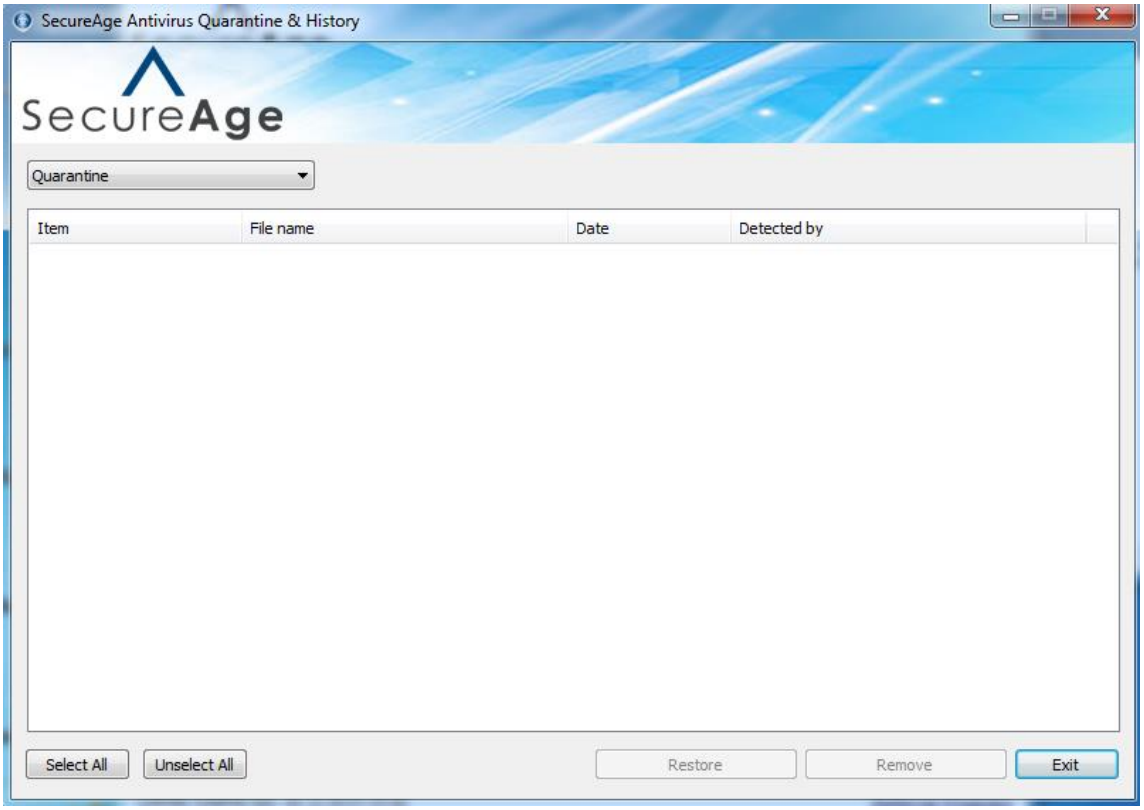


To restore items from the quarantine list, follow the steps below:

- In the **SecureAge Antivirus Quarantine & History** window, select **Quarantine** from the dropdown box.
- Check the items to be restored and click on **Restore** button.

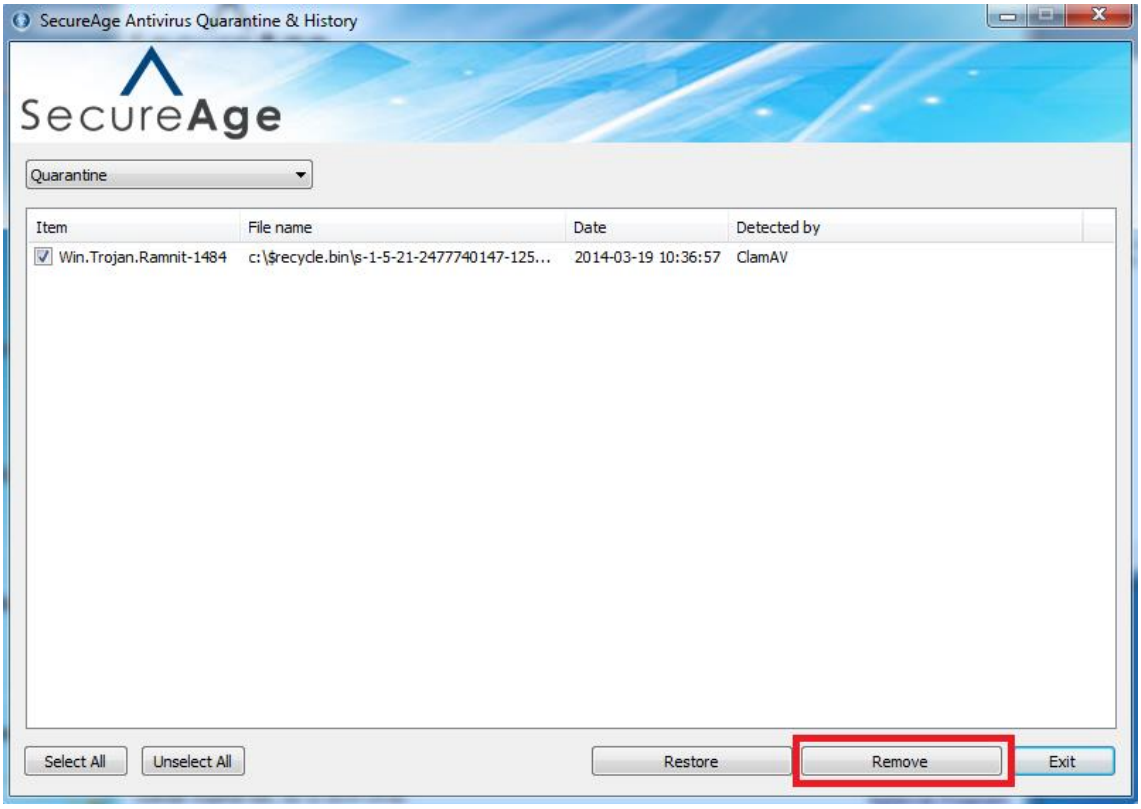


- The selected items will be restored to its original location and cleared from the quarantine list.

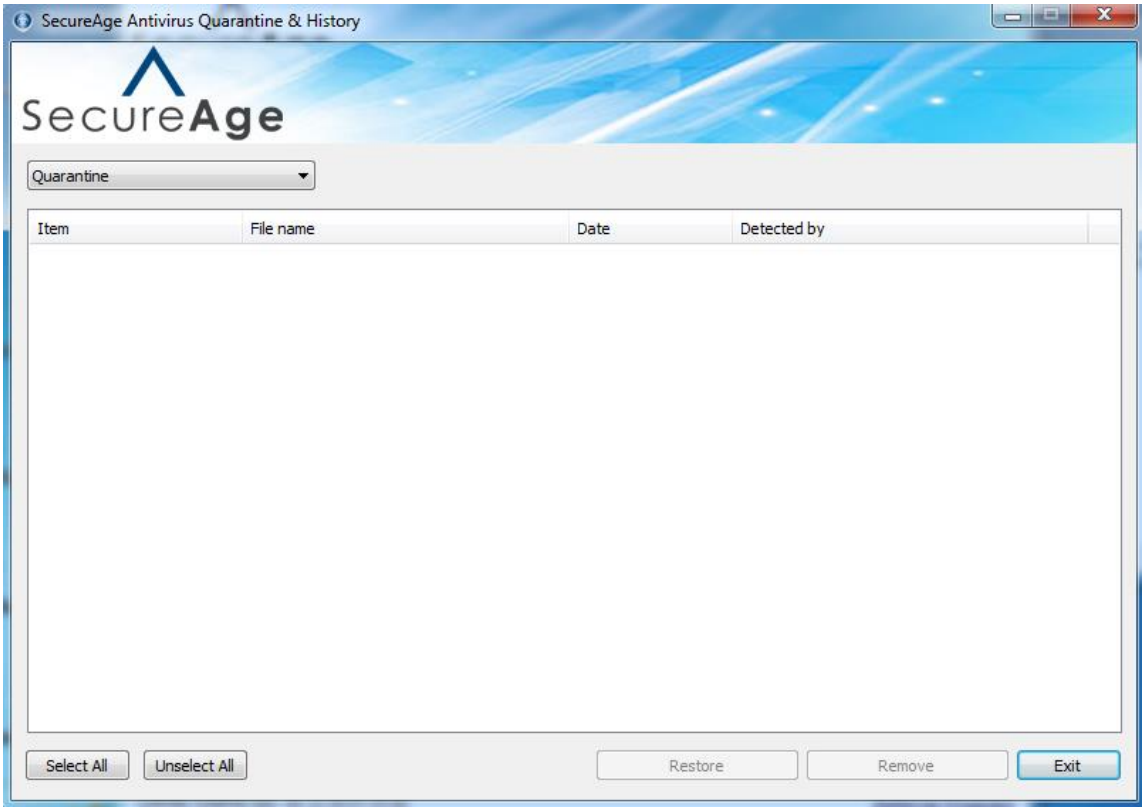


To remove items from the quarantine list, follow the steps below:

- In the **SecureAge Antivirus Quarantine & History** window, select **Quarantine** from the dropdown box.
- Check the items to be removed and click on **Remove** button.



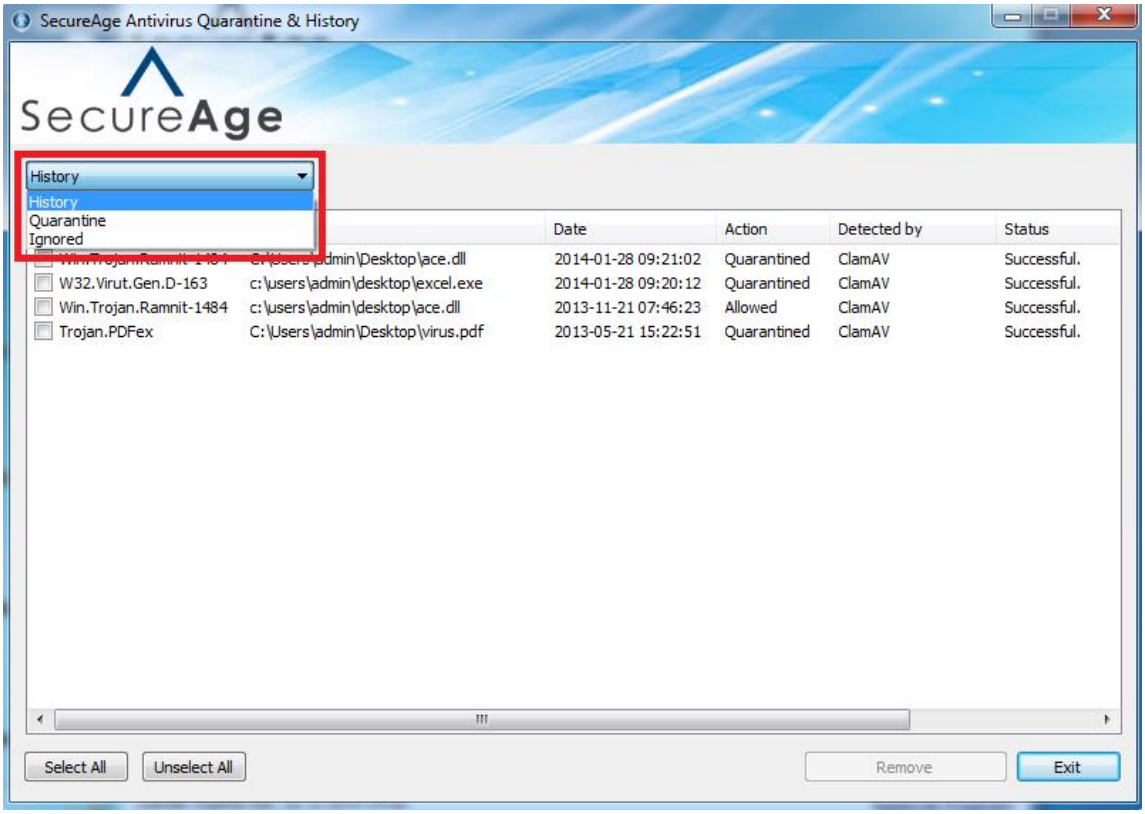
- The selected items will be cleared from the quarantine list.



6.2 History List

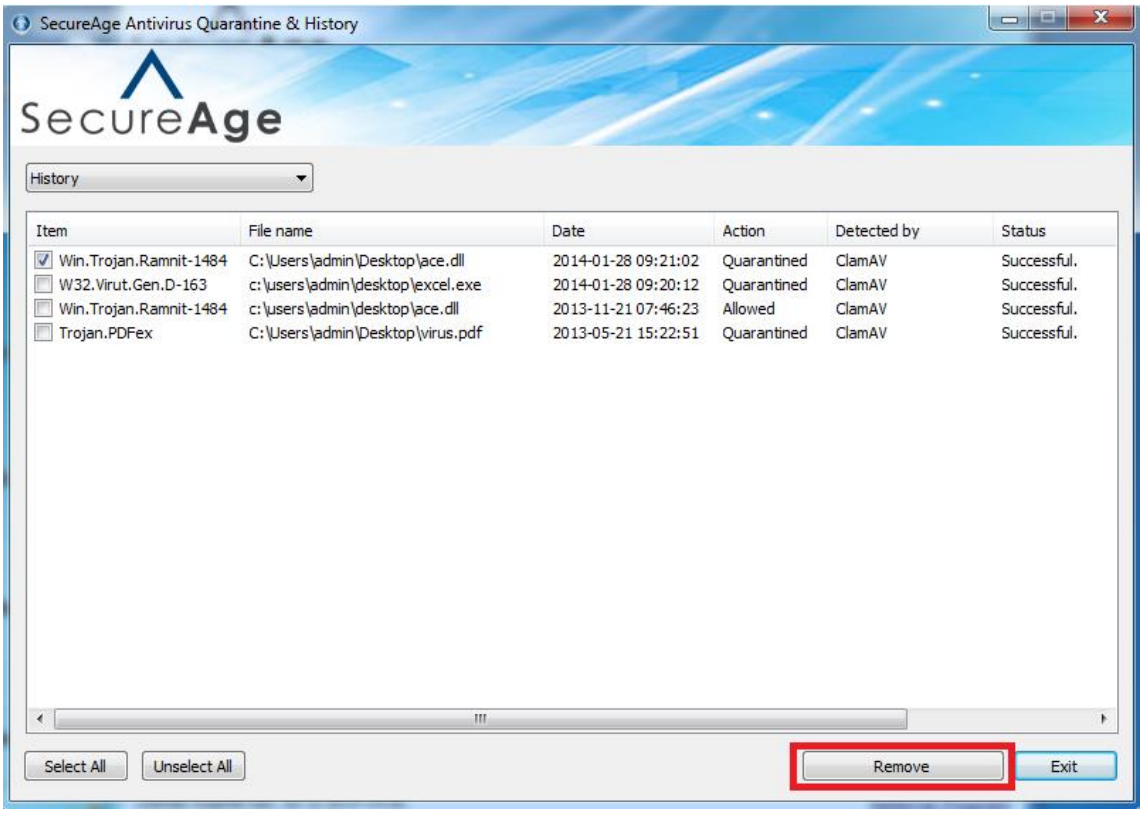
To view the history, follow the steps below:

- Start SecureAPlus. Please refer to **Section 2.1** for the steps to start SecureAPlus.
- In **SecureAPlus** window, click on **Quarantine & History** icon.
- In the **SecureAge Antivirus Quarantine & History** window, select **History** from the dropdown box.
- History of the quarantine and detected items with detailed information such as threat name, affected filename, date of detection and action taken will be shown in the history list.

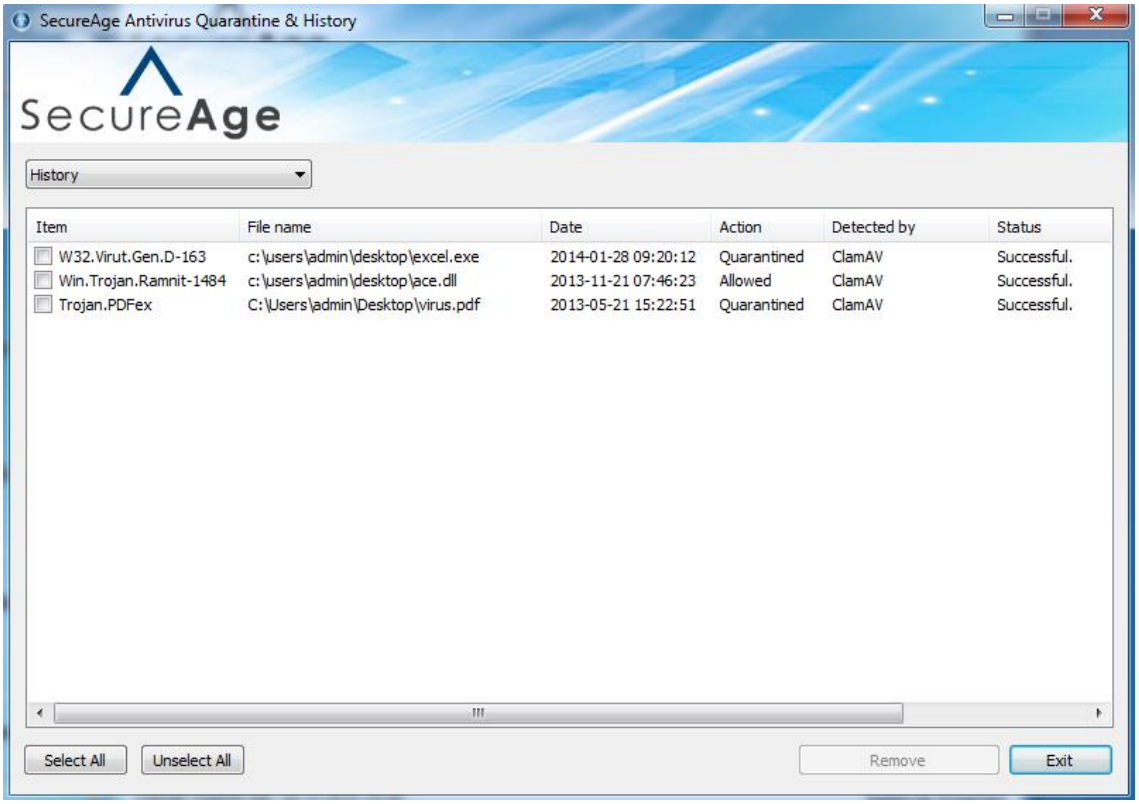


To remove items from the history list, follow the steps below:

- In the **SecureAge Antivirus Quarantine & History** window, select **History** from the dropdown box.
- Check the items to be removed and click on **Remove** button.



