

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

About	SecureAPlus	. 1		
Getting Started2				
2.1	Starting SecureAPlus Software	.2		
2.2	SecureAPlus Tray Icon Menu	.4		
	2.2.1 Normal Mode	.5		
	2.2.2 Silent Mode	.5		
	2.2.3 Interactive Mode	.6		
	2.2.4 Lockdown Mode	.7		
	2.2.5 Trust All for 5 minutes	.8		
	2.2.6 Trust All for 30 minutes	.9		
	2.2.7 Trust All until computer is restarted	10		
	2.2.8 Settings	11		
Secur	eAPlus Main Console	13		
3.1	SecureAPlus Store	13		
3.2	SecureAPlus Account	14		
3.3	Lockcube (Secure Cloud Storage)	15		
3.4	About	16		
3.5	SecureAPlus Premium Trial	17		
3.6	SecureAPlus License	18		
3.7	Main Summary	21		
3.8	Application Whitelisting Modes	23		
3.9	SecureAPlus Settings	28		
3.10	SecureAPlus Complete Scan	30		
3.11	SecureAPlus Quarantine & History	31		
3.12	SecureAPlus Software Update	33		
3.13	License Extension	35		
3.14	Help	36		
Secur	eAPlus Settings	37		
4.1	Universal AV	39		
	4.1.1 Daily Upload Limit	40		
	4.1.2 Message Popup ("Good News" Message Prompt)	41		
	4.1.3 UAV Engines Exclusions	42		
4.2	Application Whitelisting	43		
	4.2.1 Application Whitelisting Standard Mode	44		
	4.2.2 Application Whitelisting Advanced Mode	45		
4.3	Scan Settings	49		
	4.3.1 Antivirus	50		
	4.3.2 Files/Folders Exclusions	61		
	4.3.3 Included File Types	64		
	About Gettin 2.1 2.2 Secur 3.1 3.2 3.3 3.4 3.5 3.6 3.7 3.8 3.9 3.10 3.11 3.12 3.13 3.14 Secur 4.1 4.2 4.3	About SecureAPlus Getting Started 2.1 Starting SecureAPlus Software 2.2 SecureAPlus Tray Icon Menu 2.2.1 Normal Mode 2.2.2 Silent Mode 2.2.3 Interactive Mode 2.2.4 Lockdown Mode 2.2.5 Trust All for 5 minutes 2.2.6 Trust All for 30 minutes 2.2.7 Trust All for 30 minutes 2.2.8 Settings SecureAPlus Main Console - 3.1 SecureAPlus Store 3.2 SecureAPlus Account 3.3 Lockcube (Secure Cloud Storage) 3.4 About 3.5 SecureAPlus Premium Trial 3.6 SecureAPlus Settings 3.7 Main Summary 3.8 Application Whitelisting Modes 3.9 SecureAPlus Gomplete Scan 3.11 SecureAPlus Software Update 3.12 SecureAPlus Software Update 3.13 License Extension 3.14 Help SecureAPlus Settings - 4.1 Universal AV		

	4.4	Update	67	
		4.4.1 Software	67	
		4.4.2 Virus Signature	74	
	4.5	Manage User Rights	78	
		4.5.1 Manage Groups/Users in Windows	78	
5	Unive	rsal AV		
	5.1	94		
	5.2	Complete Scan	97	
	5.3	Retrieve Last Scan	99	
	5.4	View Universal AV's Log	100	
	5.5	Delete Universal AV's Log	101	
6	Quara	Intine & History	102	
	6.1	Quarantine List		
	6.2	History List		
	6.3	Ignored List	109	
7	applic	cation Whitelisting		
	7.1	Definitions of Trust Levels		
	7.2	Application Whitelisting Advanced Settings		
		7.2.1 General Settings		
		7.2.2 Restricted Applications	120	
		7.2.3 Trusted Certificate	124	
		7.2.4 Script	128	
		7.2.5 Status	132	
	7.3	View Trust levels in Applications	133	
	7.4	Behaviours of Application Whitelisting	135	
		7.4.1 On-the-fly Trust	135	
		7.4.2 Manually Set Trust Level	144	
8	Manua	al Scan	146	
9	Conta	ct Us		

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.



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.

۵	0	Ð	())	4:58 PM	

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

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

6	Open SecureAPlus		
	Application Whitelisting		
\checkmark	Normal Mode		
	Silent Mode		
0	Help		
0	About		

 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.

SecureAPlus v3.4.1.2			_ ×
		Interactive Mod You will be prompted w and run a program that the trusted list.	e /hether to trust is not found in Change Mode ►
 ✓ Security Features: Running ✓ Software Update: Up-to-date Last Complete Scan: Never 	X Settings	Complete Scan	Quarantine & History
More details 🕨	Update	License Extension	PHelp
Premium Trial			Enter license code
🛒 Store 👃 Account 🔒 LockCube 🔨 About		Copyright © SecureAge Tech	nology. All rights reserved.