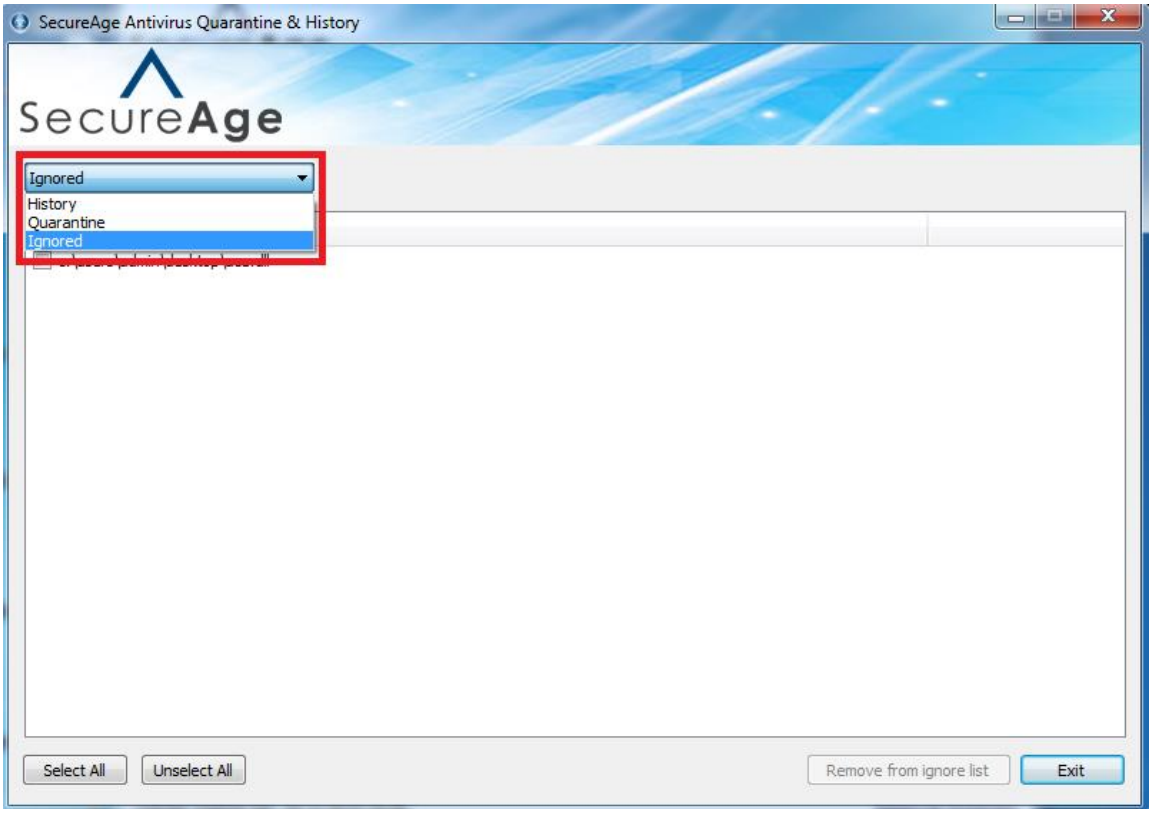
- The selected items will be cleared from the history list.



6.3 Ignored List

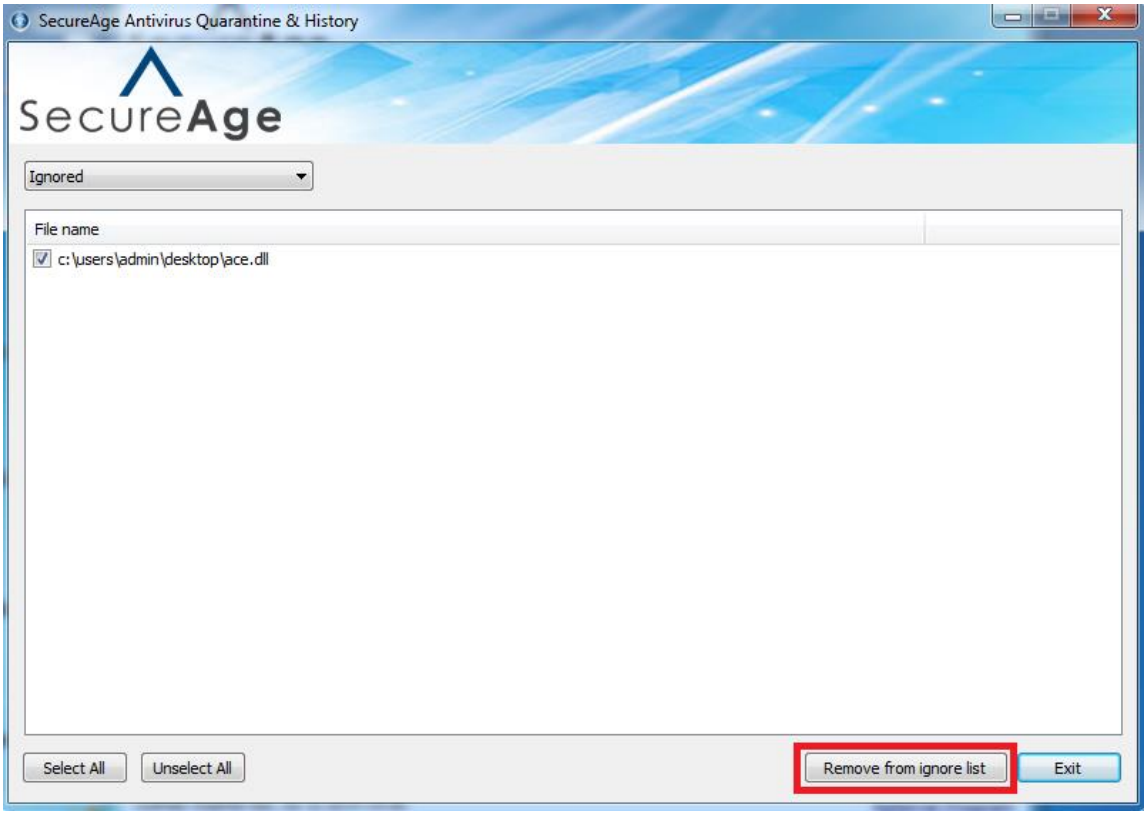
To view the ignored list, follow the steps below:

- Start SecureAPlus. Please refer to **Section 2.1** for the steps to start SecureAPlus.
- In **SecureAPlus** window, click on **Quarantine & History** icon.
- In the **SecureAge Antivirus Quarantine & History** window, select **Ignored** from the dropdown box.
- The files which are being opted to be ignored at the point of detection will be shown in the ignored list.

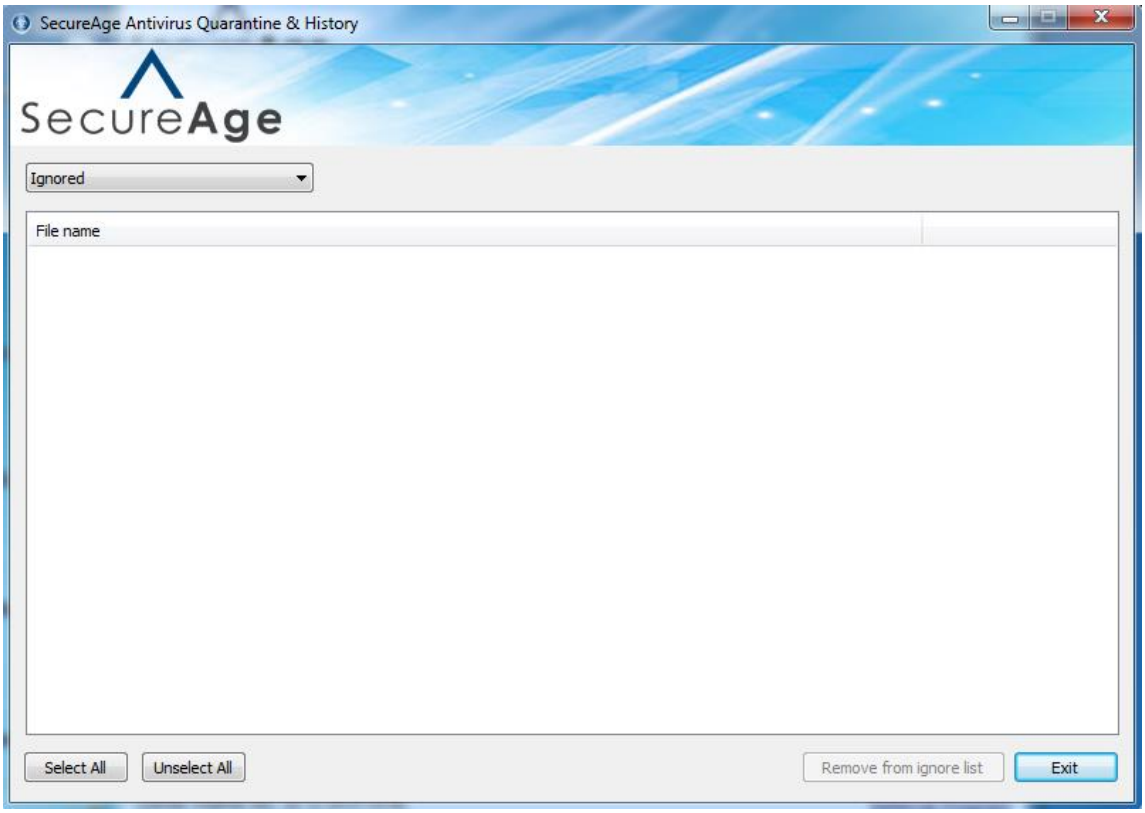


To remove items from the ignored list, follow the steps below:

- In the **SecureAge Antivirus Quarantine & History** window, select **Ignored** from the dropdown box.
- Check the items to be removed and click on **Remove from ignore list** button.



- The selected items will be cleared from the ignored list.



7 Application Whitelisting

Application Whitelisting is a new feature of SecureAge that is being bundled together with SecureAPlus to further enhance and strengthens the antivirus scanning with trusted protection. Application Whitelisting tags a trust level to all the applications and executable, such that untrusted (not whitelisted) applications will not be able to execute, hence minimising the chances of unauthorised malware from damaging user's systems.

7.1 Definitions of Trust Levels

In Application Whitelisting, there are three levels of trust for applications and are summarized in the table below:

Trust Level	Explanation
Not Trusted (0)	The application is not allowed to be executed at all. Any files that are created by this application will not be trusted as well.
Trusted Application (1)	The application is allowed to be executed, but all the files that are created by a **Trusted Application** will be **Not Trusted**. For example, explorer.exe is a **Trusted Application**, but all files that are created by explorer.exe will not be automatically trusted. Using explorer.exe, a user may copy any files from anywhere, and all of these files cannot be automatically set as **Trusted Application** without the administrator approval. Similar situations apply for applications such as Internet Browser, FTP, e-mail client, etc. For better security measurement, most of applications should fall under this category.
Trusted Installer (2)	Installer, uninstaller, and updater applications are usually fall into this category. A **Trusted Installer** is allowed to be executed, and all files that are created or rename by a **Trusted Installer** will be automatically set as **Trusted Application**. There is a special exception for update process. When a **Trusted Installer** found that the file already exists, and the trust level has been set to be **Trusted Installer**, **Trusted Installer** will not downgrade the file as a **Trusted Application**, instead it will keep the trust level as it is.

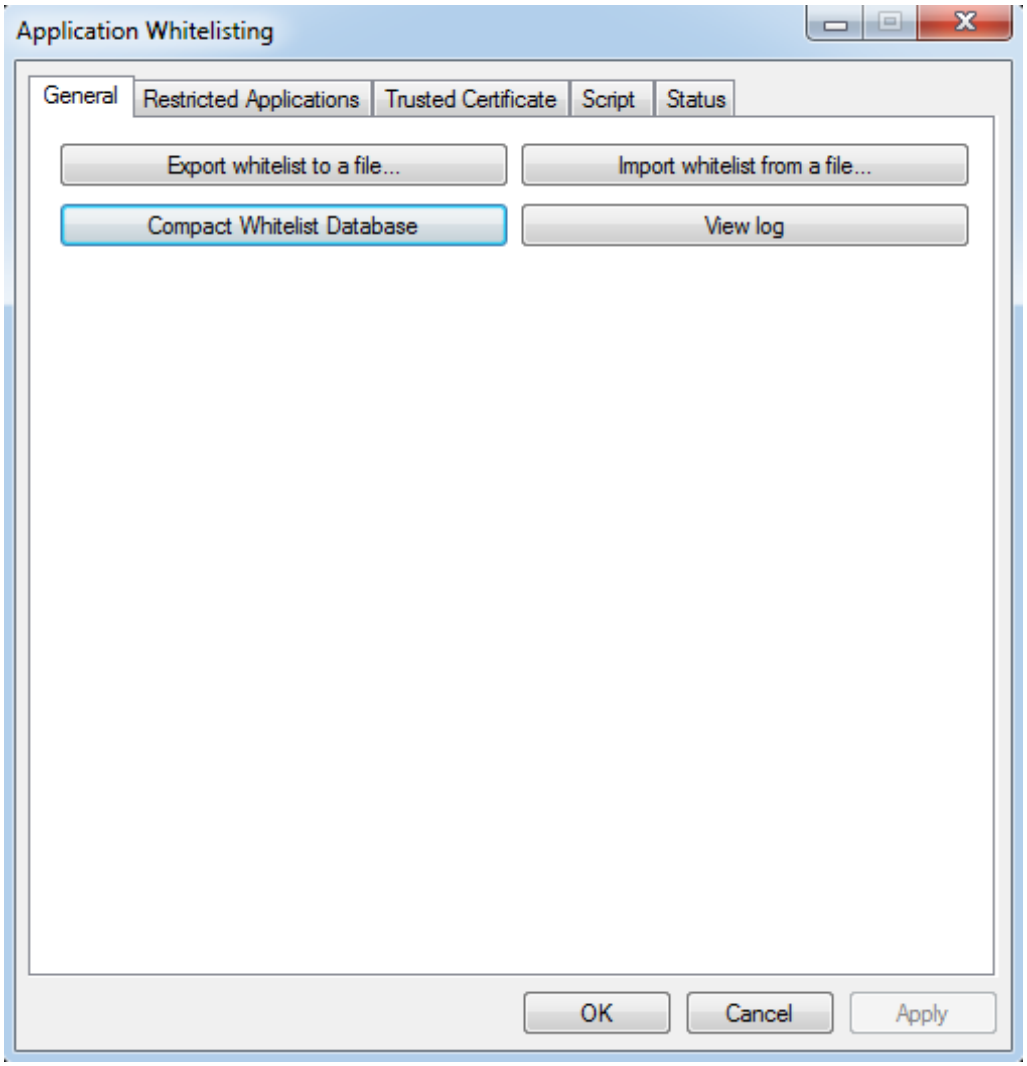
Note:

- Refer to **Section 7.3, 7.4** on how to view and manually set the trust levels of applications, also managing the behaviours of Application Whitelisting.

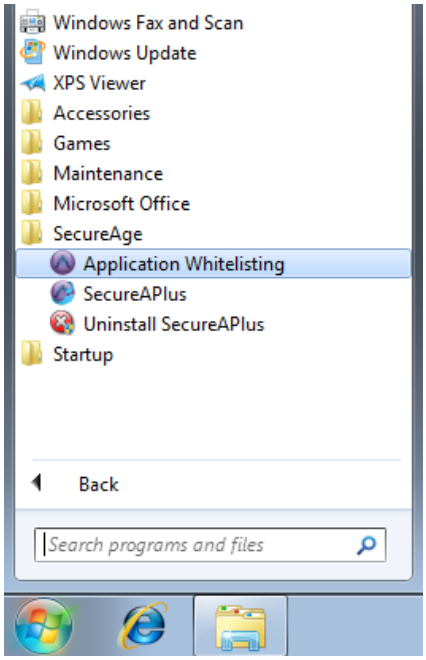
7.2 Application Whitelisting Advanced Settings

To configure Application Whitelisting advanced settings, follow the steps below:

- Start SecureAPlus. Please refer to **Section 2.1** for the steps to start SecureAPlus.
- In **SecureAPlus** window, click on the **Settings** icon to view the settings.
- In the **SecureAPlus Settings** window, click on **Application Whitelisting** on the left menu.
- Click on the **Advanced Settings** button within either the **Standard Mode** tab or **Advanced Mode** tab under **Application Whitelisting** on the left menu. The **Application Whitelisting** window will launch.



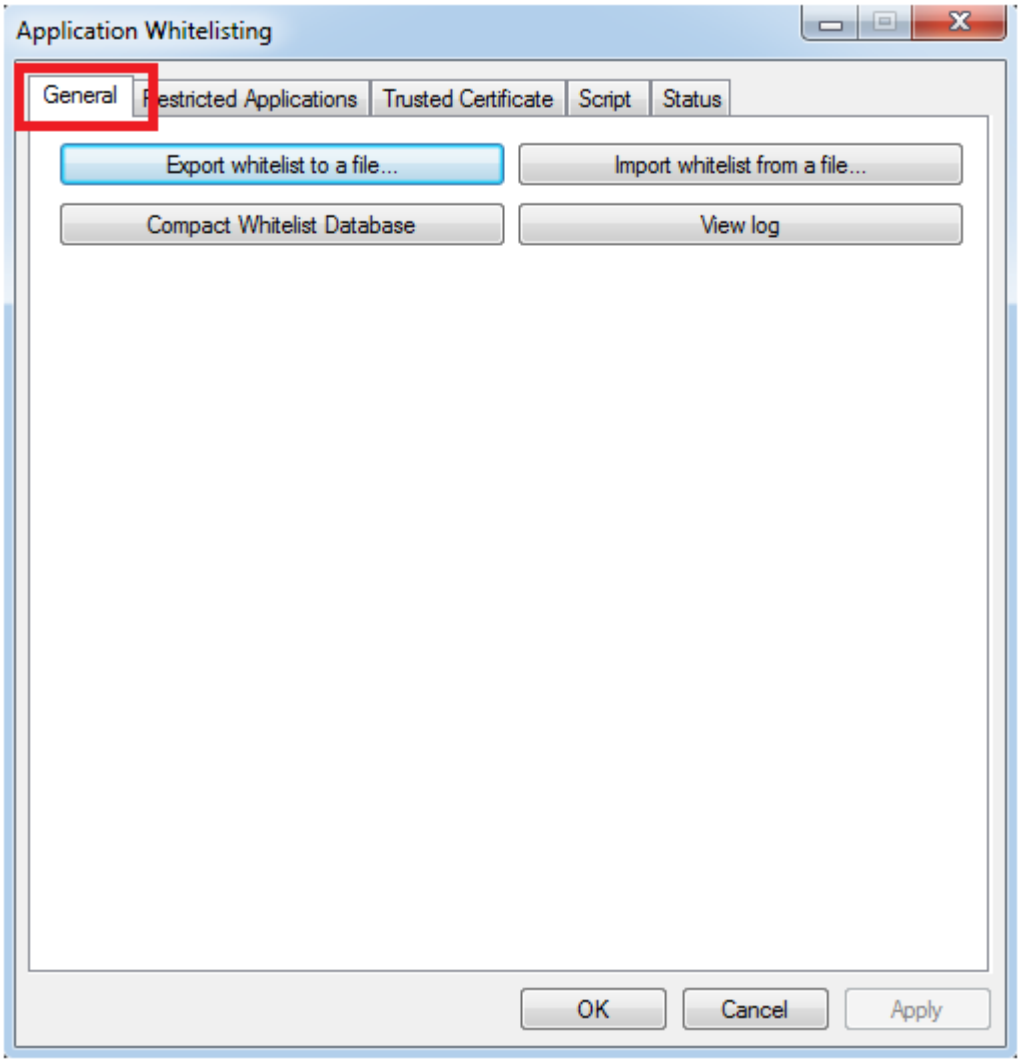
- Alternatively to navigate to this **Application Whitelisting Settings** window directly, you can click **Start**, point to **All Programs**. Click on **SecureAge** and click on **Application Whitelisting**.



7.2.1 General Settings

In the **General** tab, users can manage the Application Whitelisting settings.

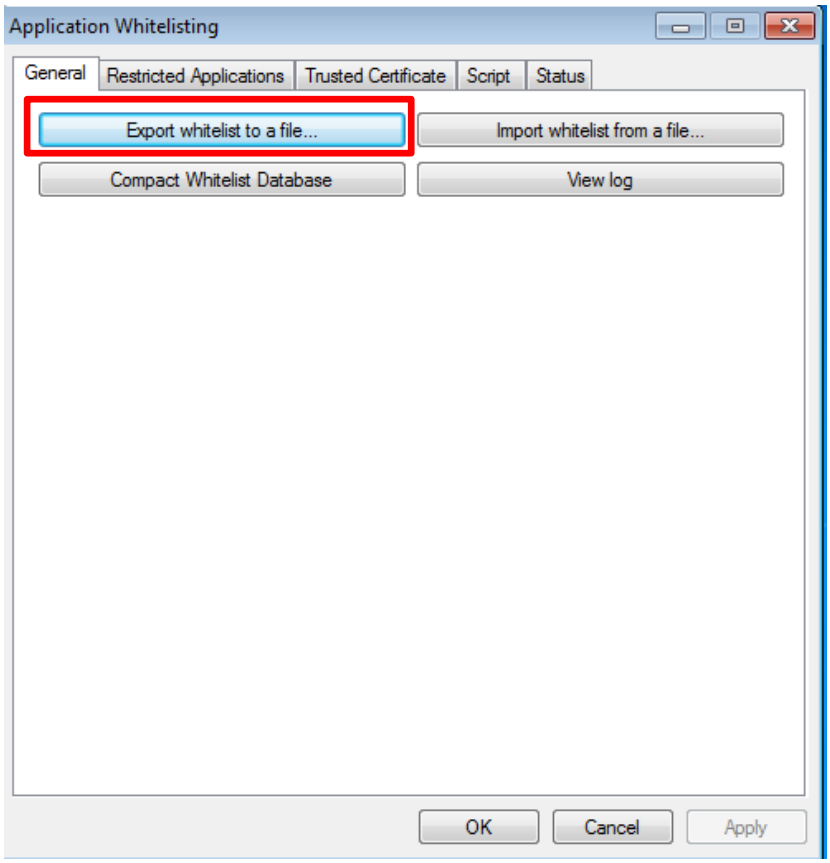
- Export whitelist to a file – Click on the **Export whitelist to a file...** button.
- Import whitelist from a file – Click on the **Import whitelist from a file...** button.
- Compact Whitelist Database – Click on the **Compact Whitelist Database** button.
- View log – Click on **View log** button to view the Application Whitelisting log.



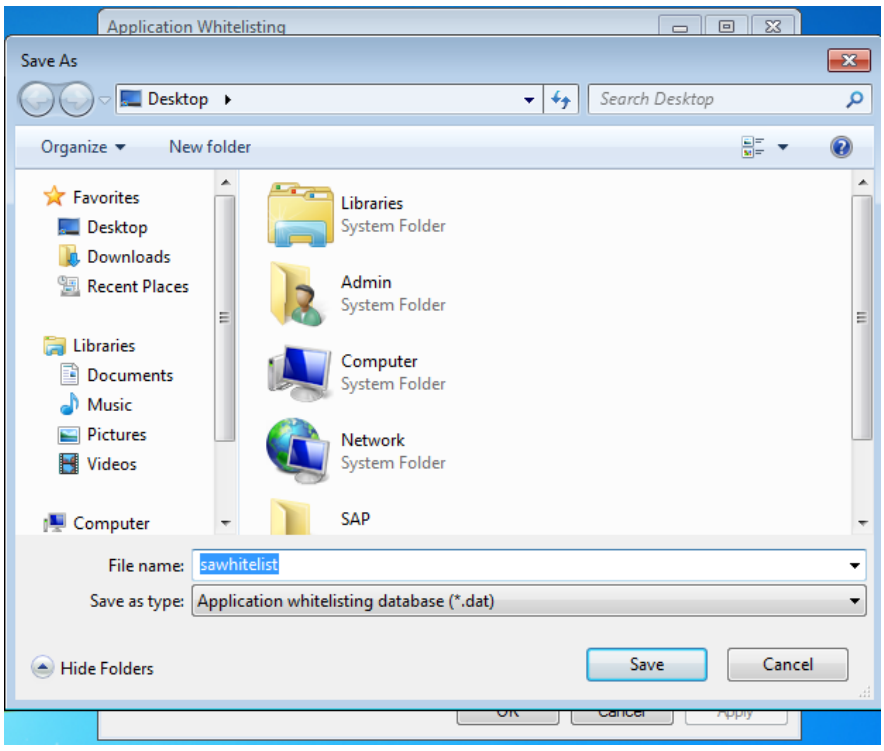
Export whitelist to a file

To export whitelist to a file, follow the steps below:

- Click on **Export whitelist to a file…** button.



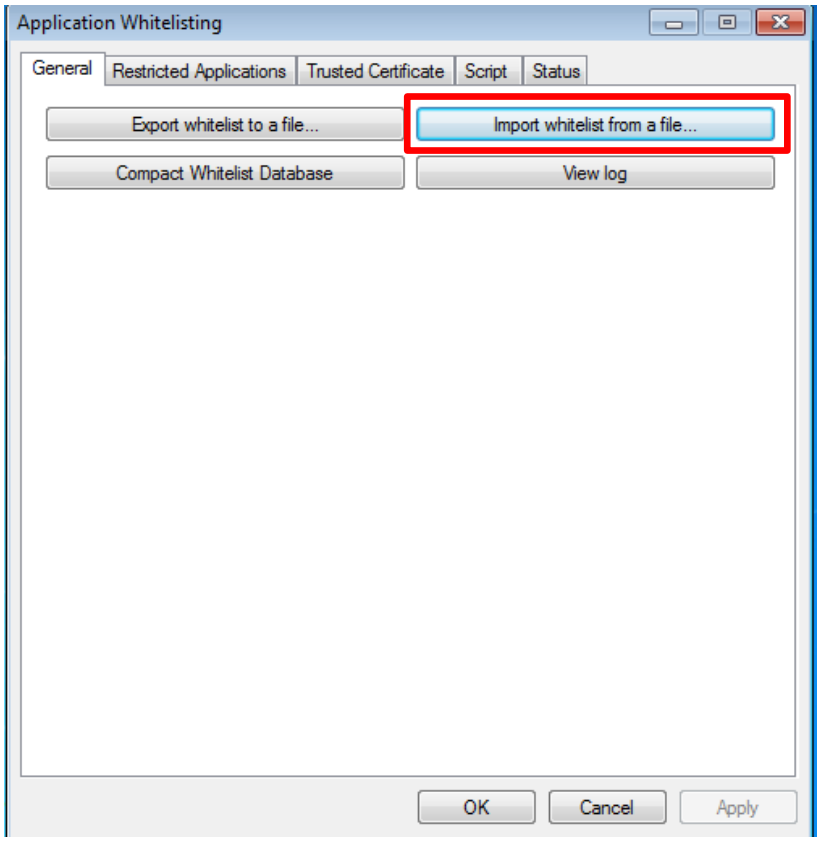
- Choose the location to save the application whitelisting database (.dat) file.



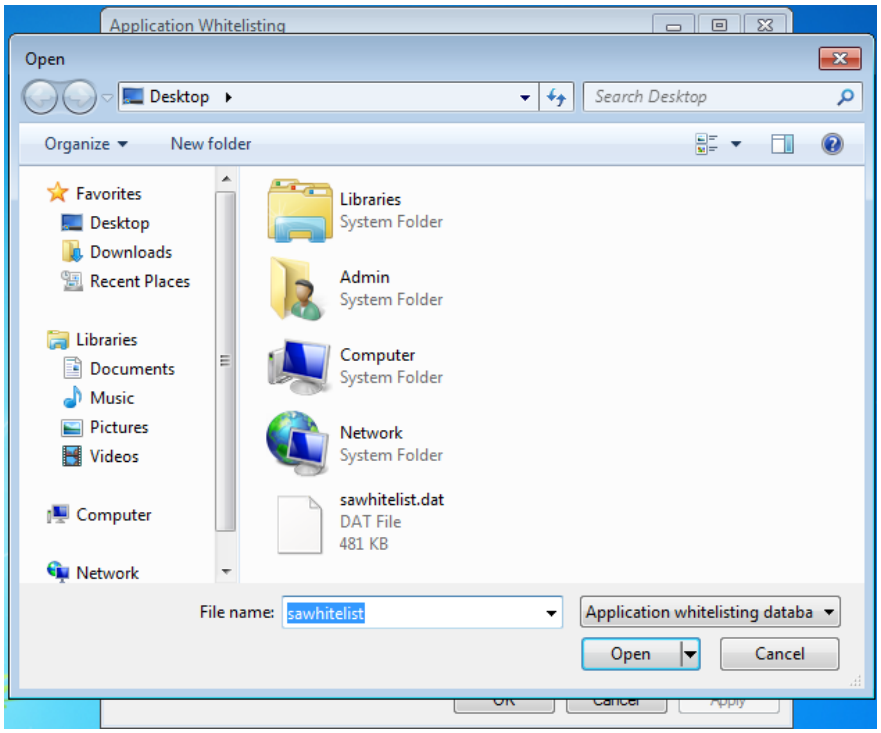
Import whitelist from a file

To import whitelist from a file, follow the steps below:

- Click on **Export whitelist to a file…** button.



- Open the application whitelisting database (.dat) file

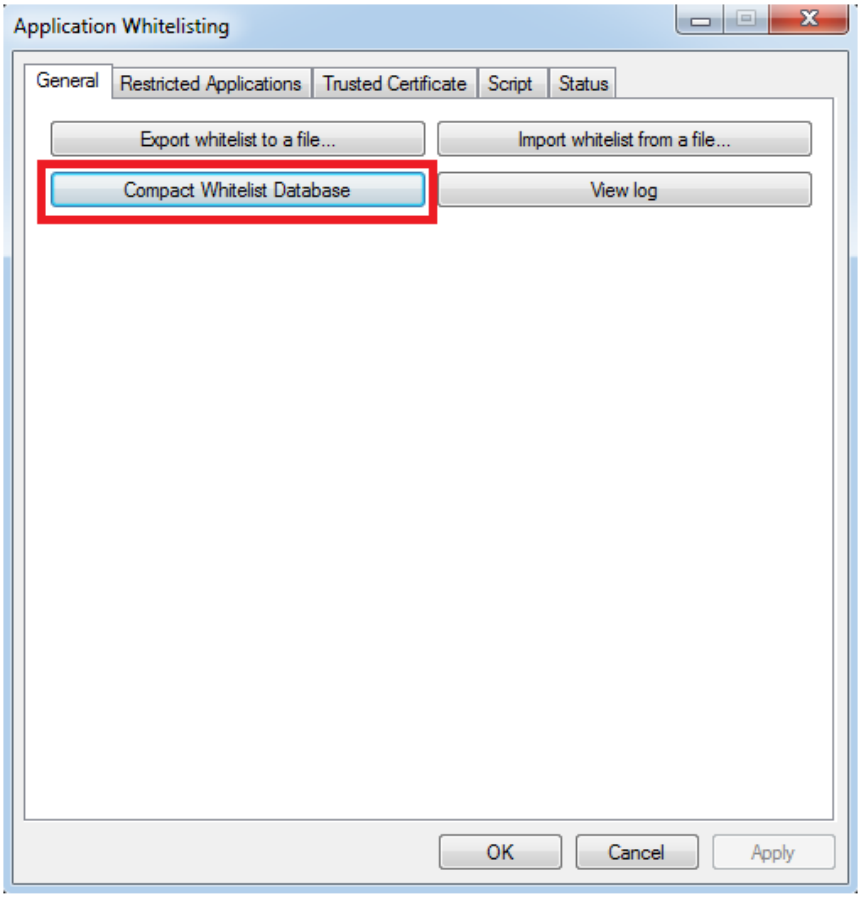


Compact whitelist database

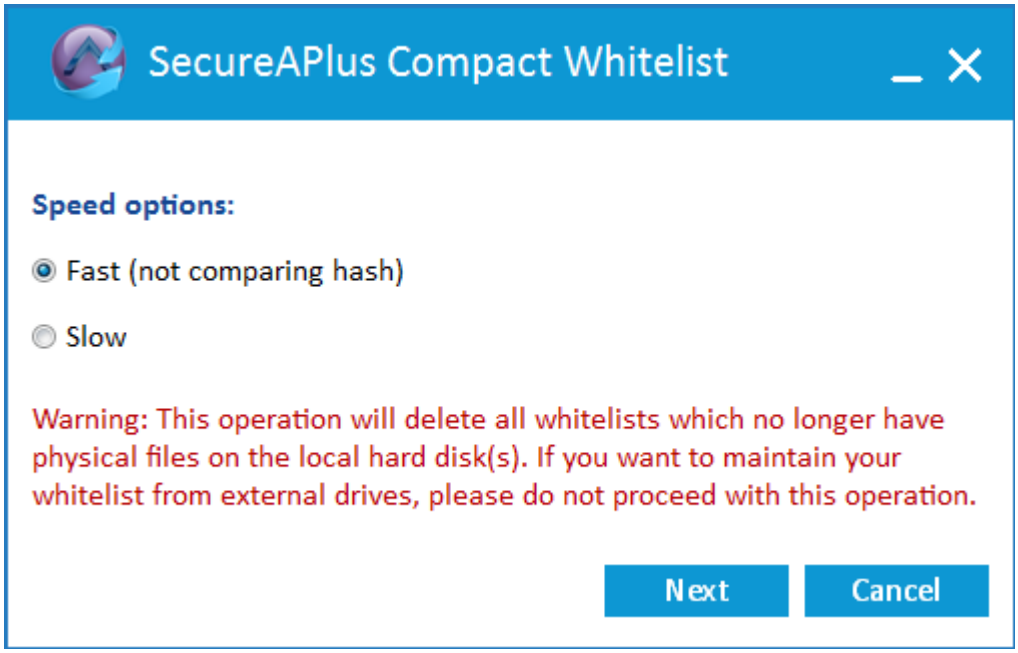
Compact whitelist database helps to remove whitelist entries where the files are no longer exist in the local hard disk.

To compact whitelist database, follow the steps below:

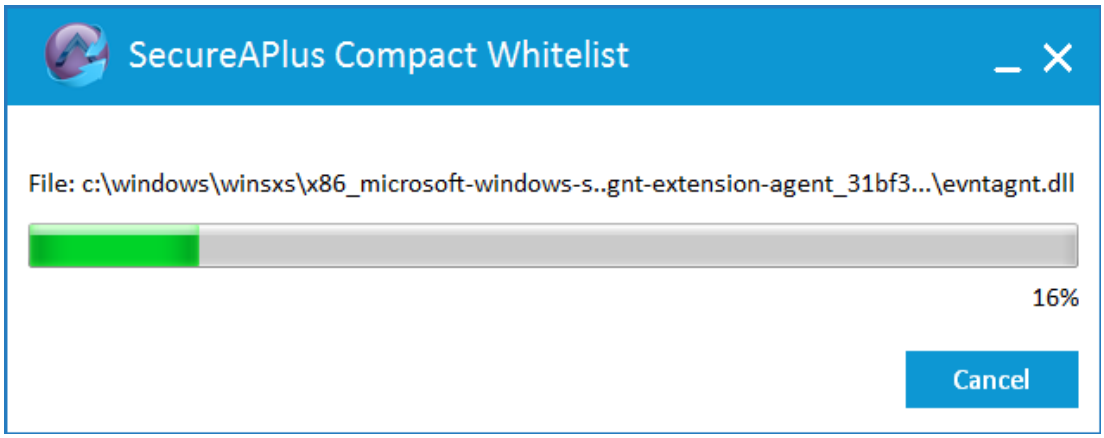
- Click on **Compact Whitelist Database** button



- Choose the speed to compact whitelist and click on **Next** button.



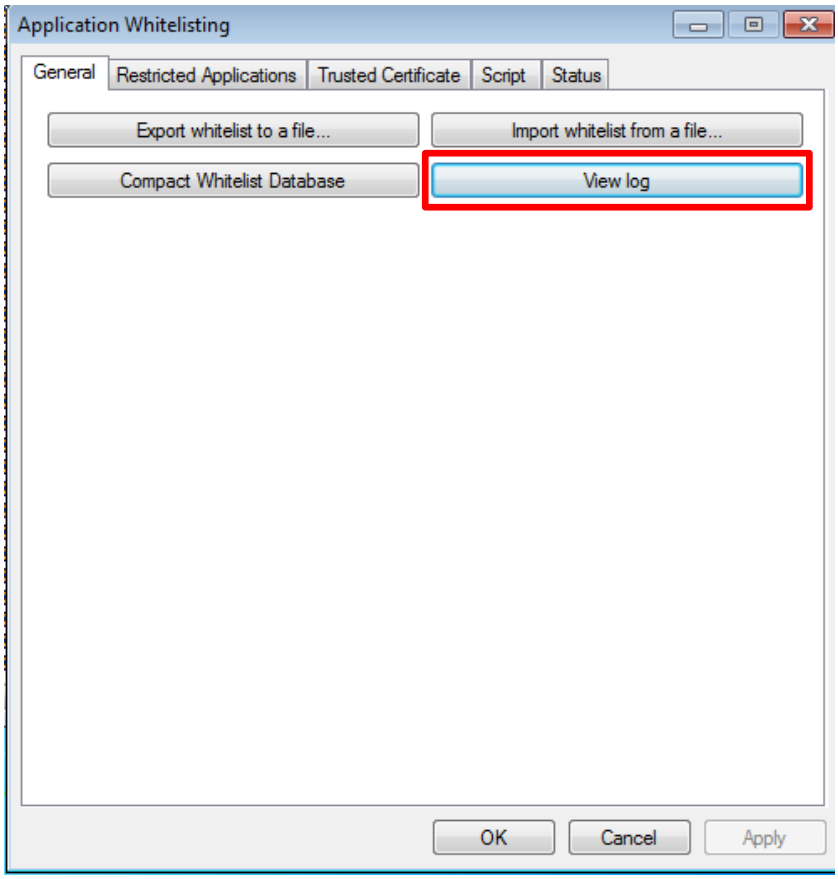
- The SecureAPlus Compact Whitelist will start.