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.

۲	Open SecureAPlus
	Application Whitelisting
✓	Normal Mode
	Silent Mode
0	Help
6	About
-	🛀 🔯 🖃 🦏 arrive 🔚

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

۲	Open SecureAPlus
	Application whitelisting
\checkmark	Normal Mode
	Silent Mode
0	Help
6	About
-	

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

SecureAPlus	s Status	_ ×
Complete Scan Complete Scan About Complete Scan License	General Information License: Expires Sat, Aug 06 2016 17:00. SecureAPlus ID: pqreRCFD-24946 SecureAPlus v3.4.1 Virus signature version: 20845, Fri Aug 28 08:38:43 2015 Website: http://www.secureaplus.com Support: secureaplus@secureage.com Forum: https://secureaplusforum.secureage.com/	2
🛒 Store 💧 Account	Copyright © SecureAge Technology. All rig	hts reserved.

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.

0	Open SecureAPlus Application Whitelisting			
<	Normal Mode			
	Silent Mode			
0	Help			
6	About			
- 👽 🔝 🖬 🦇				

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**.

0	Open SecureAPlus Application Whitelisting			
	Normal Mode			
\checkmark	Silent Mode			
0 ©	Help About			



- 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.

~	Interactive Mode		
	Lockdown Mode Trust All for 5 minutes		
	Trust All for 30 minutes Trust All until computer is restarted	0	Onen Segura A Plus
	Settings		Application Whitelisting
-		v	Normal Mode Silent Mode
		0 Ø	Help About

 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 <u>3.8</u> – 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.

	Interactive Mode		
√	Lockdown Mode		
	Trust All for 5 minutes Trust All for 30 minutes Trust All until computer is restarted	6	Open SecureAPlus
	Settings		Application Whitelisting
		 Image: A start of the start of	Normal Mode Silent Mode
		0 Ø	Help About

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

	0	-	4.5			
^			())	5:14	I PM	
~						

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 <u>3.8</u> – 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.

			0	Open SecureAPlus	
		Interactive Mode		Application Whitelisting	
		Lockdown Mode		Normal Mode	
1	\checkmark	Trust All for 5 minutes	Ľ	Silent Mode	
		Trust All for 30 minutes			
		Trust All until computer is restarted	0	Help	
		Settings	0	About 스 🔨 님 (마) - 5:10 Pivi	

 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.

Trus	st all	(3 m	in 11	sec remaining	g)
^	<u>^</u>	口	())	5:17 PM	

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 <u>3.8</u> – 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.

		0	Open SecureAPlus
	Interactive Mode		Application Whitelisting
	Lockdown Mode		Normal Mode
	Trust All for 5 minutes	P	Silent Mode
\checkmark	Trust All for 30 minutes		Shent mode
	Trust All until computer is restarted	0	Help
	Settings	0	About

 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.

Trust	all (2	28 m	in 31	sec ren	naining	g)
^	<u>^</u>	Ð	())	5:20	PM	

Solution 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 <u>3.8</u> – 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.

^	<u>^</u> t	())	5:16 PM	ſ

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



Solution 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 <u>3.8</u> – 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.

 Interactive Mode Lockdown Mode Trust All for 5 minutes Trust All for 30 minutes 		
Trust All until computer is restarted	6	Open SecureAPlus
Settings		Application Whitelisting
	 Image: A start of the start of	Normal Mode Silent Mode
	0	Help About

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

😯 User Account	Control	×			
Do you want to allow the following program to make changes to this computer?					
	Program name: A Verified publisher: S File origin: H	pplication Whitelisting Settings ecureAge Technology Pte Ltd lard drive on this computer			
Show detai	ls	Yes No			
		Change when these notifications appear			

Applicatio	n Whitelisting		- • •
General	Restricted Applications Trusted Certifi	cate Script Status	
	Export whitelist to a file	Import whitelist from a	a file
	Compact Whitelist Database	View log	
		OK Cancel	Apply

• The Application Whitelisting window will launch.

• Refer to **Section <u>7.2</u>** 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.

SecureAPlus v	/3.4.1.1			_ ×
			Interactive Mod You will be prompted w and run a program that the trusted list.	e vhether to trust is not found in Change Mode ►
 ✓ Security Features: ✓ Software Update: Last Complete Scale 	tected Running Up-to-date n: 2015/08/28	X Settings	Complete Scan	Quarantine & History
Premium Trial	More details >	Update	Copyright © SecureAge Tech	Help Enter license code
∫ ● LosCube - Fait Secure (x) ← ⇒ C	ng @ SecureAge Manage @ SecureAge - Infolton Lock Cube		ity Ac. 🗋 Installing and config 🗋 Riving The Horri If Service 🜒 Help 🐧 Contact Us	E -
	Wel So Backup and share any fi	Icome to LockCube ecure cloud storage. Iles, anytime, anywhere, with	any devices.	
	Limai Password Forgot your pass			
	Powered by Copyright © 20	015 SecureAge Technology, All Rights Reserved.		