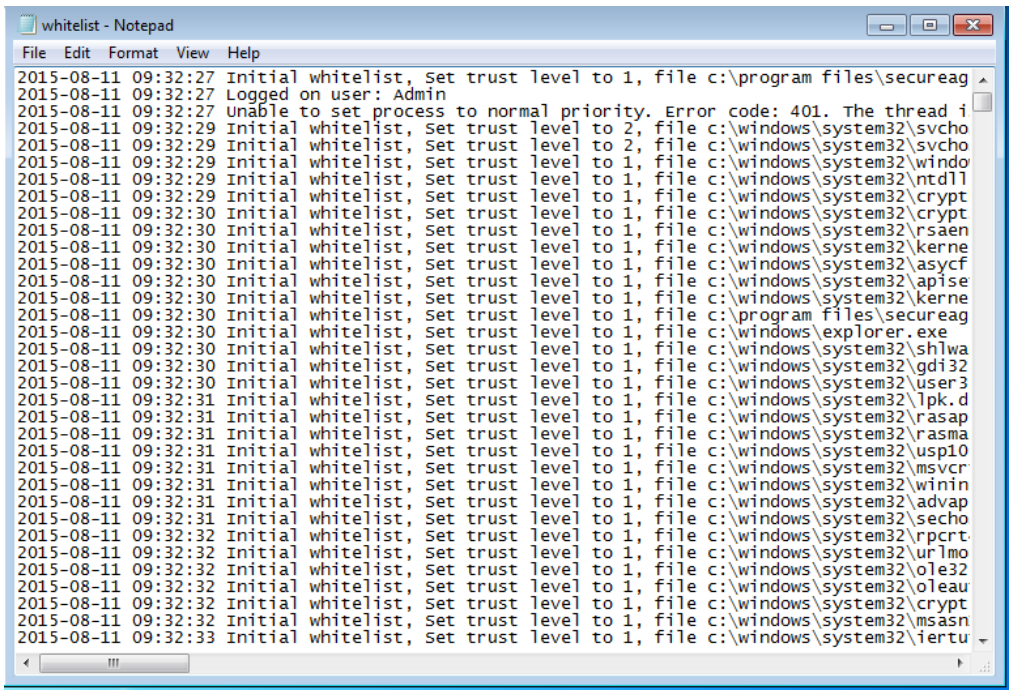
View Log

To view the application whitelisting log, follow the step below:

- Click on **View Log** button



- The application whitelisting log file will be opened using the default program.

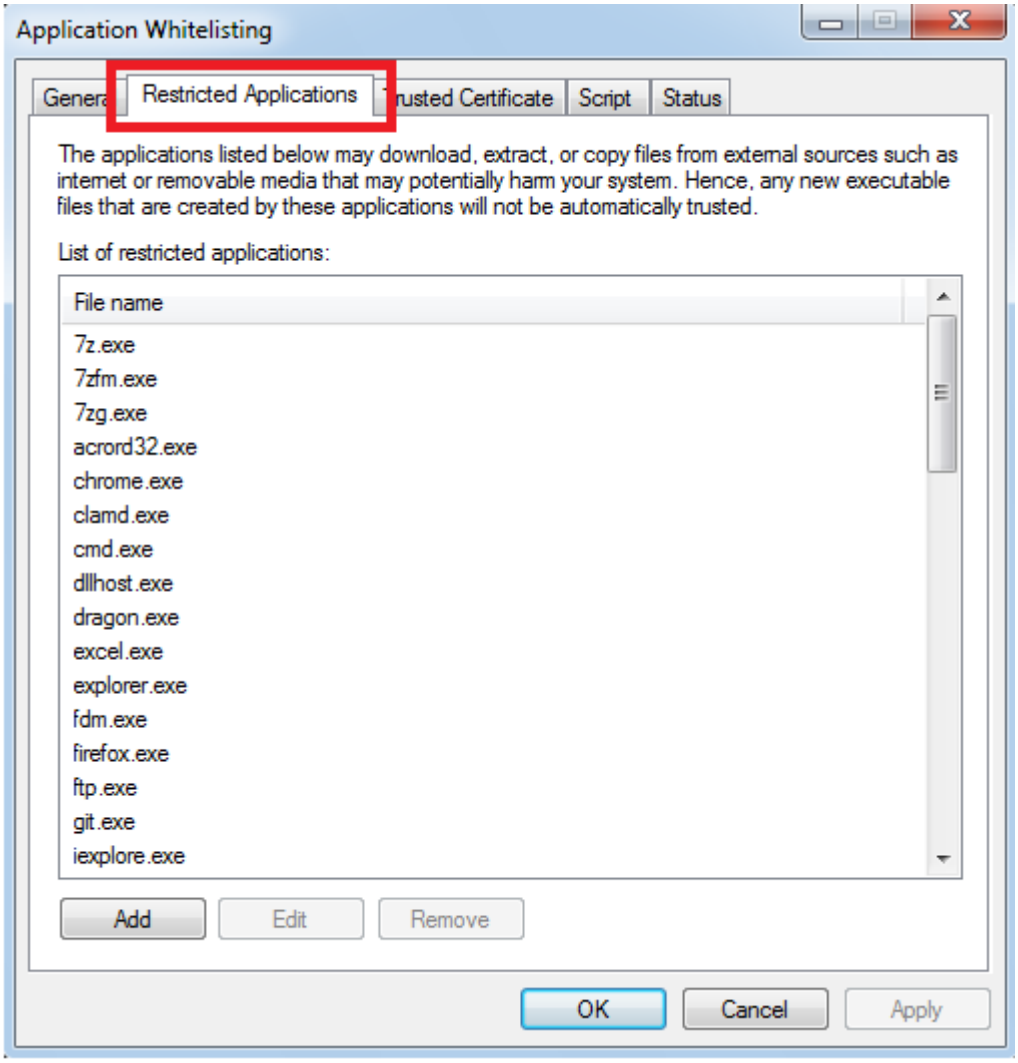


7.2.2 Restricted Applications

In the **Restricted Applications** tab, users can choose to set the application as restricted application (trusted application with restrictions) in which any new files created by it will not be automatically trusted. This is to restrict the application so that it does not automatically bring in other applications that may potentially harm the user's system.

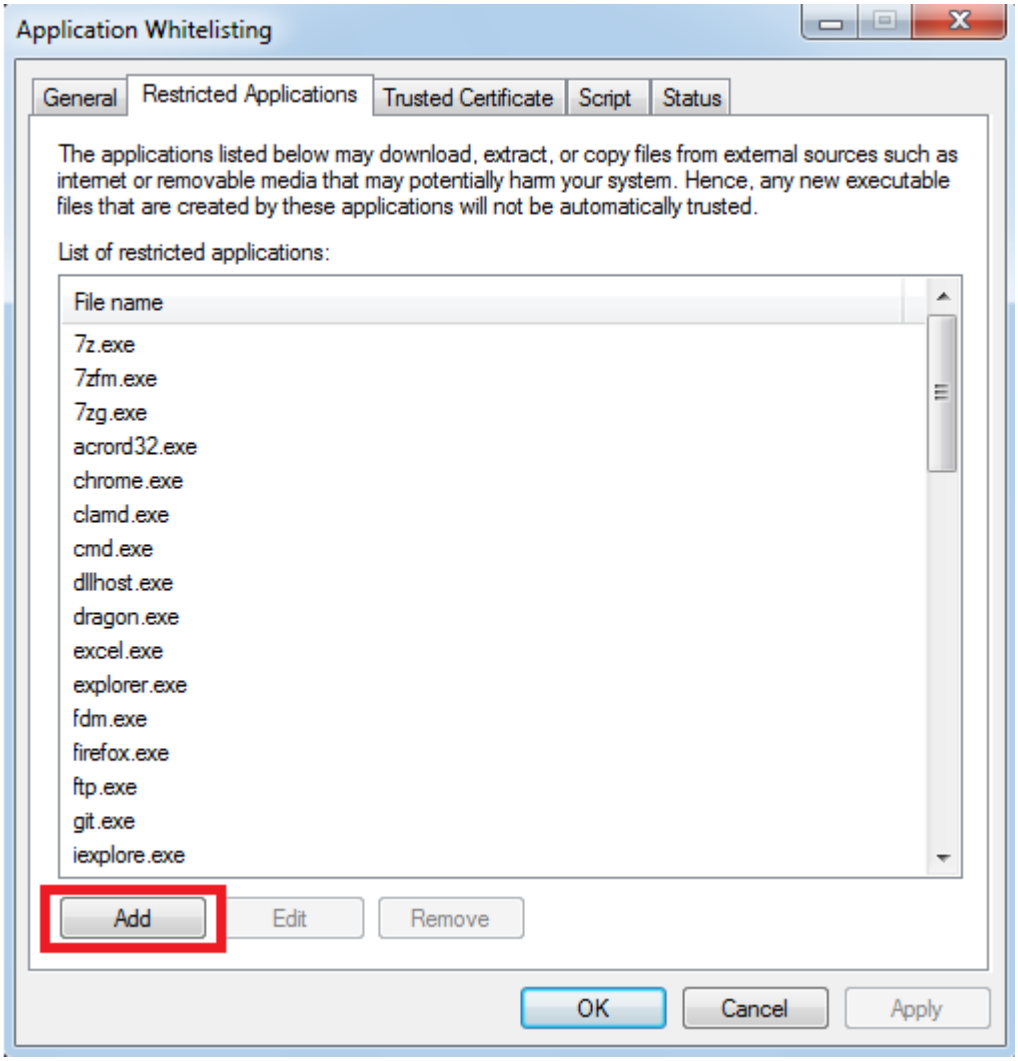
For example:

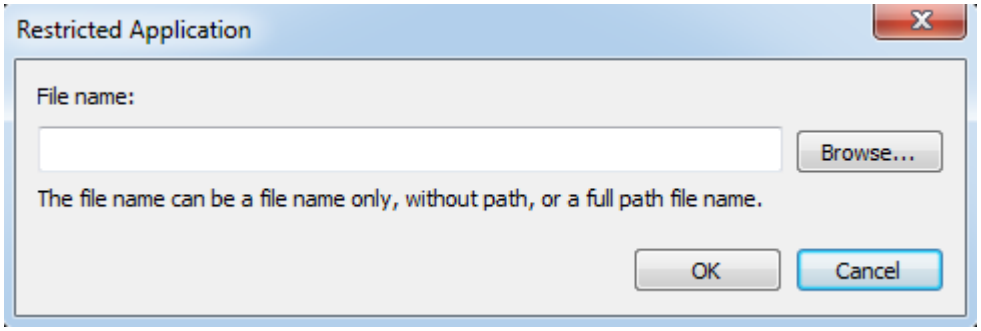
Internet Explorer can download, extract or copy files from external sources and some of these files may be potentially harmful to the system. Especially for unsigned files (not trusted) and when it tries to execute, Application Whitelisting will block it or prompt user for appropriate actions.



To add Restricted Application, follow the steps below to add:

- Click on **Add** button.
- In **Restricted Applications** window, under **File name**, click on **Browse** to select the restricted application executable. Click **OK**.

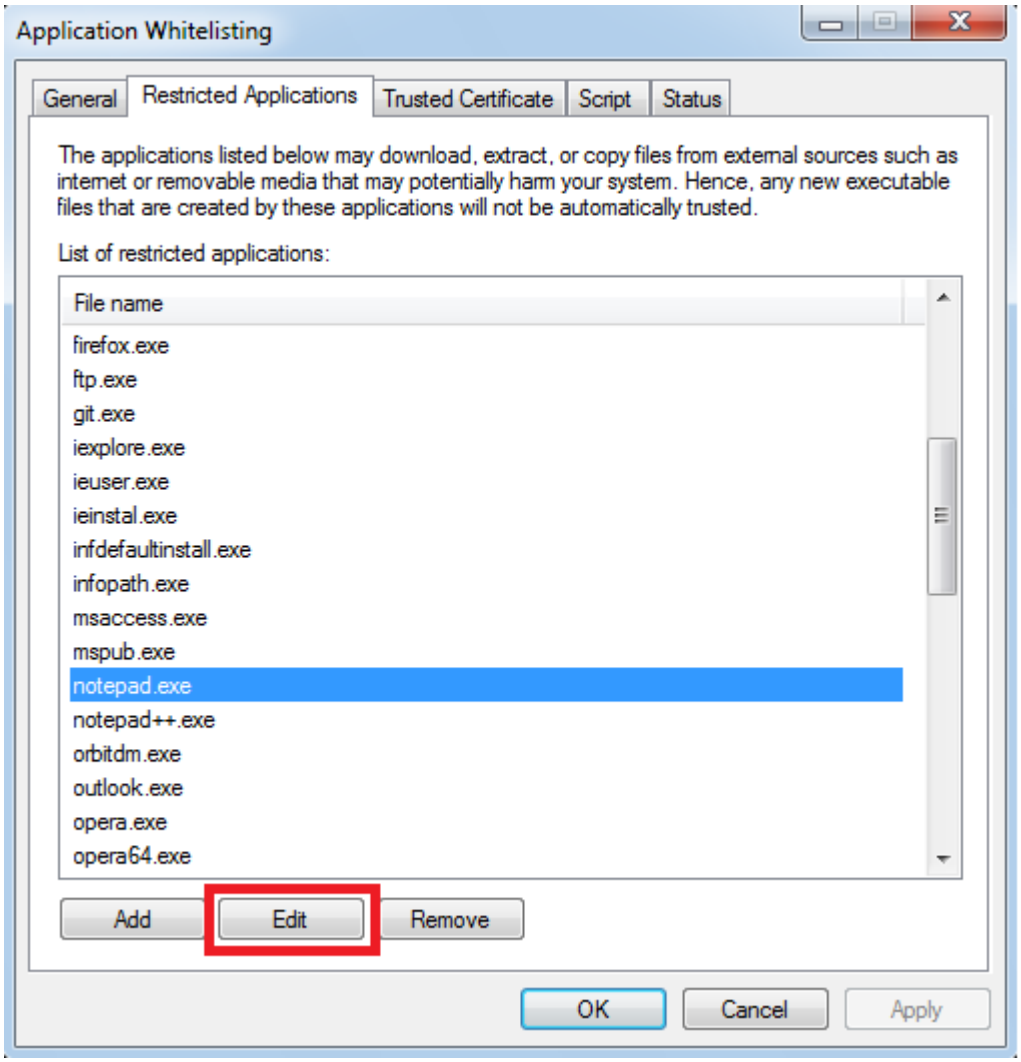


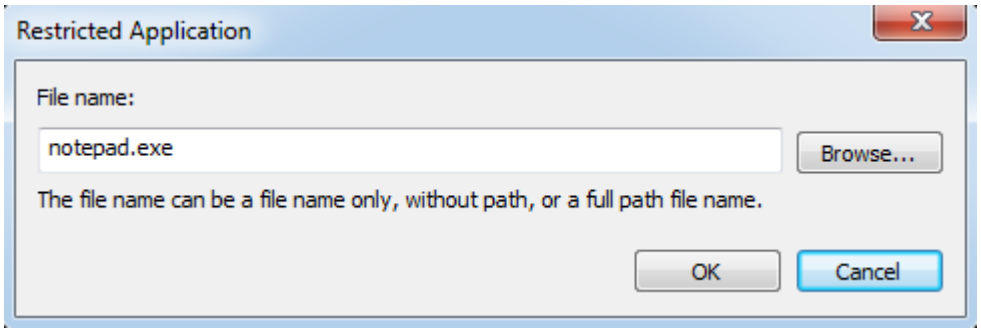


- The newly added restricted application will be added to the list. Then click on **Apply** button to apply the changes made.

To edit Restricted Application, follow the steps below to edit:

- Select a restricted application from the list and click on **Edit** button.
- Make changes and click on **OK** button.

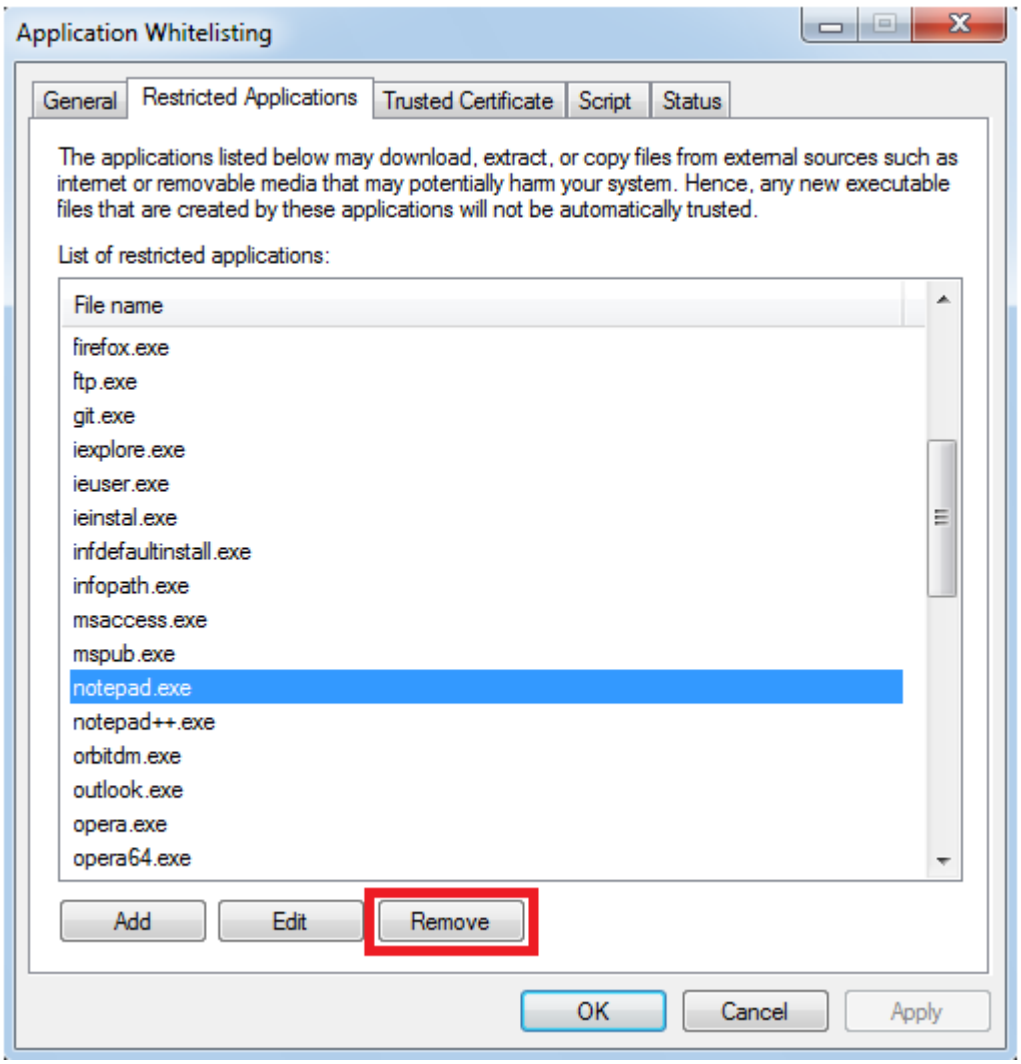




- The restricted application will be edited. Then click on **Apply** button to apply the changes made.