► Visit <u>http://www.secureage.com/prd_SecureCloudStorage.jsp</u> 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** <u>2.1</u> for the steps to start SecureAPlus.
- In the SecureAPlus window, click on the **^About** icon on the bottom left of the window.

SecureAPlus v3.4.1.1			_ × _
		Interactive Mod You will be prompted w and run a program that the trusted list.	e rhether to trust is not found in Change Mode ►
 ✓ Security Features: Running ✓ Software Update: Up-to-date Last Complete Scan: 2015/08/28 	X Settings	Complete Scan	Quarantine & History
More details >	Update	License Extension	P Help
Premium Trial			Enter license code
🛒 Store 💄 Account 🔒 LockCube 📐 About		Copyright © SecureAge Tech	nology. All rights reserved.

• The General Information will be displayed as shown below.

SecureAPlus	Status	_ ×
Complete Scan Complete Scan About Complete Scan License	General Information License: Expires Thu, Aug 11 2016 09:31. SecureAPlus ID: VsjOjabe-46569 SecureAPlus v3.4.1.1 Virus signature version: 20836, Wed Aug 26 04:51:25 2015 Website: http://www.secureaplus.com Support: secureaplus@secureage.com Forum: https://secureaplusforum.secureage.com/	
🛒 Store 💄 Account	About About Copyright © SecureAge Technology. All r	ights reserved.

 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.

SecureAPlus v3.4.1.1			_ ×
		nteractive Mod You will be prompted w and run a program that he trusted list.	e rhether to trust is not found in Change Mode ►
 ✓ Security Features: Running ✓ Software Update: Up-to-date Last Complete Scan: 2015/08/28 More details ► 	Settings	Complete Scan	Quarantine & History
Premium Trial		C EXtension	Enter license code
SecureAPlus Account x C SecureAPlus Account of mttps://secureaplus.secureage.com/sapportal/site/register.sa SecureAPlus SecureAPlus SecureAPlus Premium requires an Account to utilize its added features. You are currently not logged in. Please login or create a new account to or	m Trial	Se 6569 to an account.	د الم
Image: Create Account with Facebook Image: Create Account with Facebook Image: Create Account with Google+ Image: Creat	Log In f Log In with 8 Log In with Already have a Sec Email Address	Facebook Google+ or cureAPlus Account?	
Last Name Email Address Retype Email Address	Password Log In	F	Forgot Password

3.6 SecureAPlus License

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

		Interactive Mod You will be prompted w and run a program that i the trusted list.	e hether to trust is not found in Change Mode ►
 ✓ Security Features: Running ✓ Software Update: Up-to-date Last Complete Scan: 2015/08/28 	Settings	Complete Scan	Quarantine & History
More details >	Update	License Extension	P Help

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

SecureAPlu	s Status .	_ ×
	Enter License Code	0
Complete Scan	License: Expires Thu, Aug 11 2016 09:31.	
🚱 About	License Code	
hicense)000000-300000-300000-300000-30	
	Apply Cancel	
	After you have purchased the user license, the license code will be emailed you. Simply copy the license code from the email and paste it on the abo License Code input box. Then click on the Apply button to activate the license	to ive e.
🛒 Store 👃 Account	LockCube About Home Copyright © SecureAge Technology. All rights re	eserved.

- 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.



🛒 Store 👃 Account 🔒 LockCube 🔥 About Copyright © SecureAge Technology. All rights reserved.



3.7 Main Summary

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

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

SecureAPlus v3.4.1.1			_ ×
		nteractive Mod You will be prompted w and run a program that he trusted list.	e vhether to trust is not found in Change Mode ►
 ✓ Security Features: Running ✓ Software Update: Up-to-date Last Complete Scan: 2015/08/28 	Settings	Complete Scan	Quarantine & History
More details >	Update	License Extension	P Help
Premium Trial			Enter license code
🛒 Store 👃 Account 🔒 LockCube 🔥 About		Copyright © SecureAge Tech	nology. All rights reserved.

• Click on More details to view more details of the status.

SecureAPlus v3.4.1.1			_ ×
		nteractive Mod You will be prompted w and run a program that he trusted list.	e rhether to trust is not found in Change Mode ►
 ✓ Security Features: Running ✓ Software Update: Up-to-date Last Complete Scan: 2015/08/28 	X Settings	Complete Scan	Quarantine & History
More details >	Update	License Extension	P Help
<u>Premium Trial</u>			Enter license code
🛒 Store 💄 Account 🔒 LockCube 🔥 About		Copyright © SecureAge Tech	nology. All rights reserved.

 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 <u>2.1</u> for the steps to start SecureAPlus.
- In the SecureAPlus window, the current mode is indicated on the top.

SecureAPlus v3.4.1.1			_ × _
		Interactive Mod You will be prompted w and run a program that the trusted list.	e vhether to trust is not found in Change Mode ►
 ✓ Security Features: Running ✓ Software Update: Up-to-date Last Complete Scan: 2015/08/28 	Settings	Complete Scan	Quarantine & History
More details >	Update	License Extension	P Help
<u>Premium Trial</u>			Enter license code
🛒 Store 👃 Account 🔒 LockCube 🔨 About Copyright © SecureAge Technology. All rights reserved.			

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

- Start SecureAPlus. Please refer to Section <u>2.1</u> 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).

SecureAPlus v3.4.1.1			_ × _
		Interactive Mod You will be prompted w and run a program that the trusted list.	e rhether to trust is not found in Change Mode ►
 ✓ Security Features: Running ✓ Software Update: Up-to-date Last Complete Scan: 2015/08/28 	Settings	Complete Scan	Quarantine & History
More details 🕨	Update	License Extension	P Help
Premium Trial			Enter license code
🛒 Store 💄 Account 🔒 LockCube 🔥 About		Copyright © SecureAge Tech	nology. All rights reserved.

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

🚱 User Account Control			
Do you want to allow the following program to make changes to this computer?			
Program name: SecureAPlus Verified publisher: SecureAge Technology Pte Ltd File origin: Hard drive on this computer			
Show details			
Change when these notifications appear			

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

SecureAPlus	Settings			×
_	Standard Mode	Advanced Mode		0
Universal AV	Standard App	lication Whitelisting	Mode Advanced Settings	
Application Whitelisting	✓ Interactive You will be promp	e Mode ted whether to trust and	I run a program not in the trusted list.	
Scan Settings	Lockdown All untrusted prog	Mode grams will be automatica	al y blocked from running on your comput	er.
Update	All trusted and un	trusted programs are al	lewed to run temporarily. Apply Cance	el 👘
Manage User Rights	- O Tips Choose "Lo allow to rur on your PC a	ckdown Mode' if you n. But please remembe as a trusted installer be	cannot decide which program to trust r to set any new program you wish to in fore installation.	and stall
🛒 Store Account	Abc	out 🏠 Home	Copyright © SecureAge Technology. All rights	reserved.

- 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

SecureAPlus v3.4.1.1			_ ×
		Lockdown Mode Any program that is not list will be automaticall running on your PC.	e in the trusted y blocked from Change Mode ►
 ✓ Security Features: Running ✓ Software Update: Up-to-date Last Complete Scan: 2015/08/28 	X Settings	Complete Scan	Quarantine & History
More details 🕨	Update		P Help
Premium Trial			Enter license code
🛒 Store 👃 Account 🔒 LockCube 🔥 About		Copyright © SecureAge Tech	nology. All rights reserved.

Trust All for 5 minutes



Trust All for 30 minutes

SecureAPlus v3.4.1.1			_ ×
		Trust All for 30 All programs, including not in the trusted list, a run for 30 minutes.	minutes those that are are allowed to Change Mode ►
At Risk X Security Features: Not Running ✓ Software Update: Up-to-date Last Complete Scan: 2015/08/28	Settings	Complete Scan	Quarantine & History
More details >	Update	License Extension	P Help
Premium Trial			Enter license code
🛒 Store 👃 Account 🔒 LockCube 🔨 About		Copyright © SecureAge Tech	nology. All rights reserved.

Trust All until computer is restarted



3.9 SecureAPlus Settings

SecureAPlus v3.4.1.1			_ ×
		Interactive Mod You will be prompted w and run a program that the trusted list.	e vhether to trust is not found in Change Mode ►
 ✓ Security Features: Running ✓ Software Update: Up-to-date Last Complete Scan: 2015/08/28 	Settings	Complete Scan	Quarantine & History
More details 🕨	Update	License Extension	? Help
Premium Trial			Enter license code
🛒 Store 💄 Account 🔒 LockCube 🔥 About		Copyright © SecureAge Tech	nology. All rights reserved.

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

😯 User Account Con	trol		×
Do you want to allow the following program to make changes to this computer?			
Ver File	ogram name: S rified publisher: S a origin: H	SecureAPlus SecureAge Technol Hard drive on this co	ogy Pte Ltd omputer
Show details			Yes No
		<u>Change when t</u>	hese notifications appear

• The SecureAPlus Settings window will launch.