To remove Restricted Application, follow the steps below to remove:

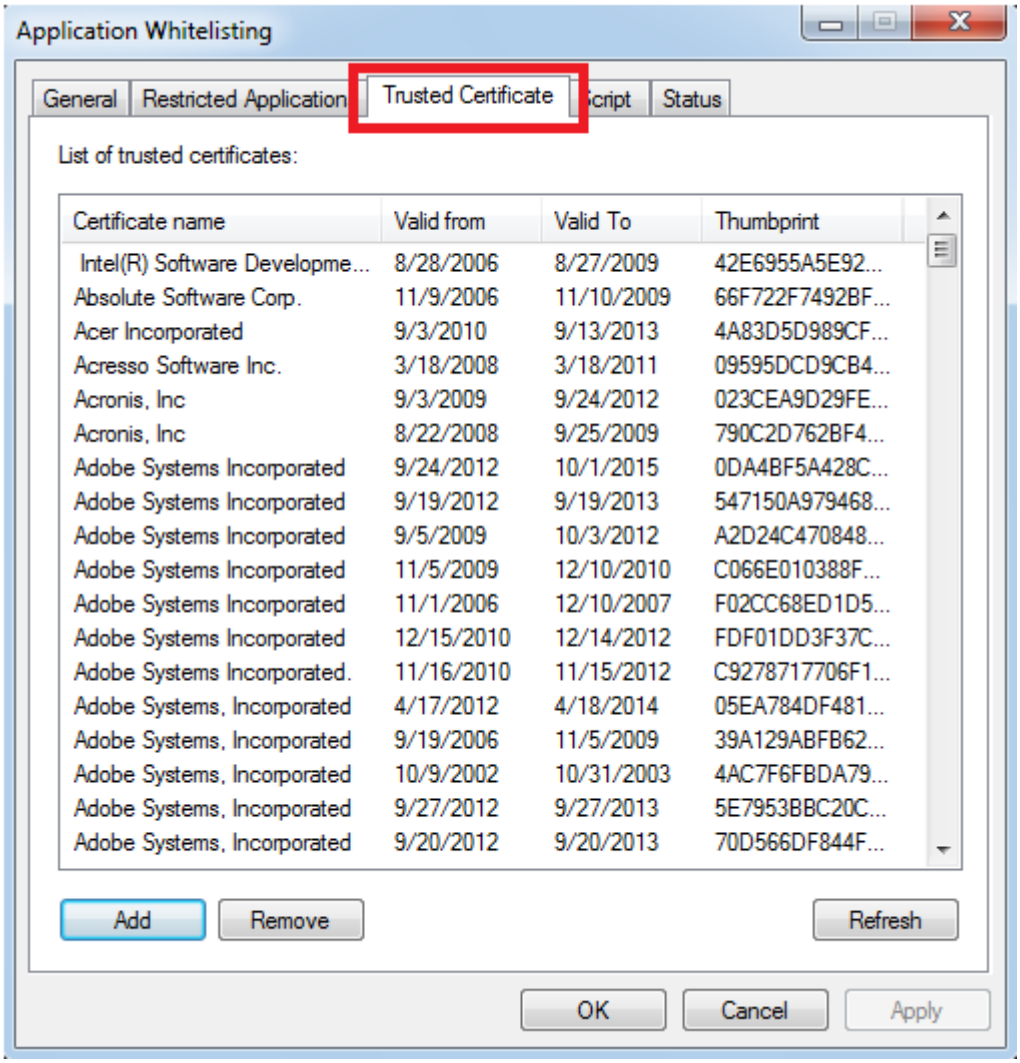
- Select a restricted application from the list and click on **Remove** button.



- The selected restricted application will be removed from the list. Then click on **Apply** button to apply the changes made.

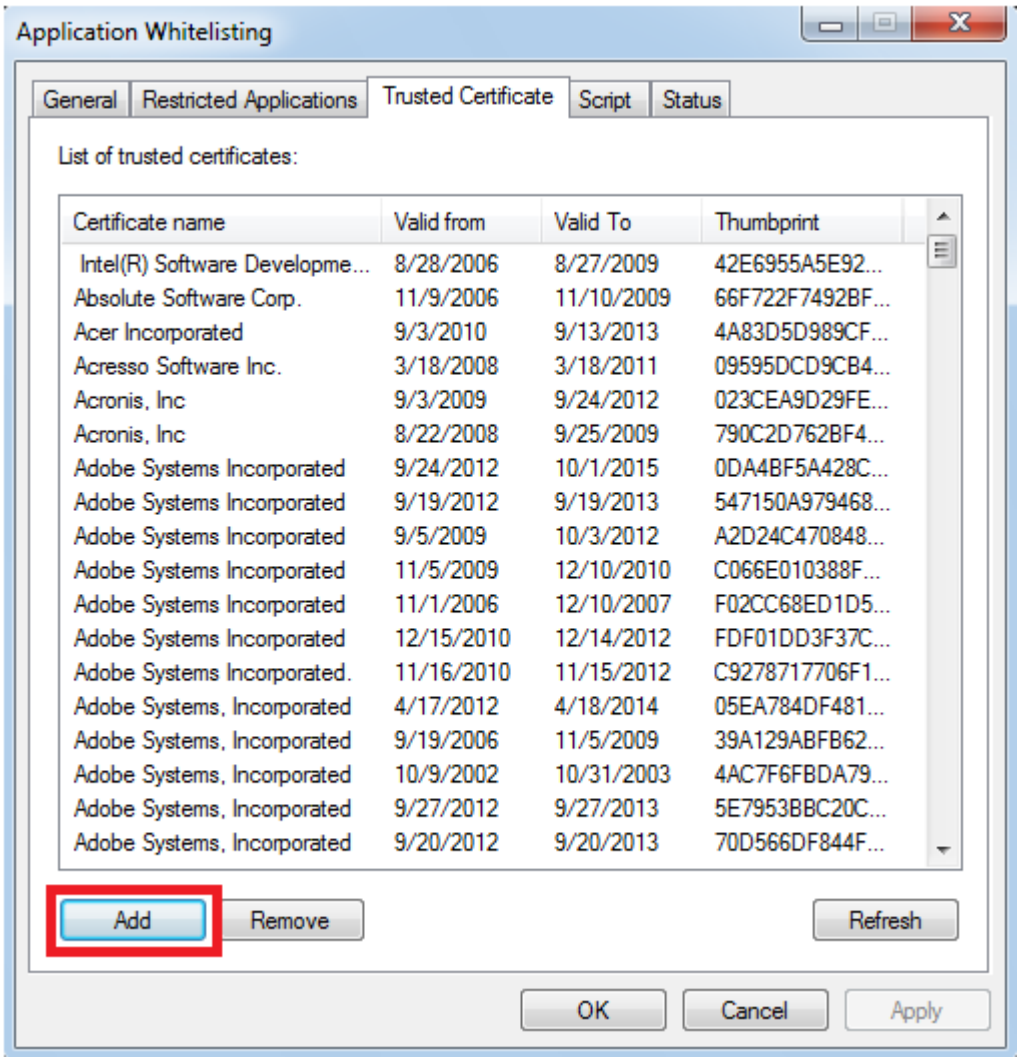
7.2.3 Trusted Certificate

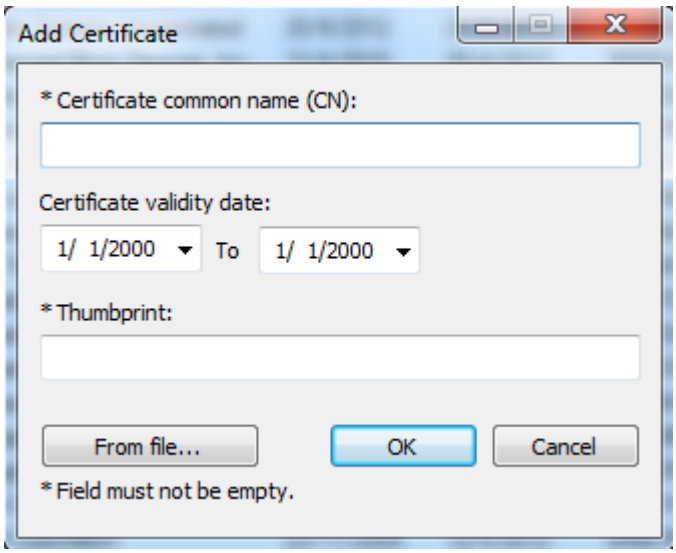
In the **Trusted Certificate** tab, users can choose to manage the list of trusted certificates which are being used by the applications. Applications which have their certificate listed under the trusted certificate list will be trusted.



To add Trusted Certificate, follow the steps below to add:

- Click on **Add** button.
- In **Add Certificate** window, click on **From file…** to select the executable. Click **OK**.

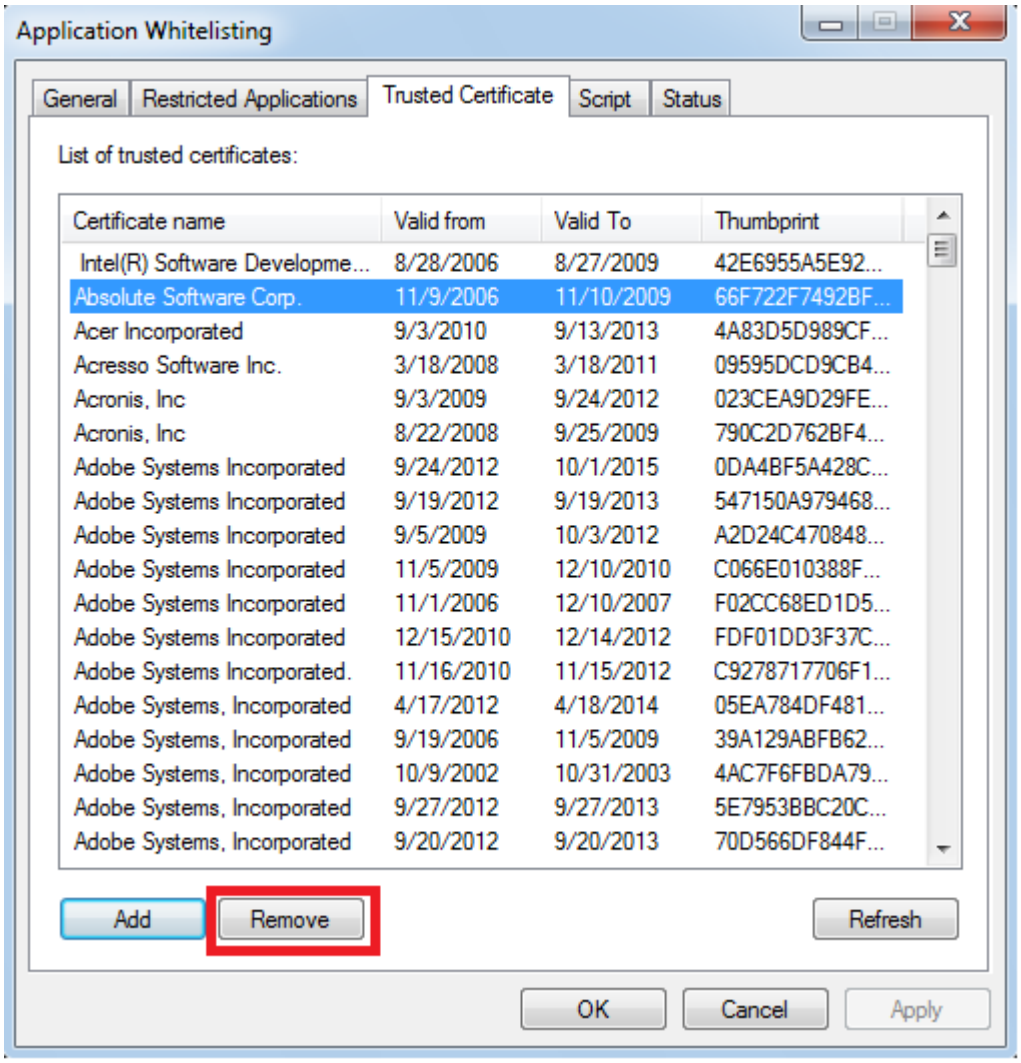




- The newly added trusted certificate will be added to the list. Then click on **Apply** button to apply the changes made.

To remove Trusted Certificate, follow the steps below to remove:

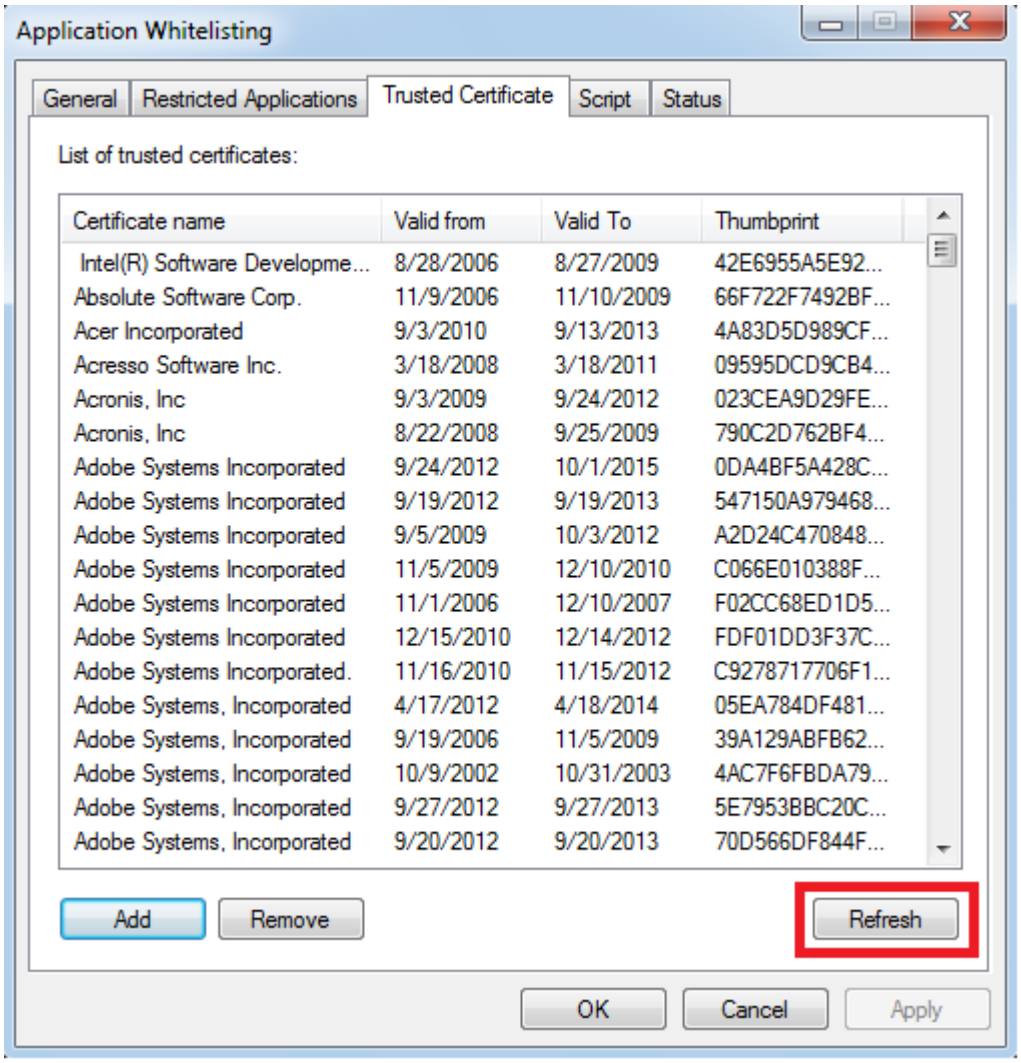
- Select a trusted certificate from the list and click on **Remove** button.



- The selected trusted certificate will be removed from the list. Then click on **Apply** button to apply the changes made.

To refresh the Trusted Certificate list, follow the steps below to refresh:

- Click on **Refresh** button.



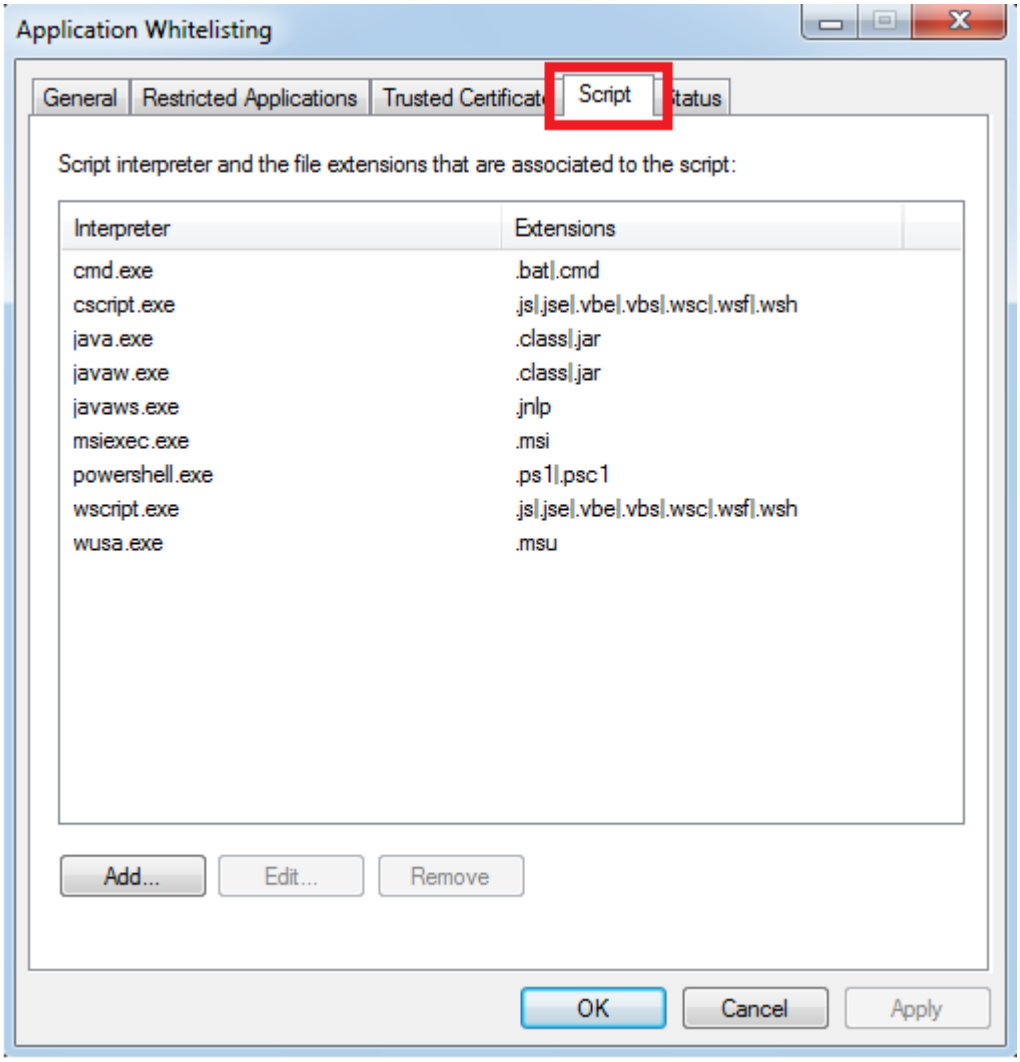
- The Trusted Certificate list will be refreshed and updated.

7.2.4 Script

In the **Script** tab, users can choose to associate script file extension types to script interpreter.