	Daily Upload Limit	Message Popup	Exclusions	
🚫 Universal AV	Choose of	ne that best meet y	our internet conne	ction plan:
Application Whitelisting		 Unlimited 		
		✔ 1 GB		
Scan Settings		▶ 100 MB		
		▶ 10 MB		
Update Update			Apply	Cancel
Manage User Rights	— 🙋 Tips — At times, so AV Server f document v	ome program files on y or complete scanning vill be uploaded as we	our computer may be u in the cloud. But none respect your privacy.	ploaded to Universal of your confidential

Note:

▶ Refer to **Section** <u>4</u> for more details on SecureAPlus Settings.

3.10 SecureAPlus Complete Scan

SecureAPlus v3.4.1.1			_ ×
		nteractive Mod You will be prompted w and run a program that he trusted list.	e vhether to trust is not found in Change Mode ►
 ✓ Security Features: Running ✓ Software Update: Up-to-date Last Complete Scan: 2015/08/28 	Settings	Complete Scan	Quarantine & History
More details 🕨	Update	License Extension	P Help
Premium Trial			Enter license code
🛒 Store 💄 Account 🔒 LockCube 🔥 About		Copyright © SecureAge Tech	nology. All rights reserved.

• 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.

	Scanning Results		(
Complete Scan About License	Universal AV Status Your computer is free from malware Number of Infected Files 1. Currently on my PC: 0 2. I have ignored: 0 Executable Files Requested by Se Number of successfully uploaded executa Total file size uploaded: 0 Bytes	! rver Today able files: 0	View Log Delete Log
	Disable Upload	Complete Scan	Retrieve Last Scan
		Convright @ SocureAcc	Technology, All rights record

▶ Refer to **Section** <u>5</u> for more details on Universal AV.

3.11 SecureAPlus Quarantine & History

SecureAPlus v3.4.1.1			_ ×
		Interactive Mod You will be prompted w and run a program that the trusted list.	e vhether to trust is not found in Change Mode ►
 ✓ Security Features: Running ✓ Software Update: Up-to-date Last Complete Scan: 2015/08/28 	Settings	Complete Scan	Quarantine & History
More details >	Update	License Extension	? Help
Premium Trial			Enter license code
🛒 Store 💄 Account 🔒 LockCube 🔥 About	:	Copyright © SecureAge Tech	nology. All rights reserved.

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

😌 User Account	Control		×
Do yo chang	u want to allow th es to this comput	ne following program to make er?	e
٢	Program name: Q Verified publisher: Se File origin: H	uarantine e cureAge Technology Pte Ltd ard drive on this computer	
Show detai	ls	Yes No	
		Change when these notifications a	<u>ppear</u>

• The SecureAge Antivirus Quarantine & History window will launch.

SecureAPlus User Guide

	antine & History		./	
Quarantine	v	Data	Detected by	
Win.Trojan.Ramnit-1484	c:\\$recyde.bin\s-1-5-21-2477740147-125	2014-03-19 10:36:57	ClamAV	
Select All Unselect All]	Restore	Remov	ve Exit

Note:

▶ Refer to **Section** <u>6</u> 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 <u>2.1</u>** for the steps to start SecureAPlus.
- In the SecureAPlus window, click on the Update icon.

SecureAPlus v3.4.1.1			_ ×
		Interactive Mod You will be prompted w and run a program that the trusted list.	e vhether to trust is not found in Change Mode ►
 ✓ Security Features: Running ✓ Software Update: Up-to-date Last Complete Scan: 2015/08/28 	Settings	Complete Scan	Quarantine & History
More details 🕨	Update		(?) Help
Premium Trial			Enter license code
🛒 Store 💄 Account 🔒 LockCube 🔥 About		Copyright © SecureAge Tech	nology. All rights reserved.

• SecureAPlus software will check for new update.

SecureAPlus	Software Update
Seci	reAge
- Shirt	Check New Update Checking whether there is any new update. Please wait
	Cancel

 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,



Refer to Section <u>4.4.1</u> 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.

V A	nteractive Mod ou will be prompted w nd run a program that he trusted list.	e hether to trust is not found in
	he trusted list.	is not round in
X	Ø	Change Mode ►
Settings	Complete Scan	Quarantine & History
Update	Extension	Enter license code
cureAge - Infobra 👰 Software Qu	alty As D Installing and config D fixing The Ho	iology. All hights reserved.
		SecureAPlus Account Portal
	Log In Email Address Password Remember Meot Pace Log In Or f Log In with Facebook S* Log In with Googlet	ssword
	Settings Settings	Settings Update Copyright © SecureAge Technol copyright © SecureAge Technol uredge - Moders uredge - Moders © Software Quality AL: Imail Address Password Rememberg megot Paal Ung in Cog in with Google No SecureAPlus Accoo

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.