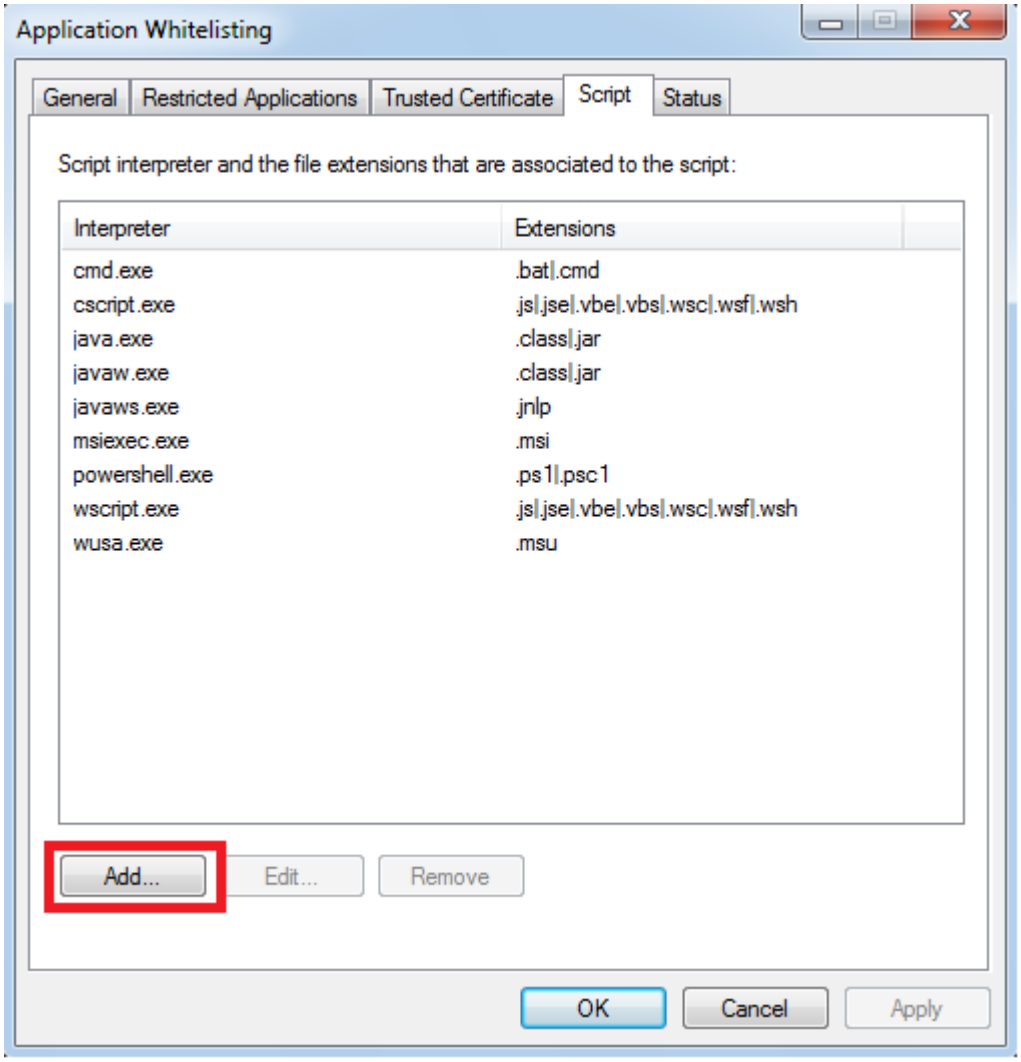
Note:

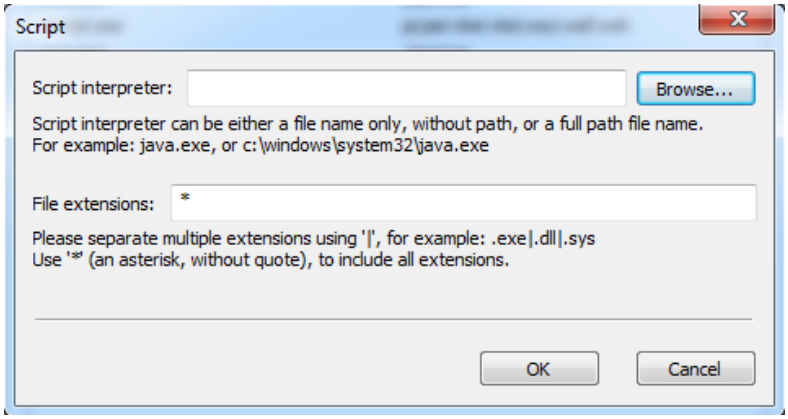
- In application whitelisting, executing a script requires both the script interpreter, which executes the script, and the script file itself to be trusted. The script interpreter will refuse to open any non-trusted file.
- If the script has higher trust level than the script interpreter, then the script interpreter trust level will be elevated to the same level as the trust level of the script file.
- If the script has lower trust level than the script interpreter, then the script interpreter will be running at its own trust level.



To add Script Interpreter, follow the steps below to add:

- Click on **Add** button.
- In **Script** window, beside **Script interpreter**, click on **Browse** to select the script interpreter executable.
- Beside **File extensions**, type in the script file extensions to be executed by the script interpreter selected above. For multiple script file extensions, type a pipe '|' to separate the two script file extensions. To include all types of script file extensions, type '*'.
- Click **OK**.

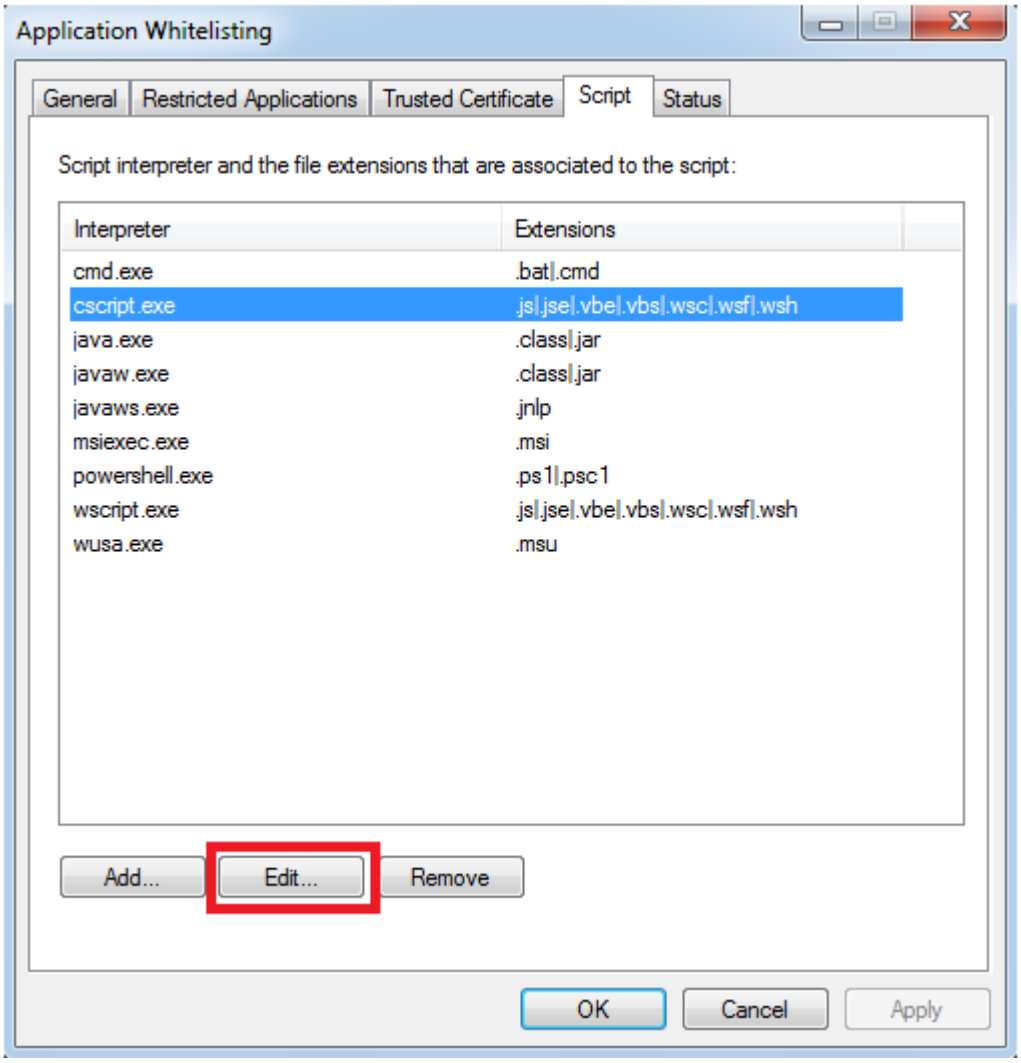


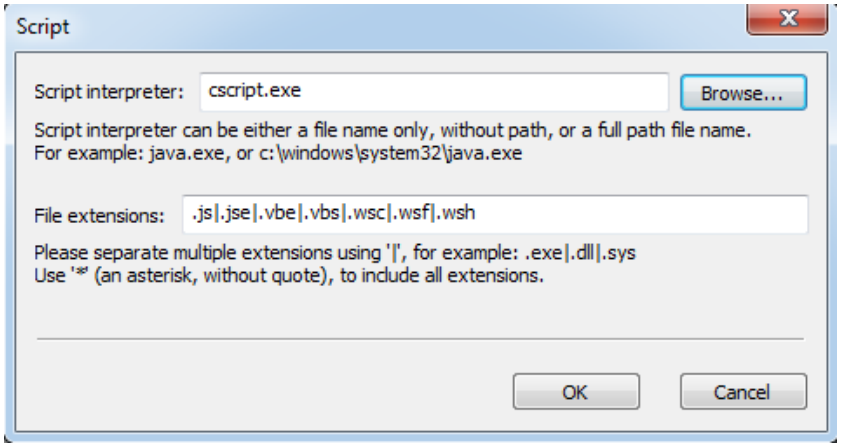


- The newly added script interpreter will be added to the list. Then click on **Apply** button to apply the changes made.

To edit Script Interpreter, follow the steps below to edit:

- Select a script interpreter from the list and click on **Edit** button.
- Make changes and click on **OK** button.

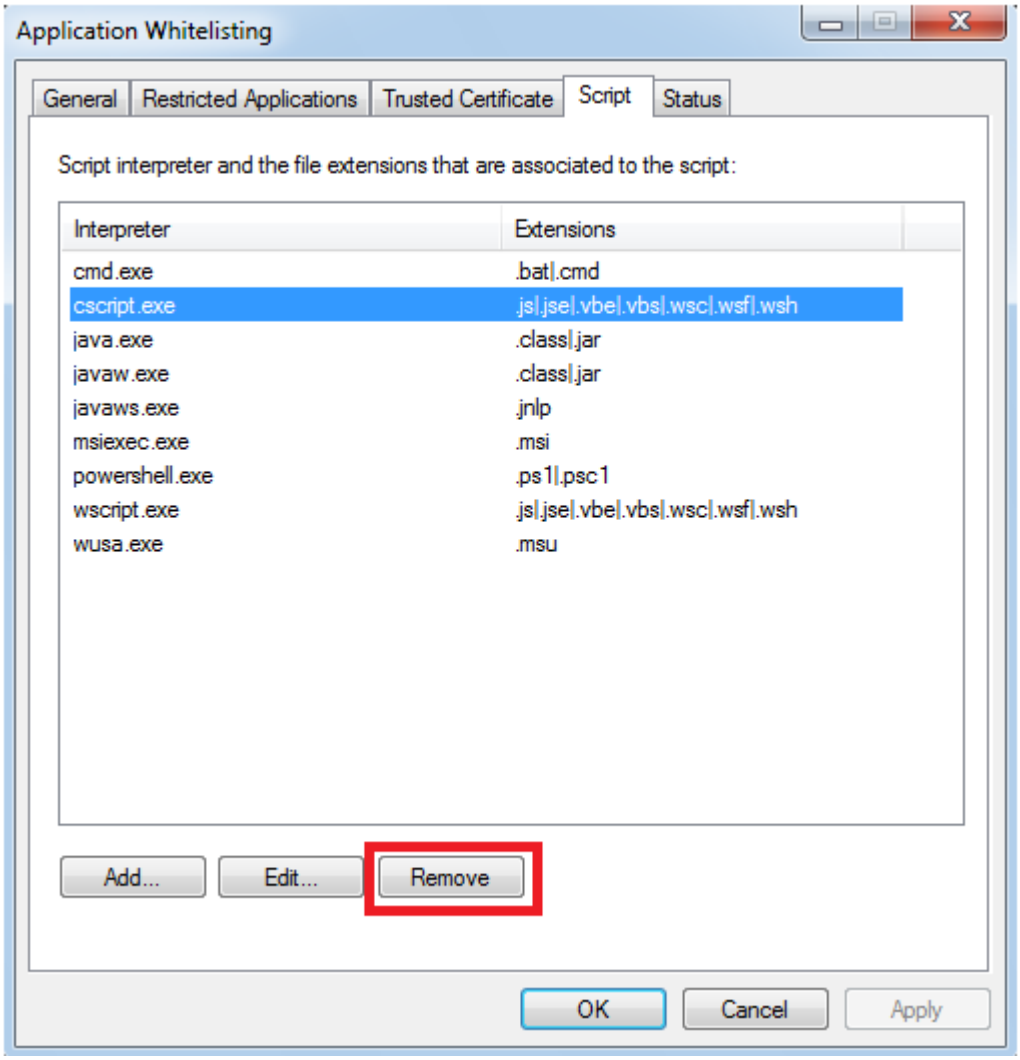




- The script interpreter will be edited. Then click on **Apply** button to apply the changes made.

To remove Script Interpreter, follow the steps below to remove:

- Select a script interpreter from the list and click on **Remove** button.



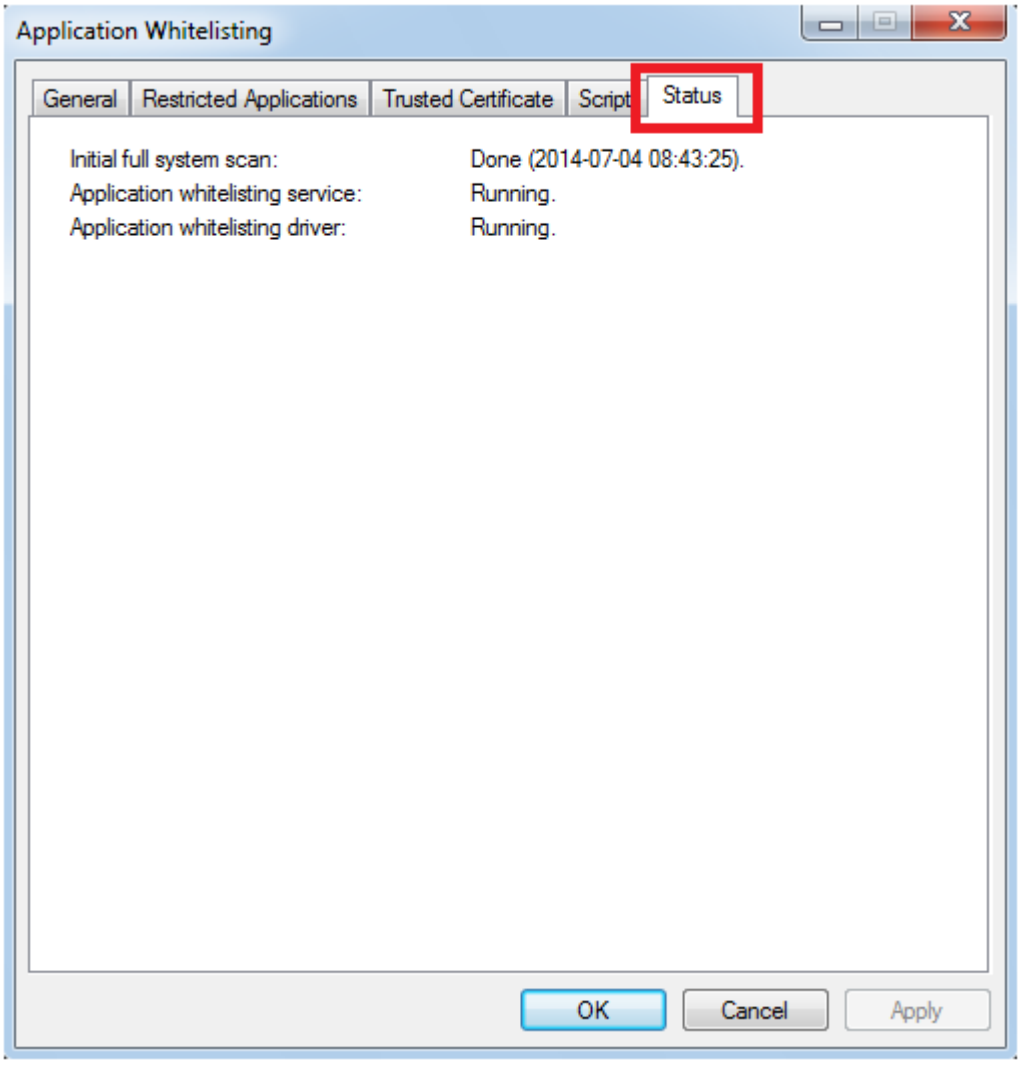
- The selected script interpreter will be removed from the list. Then click on **Apply** button to apply the changes made.

7.2.5 Status

The **Status** tab shows the status of the Application Whitelisting service, driver and also the date and time of the initial full system scan. The service and drive should be in **Running** state if Application Whitelisting works normally.

To view the status of the Application Whitelisting, follow the step below:

- Click on **Status** tab in the Application Whitelisting window.



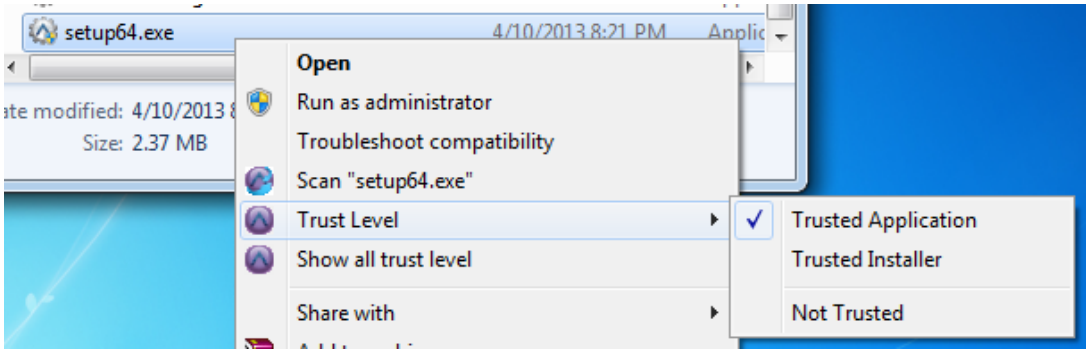
7.3 View Trust levels in Applications

To view the trust levels for the applications, follow the steps below:

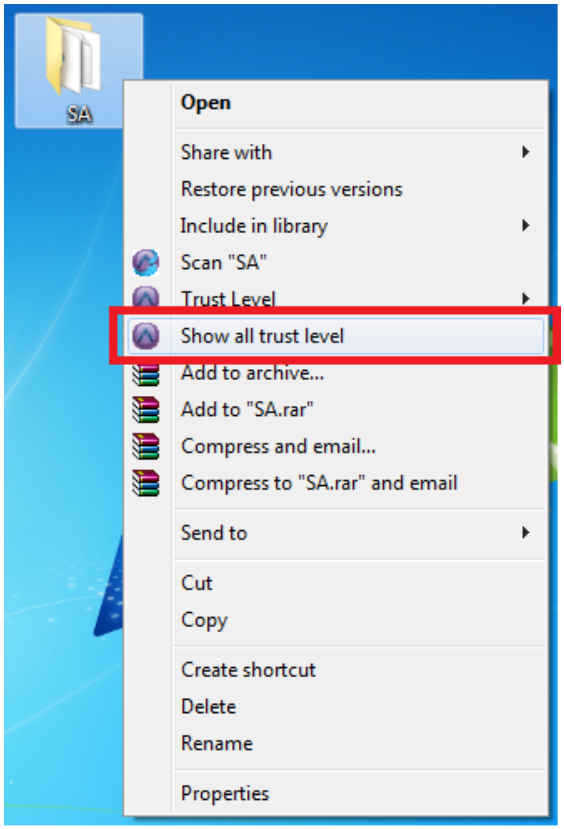
- **Right click** on the executable file, point to **Trust Level**. In the menu displayed, the tick will indicate the trust level the executable file.

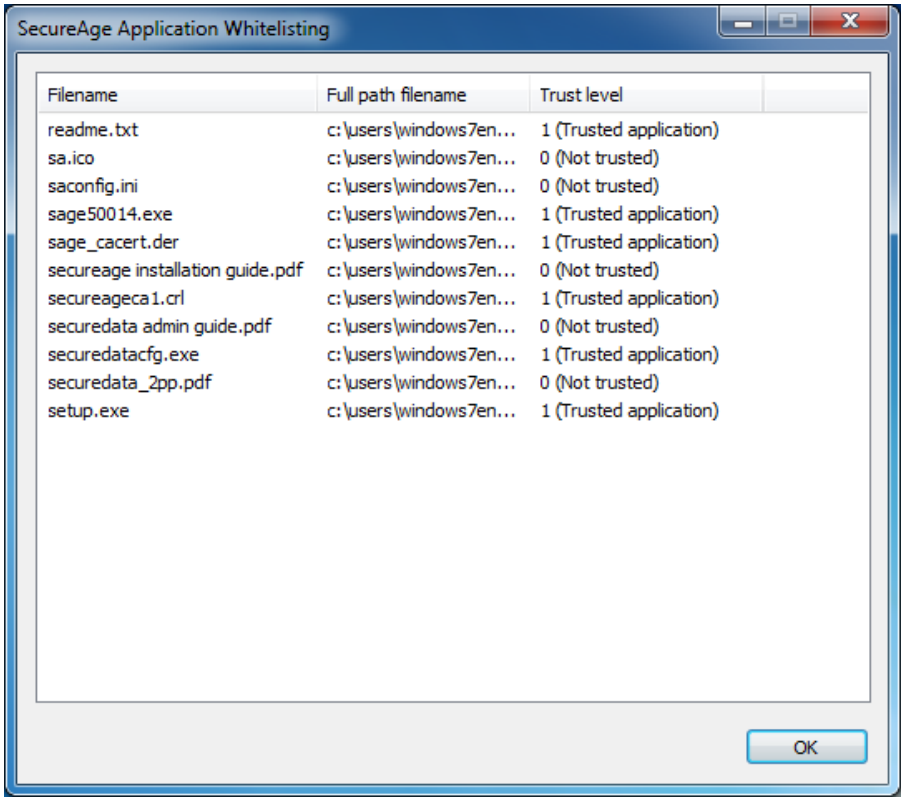
Note:

- The tick may not appear immediately for large files.



- Alternatively, right click on a folder directory and click on **Show all trust level**. A **SecureAge Application Whitelisting** window will appear, listing the trust levels of the files in the folder directory. Click **OK** to exit.





7.4 Behaviours of Application Whitelisting

Note:

- For installer packages that contains multiple executable files, it is recommended to put the package into a common folder and set the folder to be **Trusted Application**. For the main installer file to be executed directly, set it as **Trusted Installer** (Eg: setup.exe) and run.
- The prompting depends on the Application Whitelisting settings (Refer to **Section 7.2.1 – General Settings**), by default, it is trust by digital signature if file is not in the whitelist but the digital signature has to be listed under the trusted certificate list (Refer to **Section 7.2.3 –Trusted Certificate**). So if a new application has a digital signature that is not under the list, user will get prompted for further actions else user will not be prompted.

7.4.1 On-the-fly Trust

Scenario 1

If an untrusted executable file is being run and it is being launched by Windows Explorer, Application Whitelisting will notify for further actions as below:

- There will be no option for user to **Remember my answer through this entire process**.

Note:

- It does not give user the option to remember the answer because we do not want everything that is being run by Windows Explorer to be automatically trusted. This is to prevent any malware being run by Windows Explorer to be trusted and enters the system.
- But it gives user an option to set the untrusted file as a trusted installer instead if user is sure that the installer file is trusted and does not want to be further prompted by Application Whitelisting.

Scenario 2

For unsigned files which are not trusted and are being executed, Application Whitelisting will notify for further actions as below:

Example for Microsoft Office 2010 starter, as the volume is hidden and not accessible by Windows Explorer, user may not be able to see and manually set the trust level of the files. Application Whitelisting on-the-fly trust is able to allow user to set the appropriate actions for these files when it is being run.

- SecureAge Application Whitelisting will prompt user for further actions on the untrusted executable file from running when the user attempts to execute the file by double-clicking on it.
- Click on **Yes** button to allow Microsoft Office 2010 starter to proceed.

- As the Microsoft Office 2010 starter requires a lot of .dll files to run, Application Whitelisting will keep prompting user when these untrusted files are created and needs to be executed.

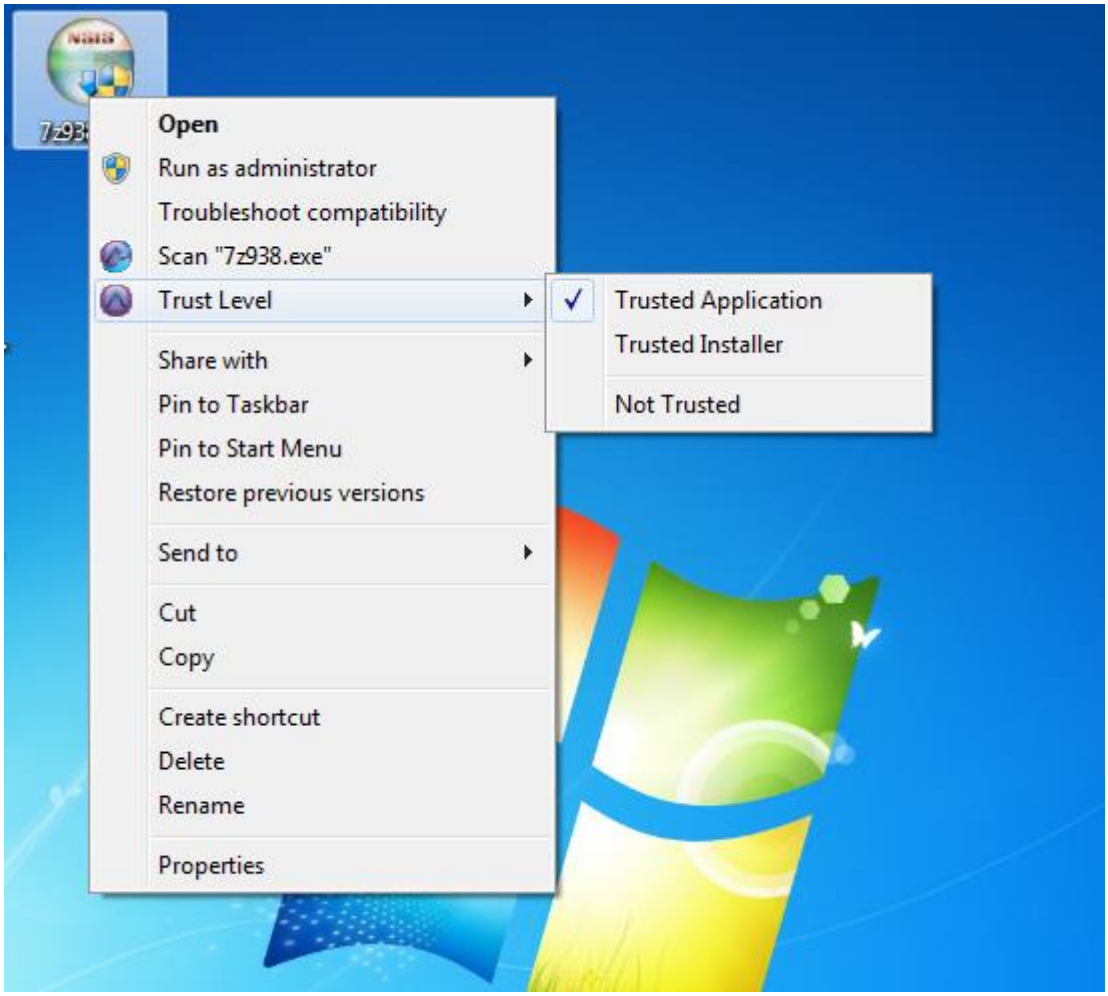
- To user whom does not want to be prompted again, check **Remember my answer for this entire process**.

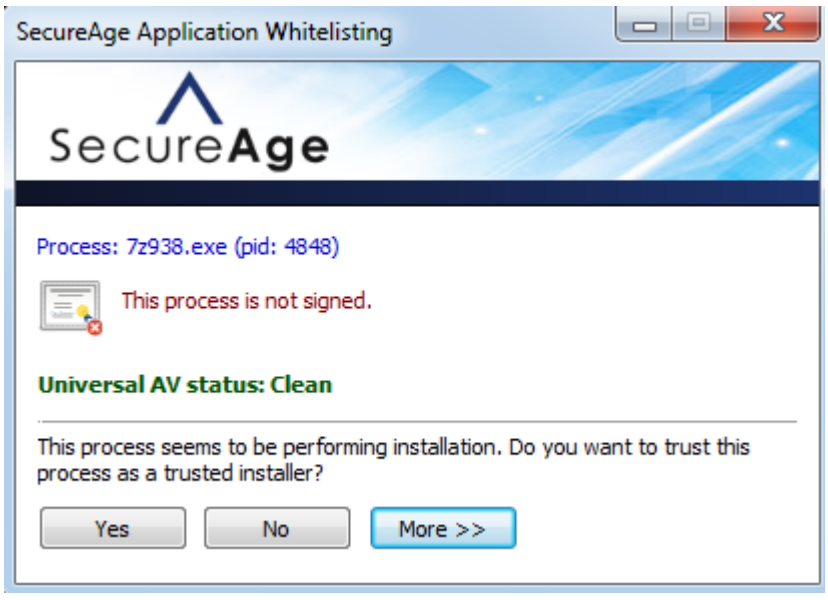
Note:

- If does not want user to be allow to have option to select and to be block straight away for untrusted files, turn SecureAPlus to Lockdown Mode (Refer to **Section 2.2.4** on how to switch to Lockdown Mode) **.**

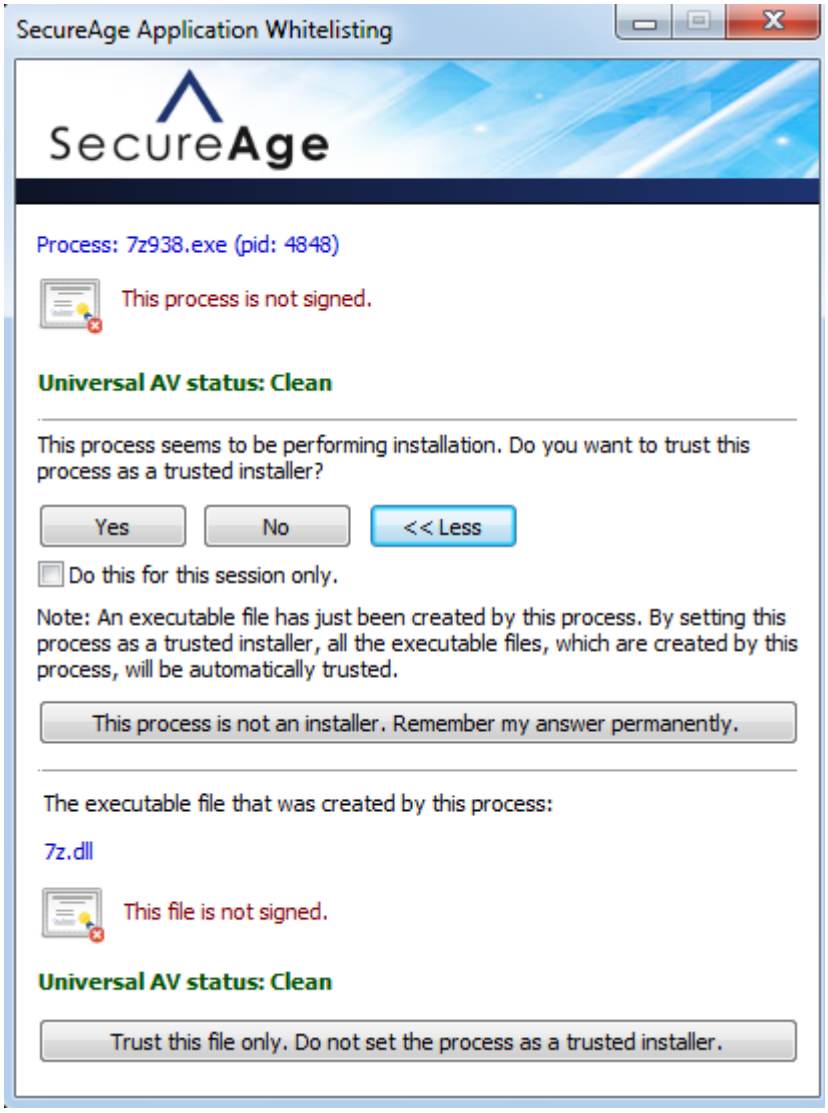
Scenario 3

For trusted applications which create new executable files during running, Application Whitelisting will notify for further actions as below:





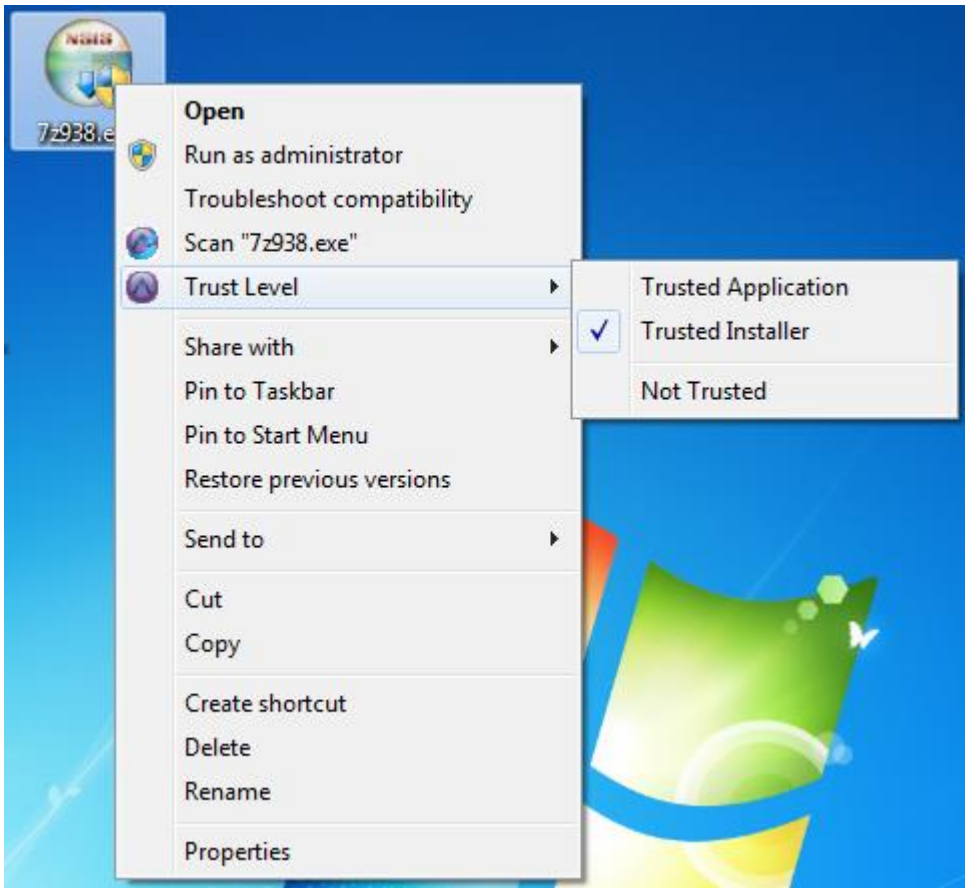
- Click on **More >>** to view more details of the executable.



- Check **Do this for this session only.** for the process to be temporarily treated as a trusted installer for that session only until the process terminated.
- To not get any further prompting and anything created by the trusted applications will be not trusted; click on **This process is not an installer. Remember my answer permanently.** This will place the application into the list of restricted applications (Refer to **Section 7.2 – Restricted Applications**). User can undo this action by removing the application from the list of restricted applications in the settings.
- Click on **Trust this file only. Do not set the process as a trusted installer.** to only allow the current newly created executable file be elevated to trusted application so that it can process. But the main trusted application will still remain as the same instead of elevating into a trusted installer. So user will get prompting again if it creates any other new executable files.

Note:

- For trusted installers, it will not prompt user for any further actions to elevate the newly created executable files by it as it will all be automatically set as trusted applications. Therefore, trusted installers can run smoothly as per normal without any unneeded prompting.



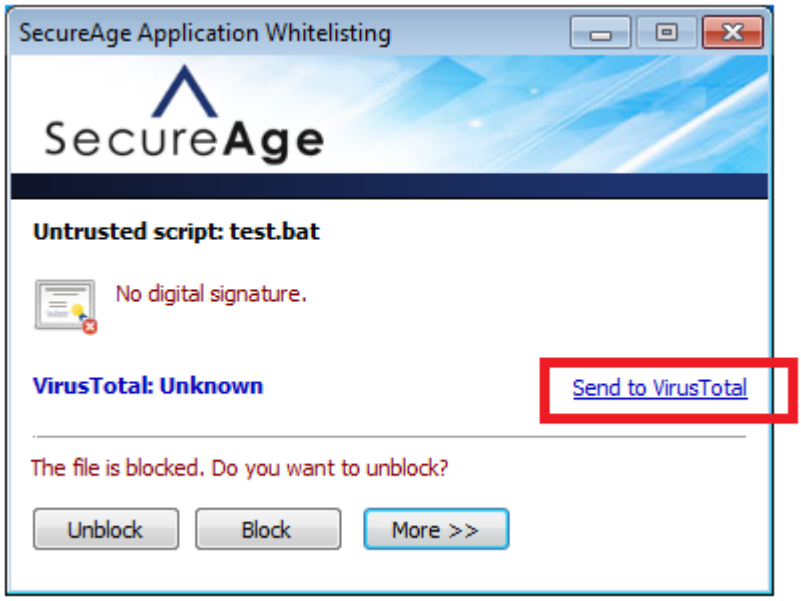
VirusTotal Scanning

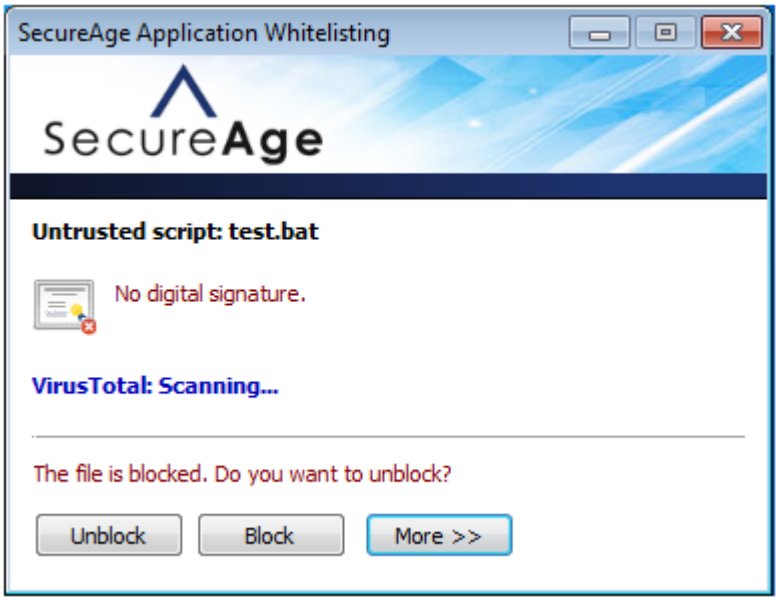
This is to help users in deciding whether to trust the new executable files or not when the hashes does not exist in the Universal AV by sending it to VirusTotal for scanning instead.