SecureAPlus v3.4.1.1			_ × _
	Ver an the term of ter	nteractive Mod ou will be prompted w nd run a program that ne trusted list.	e /hether to trust is not found in Change Mode ►
 Fully Protected ✓ Security Features: Running ✓ Software Update: Up-to-date Last Complete Scan: 2015/08/28 	Settings	Complete Scan	Quarantine & History
More details >	Update	License Extension	PHelp
Premium Trial			Enter license code
🛒 Store 💄 Account 🔒 LockCube 🔥 About	c	opyright © SecureAge Tech	nology. All rights reserved.
Note:			

This corresponds to launching the SecureAPlus User Guide via the SecureAPlus Tray Icon (Section <u>2.2</u>).

4 SecureAPlus Settings

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

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

SecureAPlus v3.4.1.1			_ × _
		Interactive Mod You will be prompted w and run a program that the trusted list.	e vhether to trust is not found in Change Mode ►
 ✓ Security Features: Running ✓ Software Update: Up-to-date Last Complete Scan: 2015/08/28 	Settings	Complete Scan	Quarantine & History
More details 🕨	Update	License Extension	(?) Help
Premium Trial			Enter license code
🛒 Store 💄 Account 🔒 LockCube 🔨 About		Copyright © SecureAge Tech	nology. All rights reserved.

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

😯 User Account Control 🛛 💌				
Do you want to allow the following program to make changes to this computer?				
Program name:SecureAPlus BetaVerified publisher:SecureAge Technology Pte LtdFile origin:Hard drive on this computer				
Show details				
Change when these notifications appear				

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

SecureAPlus	Settings			×
	Daily Upload Limit	Message Popup	Exclusions	0
S Universal AV	Choose on	e that best meet y	our internet conne	ction plan:
Application Whitelisting		Unlimited		
🛞 Scan Settings		✓ 1 GB		
		 100 MB 10 MB 		
Update			Apply	Cancel
Manage User Rights	At times, so AV Server fo	me program files on yo or complete scanning i	our computer may be u in the cloud. But none	ploaded to Universal of your confidential
	document w	vill be uploaded as we r	respect your privacy.	
🛒 Store 💧 Account	LockCube 🔨 Abo	ut 🏠 Home	Copyright © SecureAge Te	chnology. All rights reserved.

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** <u>2.1</u> 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.

SecureAPlus	Settings			×
🔊 Universal AV	Daily Upload Limit	Message Popup	Exclusions	0
Application Whitelisting	Choose or	 that best meet y Unlimited 	our internet conne	ction plan:
Scan Settings		✓ 1 GB▶ 100 MB		
Update		▶ 10 MB	Apply	Cancel
Manage User Rights	- 💋 Tips At times, so AV Server fo document w	me program files on yo or complete scanning i vill be uploaded as we r	our computer may be u in the cloud. But none respect your privacy.	ploaded to Universal of your confidential
🛒 Store 💄 Account	Abo	ut 🏠 Home	Copyright © SecureAge Te	chnology. All rights reserved.

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.

SecureAPlus	Settings			×
	Daily Upload Limit	Message Popup	Exclusions	0
Oniversal AV	Choose on	ie that best meet y	our internet conne	ction plan:
Application Whitelisting		Unlimited		
Scan Settings		✓ 1 GB▶ 100 MB		
Update		▶ 10 MB		
			Apply	Cancel
Manage User Rights	At times, son AV Server fo document w	me program files on yo or complete scanning vill be uploaded as we r	our computer may be u in the cloud. But none respect your privacy.	ploaded to Universal of your confidential
🛒 Store 👃 Account	LockCube Abo	ut 🏠 Home	Copyright © SecureAge Te	chnology. All rights reserved.

• 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.

SecureAPlus	Settings			×
Universal AV Control Contro Control Control Control Control Control Control Control Co	Daily Upload Limit Me "Good News" M When no virus is after rebooting y ☑ Show message — ◯◯ Tips	ssage Popup lessage Promp detected by Ur your computer ge prompt	Exclusions t niversal AV, this pop	pup will appear
User Rights	By default, the "Go your computer if no checkbox to remov	Home	ge prompt will show a d by Universal AV. To d Copyright © SecureAge Te	after every reboot of lisable it, click on the chnology. All rights reserved.

- 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.

SecureAPlus	Settings			×
Image<	Daily Upload Limit Untick the engine tha AVG Avira BitDefender ClamAV ESET Emsisoft McAfee Microsoft Securit Norman QuickHeal Sophos TotalDefense	Message Popup It you want to exclude.	Exclusions	Cancel
🛒 Store 💄 Account	Abo	ut 🏠 Home	Copyright © SecureAge Tech	nology. All rights reserved.

- 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** <u>2.1</u> 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.

SecureAPlus	Settings			×
	Standard Mode	Advanced Mode		0
Oniversal AV	Standard App	lication Whitelisting	g Mode Advanced Set	tings
Application Whitelisting	✓ Interactive You will be promp	e Mode oted whether to trust and	d run a program not in the trusted lis	t.
Scan Settings	Lockdown All untrusted prog	n Mode grams will be automatic	ally blocked from running on your co	omputer.
Update	Trust All All trusted and ur	▼ atrusted programs are a	llowed to run temporarily.	
Manage User Rights	Choose "Lo allow to rui on your PC	ockdown Mode' if you n. But please remembe as a trusted installer be	Apply C cannot decide which program to r to set any new program you wish efore installation.	ancel trust and to install
🛒 Store 💄 Account	Abo	out 🏠 Home	Copyright © SecureAge Technology. All	rights reserved.

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

	Standard Mode Advanced Mode	
Universal AV	Standard Application Whitelisting Mode Advanced Settings	
Application Whitelisting	✓ Interactive Mode You will be prompted whether to trust and run a program not in the trusted list.	
Scan Settings	Lockdown Mode All untrusted programs will be automatically blocked from running on your computer	:
Update	All trusted and F for 5 minutes All bwed to run temporarily.	
Manage User Rights	Tips For 30 minutes until reboot Choose Huntil reboot cannot decide which program to trust ar allow to rup. But please remember to set any new program you wish to inst.	nd all

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

Note:

- This corresponds to selecting the modes via the SecureAPlus Tray Icon Menu (Section <u>2.2</u>).
- 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 <u>7.2.3</u> – 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 <u>7.2.3</u> – 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.

SecureAPlus	Settings				×
	Standard Mode	Advanced Mode		e	
Conversal AV Conve	Advanced App Trust based Allow applic its certifi its certifi its certifi	on digital signature ation with valid digit cate is trusted by the cate name is in the tr cate name and thum	al signature to be operating system usted certificate l bprint is in the tru	Advanced Settings e trusted as installer if: ist usted certificate list	
Update Update Manage User Rights	 Learning model This is an obditive whitelist Tips This configutive this setting, robust protection 	ode servation mode. All t t log. Vie ration is for advanced you can just go with ecction against dubious	he blocked applie ew Log A users. If you are u the default settin programs.	cations are recorded in pply Cancel nsure of how to configure g which already provides	
🛒 Store 👃 Account	CLockCube Abo	out 🏠 Home	Copyright © Secure	Age Technology. All rights reserved	d.

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.

SecureAPlu	is Settings	×
Oniversal AV	Standard Mode Advanced Mode Standard Application Whitelisting Mode Advance	? ed Settings
Application Whitelisting	✓ Interactive Mode You will be prompted whether to trust and run a program not in the trust	sted list.
Scan Settings	All untrusted programs will be automatically blocked from running on Trust All	your computer.
Lpdate	All trusted and For 5 minutes allowed to run temporarily. For 30 minutes	Cancel
Manage User Rights	Choose " • until reboot allow to run. But please remember to set any new program yo on your PC as a trusted installer before installation.	am to trust and ou wish to install
🛒 Store 🕹 Account	t 🔒 LockCube 🔨 About 🏠 Home Copyright © SecureAge Technol	logy. All rights reserved.
SecureAPlus	Settings	×
SecureAPlus	Settings Standard Mode Advanced Mode	× ?
SecureAPlus	Settings Standard Mode Advanced Mode Advanced Application Whitelisting Mode Advanced	× ?
SecureAPlus	Standard Mode Advanced Mode Advanced Application Whitelisting Mode Trust based on digital signature Allow application with valid digital signature to be trusted as i is certificate is trusted by the operating system its certificate name is in the trusted certificate list	X Settings installer if:
SecureAPlus SecureAPlus Oniversal AV Mitelisting Scan Settings	Standard Mode Advanced Mode Advanced Application Whitelisting Mode Trust based on digital signature Allow application with valid digital signature to be trusted as i its certificate is trusted by the operating system its certificate name is in the trusted certificate list its certificate name and thumbprint is in the trusted certificate Learning mode	Settings installer if: cate list
SecureAPlus SecureAPlus Application Application Composition Compo	Standard Mode Advanced Mode Advanced Application Whitelisting Mode Advanced Image: Trust based on digital signature Advanced Image: Trust based on digital signature Advanced Image: Allow application with valid digital signature to be trusted as it Image: Standard Mode Image: Standard Mode Image: Standard Mode Image: Standard Mode Advanced Image: Standard Mode Image: Standard Mode Image: Standard Mode Advanced Image: Standard Mode Image: Standard Mode Image: Standard Mode Advanced Image: Standard Mode Image: Standard Mode Image: Standard Mode Advanced Image: Standard Mode Image: Standard Mode Im	Settings installer if: cate list recorded in Cancel
SecureAPlus SecureAPlus Outiversal AV Application Whitelisting Scan Settings Update Manage User Rights	Standard Mode Advanced Mode Advanced Application Whitelisting Mode ✓ Trust based on digital signature Allow application with valid digital signature to be trusted as it o its certificate is trusted by the operating system o its certificate name is in the trusted certificate list o its certificate name and thumbprint is in the trusted certificate Learning mode This is an observation mode. All the blocked applications are re the whitelist log. View Log Apply Tips This configuration is for advanced users. If you are unsure of how this setting, you can just go with the default setting which alre robust protection against dubious programs.	Settings installer if: cate list recorded in Cancel w to configure eady provides