For files which are not trusted with no hashes exist in the Universal AV and are being executed, Application Whitelisting will notify for further actions as below:

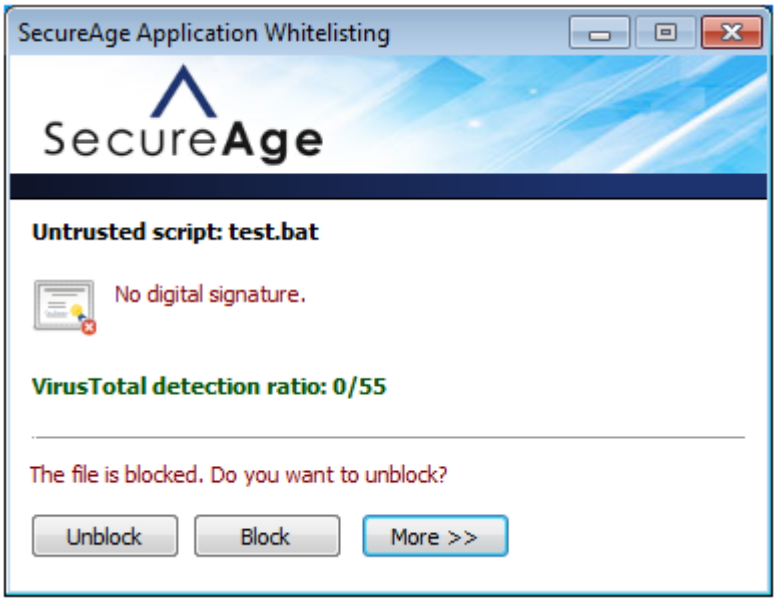
Note:

- The **Send to VirusTotal** link will not appear when the file exceeds 20MB.
- Click on the **Send to VirusTotal** link to send it to VirusTotal for scanning results.





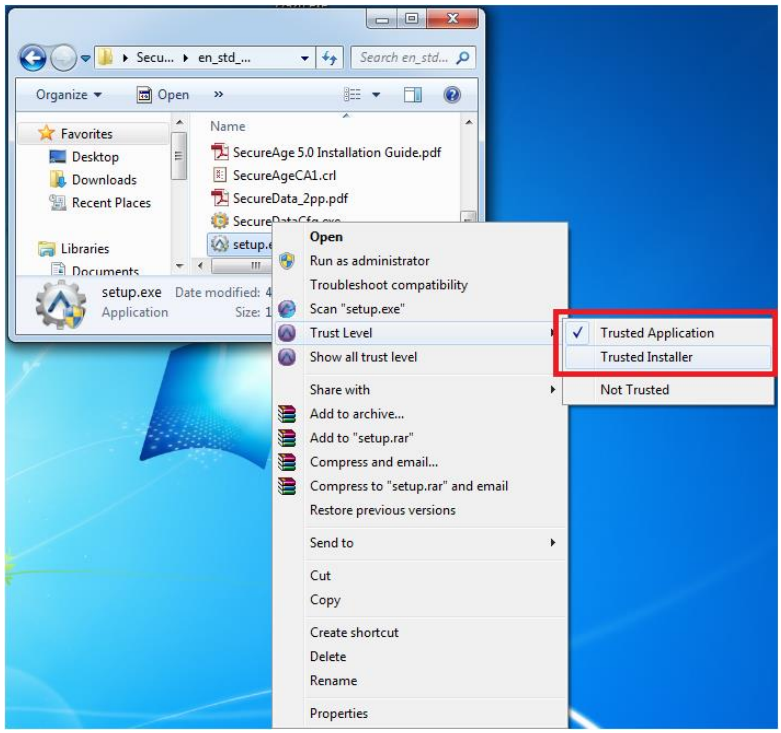
- It will show the virus detection ratio after completed scanning. User can then decide whether the file is trustable or not.



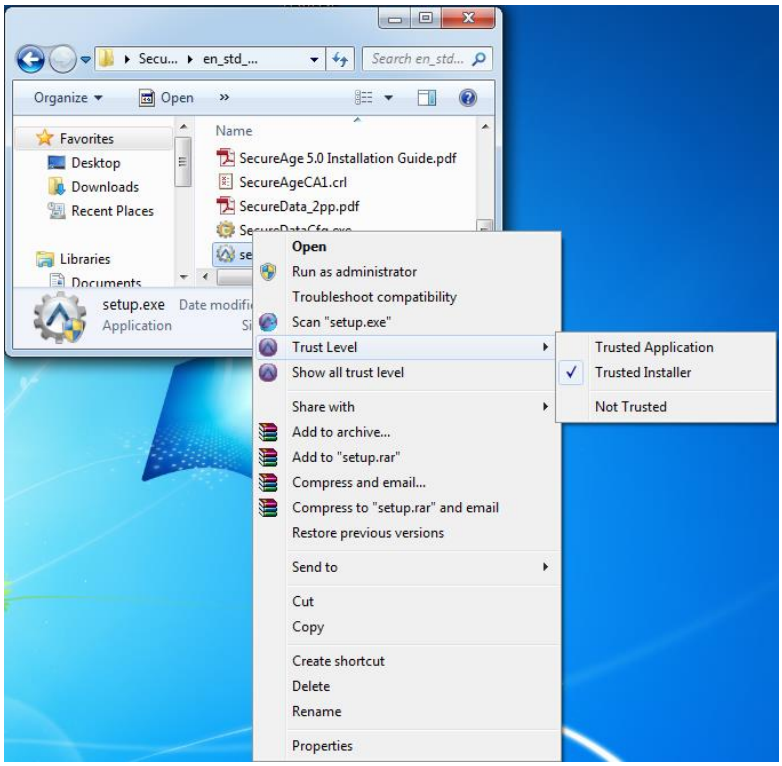
7.4.2 Manually Set Trust Level

To manually set trust levels for applications, follow the steps below:

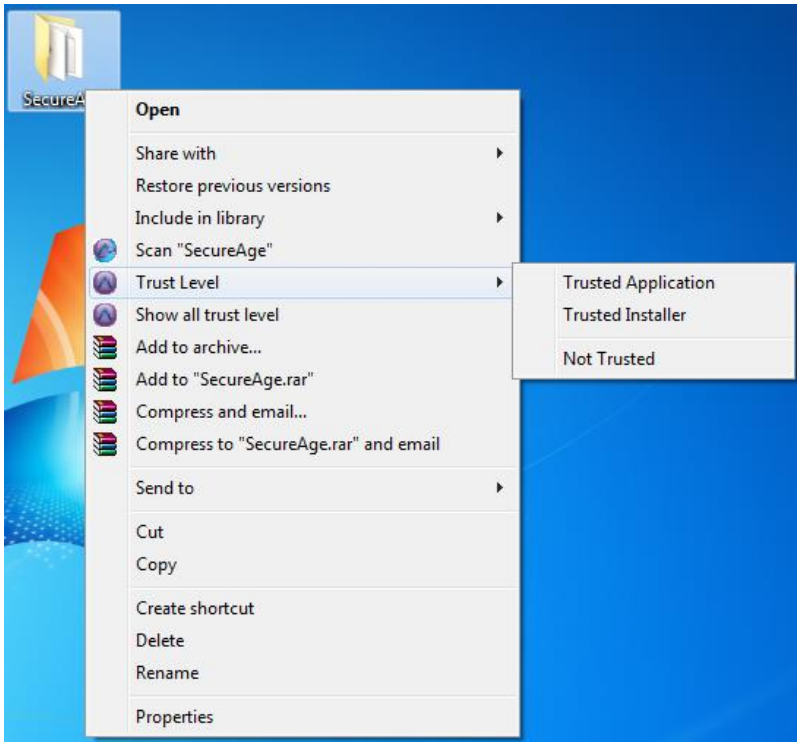
- Right click on the executable file, point to **Trust Level**. In the menu displayed, the tick will indicate the trust level the executable file. Select the desired trust level for the executable file.



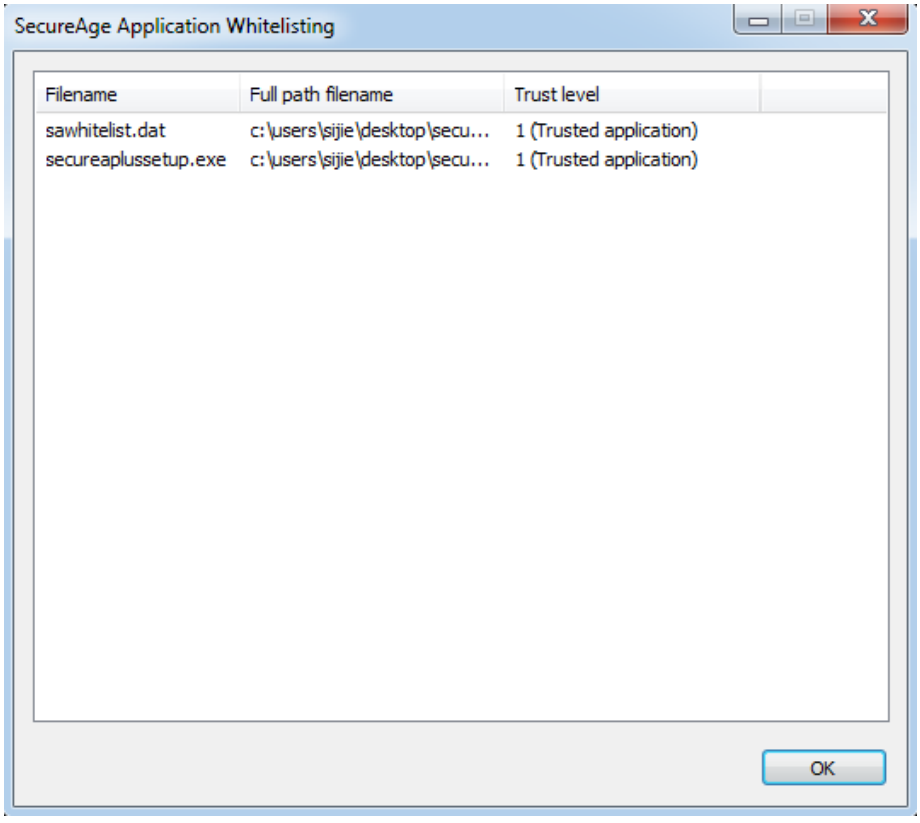
- Right click on the executable file again, point to **Trust Level**. In the menu displayed, the tick will indicate the new trust level the executable file.



- Alternatively, you can also set trust levels for the files within a folder. Right click on the executable file, point to **Trust Level**. In the menu displayed, select the desired trust level.



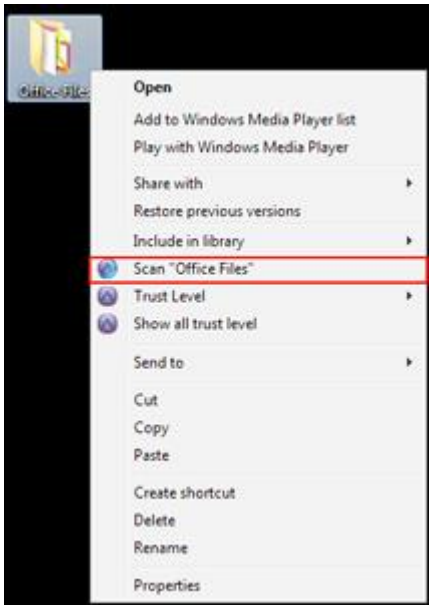
- Right click on the folder again, point to **Show all trust level**. A SecureAge Application Whitelisting window will show the new trust level of the files within the folder.



8 Manual Scan

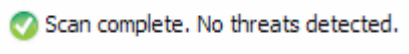
To do manual scanning on particular files or folders with Universal AV and Offline AV, follow the steps below:

- Right click the file/folder to scan and select Scan “[Insert Name of File/Folder]”.

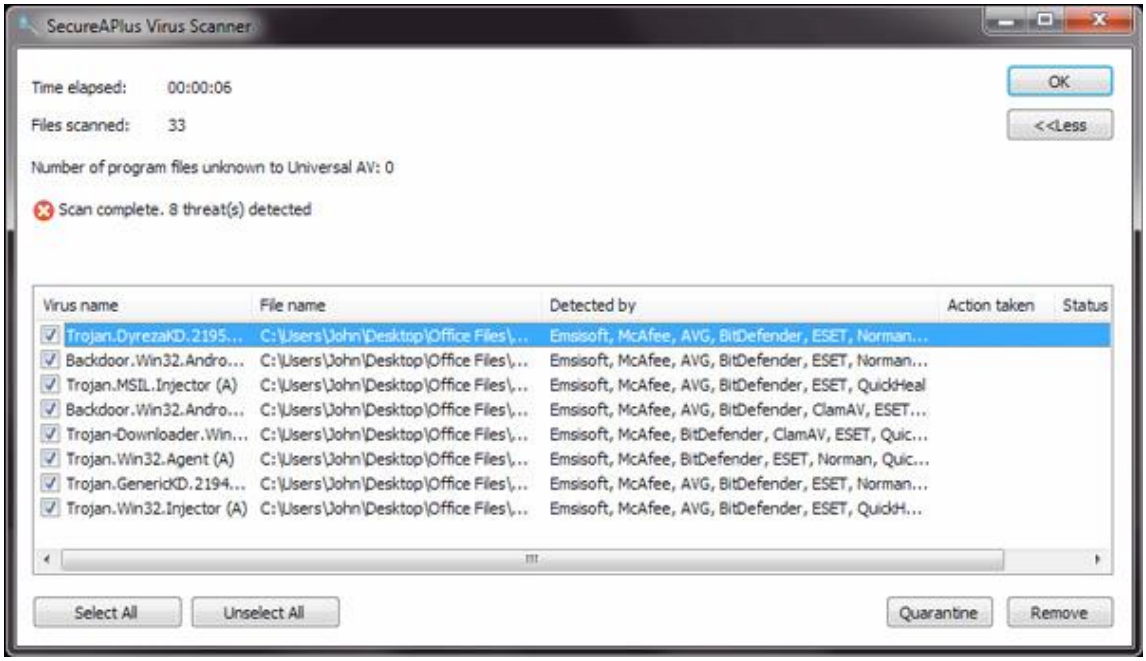


- The SecureAPlus Virus Scanner window will open and begin scanning.

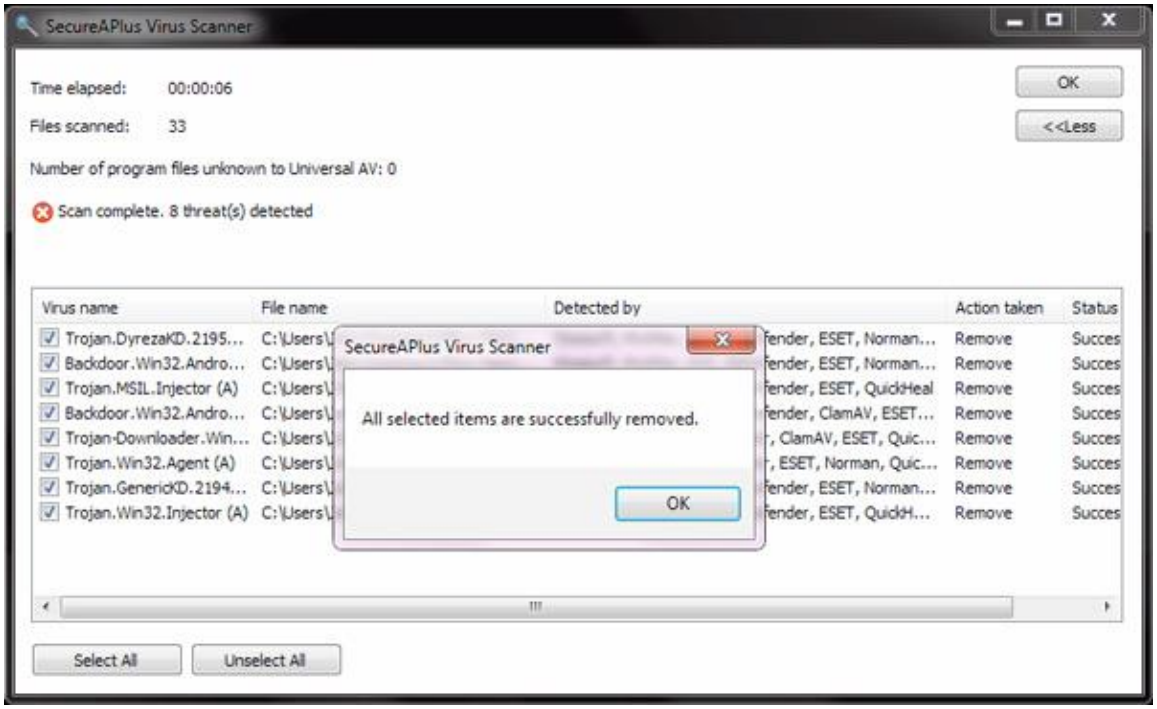
- If there is no viruses and malware detected, it will display as below:



- If threats are detected, the list of infected files will be shown along with information of which Universal AV’s engines had detected the files as threat.



- Choose Quarantine or Remove the infected files.



Note:

- SecureAPlus automatically scan the entire computer every hour with Universal AV and has real-time protection against new possible threats that are being saved in the PC's hard drive
- The time taken for scanning depends on the numbers of files and size of the files.
- Files and Folder scanning uses either or both of Universal AV and Offline AV to ensure the best detection rate.
- Files and Folder scanning may be unavailable on the following scenarios:
    - When both Universal AV and Offline AV is disabled. (Refer to **Section 4.31** on how to enable Antivirus settings)
    - If Offline AV was not installed and there is no internet connection.
    - If only Offline AV was disabled (Refer to **Section 4.31** on how to enable Antivirus settings) and there is no internet connection.

9 Contact Us

For more information, please feel free to contact us.

SecureAge Technology Pte Ltd

3, Fusionopolis Way

#05-21, Symbiosis

Singapore 138633

Tel: (65) 6873 3710

Fax: (65) 6234 4992

Email: contactus@secureage.com

URL: http://www.secureage.com