• The Application Whitelisting window will launch.

SecureAPlus User Guide

Secur	Application Whitelisting	×
	General Restricted Applications Trusted Certificate Script Status	
	Export whitelist to a file Import whitelist from a file	0
	Compact Whitelist Database View log	
		Settings
Applicati Whitelist		list.
Scan Sett		ir computer.
Update		Cancel
Manage User Righ		to trust and vish to install
🛒 Store 🛛 🐣		. All rights reserved.
17	OK Cancel Apply	

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.

and seat
Windows Update
XPS Viewer
Games
Maintenance
Microsoft Office
SecureAge
Application Whitelisting
SecureAPlus
Whinstall SecureAPlus
Startup
1 Back
1 Back
Back Search programs and files
Back Search programs and files
Back Search programs and files
Back Search programs and files
Back Search programs and files
Back Search programs and files

▶ Refer to **Section** <u>7.2</u> 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** <u>2.1</u> 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.

SecureAPlus	Settings			×
Universal AV Application Whitelisting Scan Settings Update	Antivirus Offline and Virus sign Antiviru I Enab I Enab I Enab	Exclusions s Information ivirus engine: ClamAV G ature version: 20846, Fi s Settings: le Offline Antivirus le Universal AV le Real-time Scannir	Included File Types 0.98.7 ri Aug 28 12:37:34 2015	Cancel
Manage User Rights	🔒 LockCube 🔥 Abo	ut 🏠 Home	Copyright © SecureAge Teo	hnology. All rights reserved.

4.3.1 Antivirus

To setup your antivirus settings, follow the steps below:

- Start SecureAPlus. Please refer to **Section** <u>2.1</u> 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.

SecureAPlus	Settings			×
	Antivirus	Exclusions	Included File Types	0
Application	Antiviru Offline ant Virus signa	s Information ivirus engine: ClamAV (ature version: 20846, F).98.7 ri Aug 28 12:37:34 2015	
Whitelisting	Antivirus 🗹 Enabl 🗹 Enabl	s Settings: le Offline Antivirus le Universal AV		
Update	🗹 Enabl	le Real-time Scannir	Apply	Cancel
Manage User Rights				
🛒 Store 👃 Account	About About	ut 🏠 Home	Copyright © SecureAge Tec	hnology. All rights reserved.

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.

SecureAPlus	Settings			×
	Antivirus	Exclusions	Included File Types	0
Application	Antiviru Offline ar Virus sign	us Information htivirus engine: ClamAV (nature version: 20836, V	0.98.7 Ved Aug 26 04:51:25 2015	
Whitelisting	Antiviro Enal Enal	us Settings: ble Offline Antivirus ble Universal AV		
Update	🗆 Enal	ble Real-time Scanni	ng Apply	Cancel
Manage User Rights				
🛒 Store 💄 Account	CLOCKCube 🔥 Ab	out 🏠 Home	Copyright © SecureAge Techn	ology. All rights reserved.

- 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.)

SecureAPlus	Settings			×
	Antivirus	Exclusions	Included File Types	0
Oniversal AV	Antiviru: Offline ant	s Information tivirus engine: ClamAV 0).98.7	
Application Secure Whitelisting	APlus		— ×	
Scan Setting:	ClamAV will remain	in the memory until the	machine is rebooted.	
Update			ОК	Cancel
Manage User Rights				
		•		
🚽 Store 🐣 Account	LockCube 🔨 Abo	ut 🏠 Home	Copyright © SecureAge Tec	hnology. All rights reserved.

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

SecureAPlus	Settings			×
	Antivirus	Exclusions	Included File Types	0
Image: Constraint of the second se	Antiviru Offline an Virus sign Antiviru Enab Enab Enab	s Information tivirus engine: ClamAV G ature version: 20836, V s Settings: le Offline Antivirus le Universal AV le Real-time Scannin	0.98.7 Ved Aug 26 04:51:25 2015 Ng	
Update Update Manage User Rights			Apply	Cancel
🛒 Store 💄 Account	CockCube Abo	ut 🏠 Home	Copyr SecureAPlu: Real-time scanr	s v x erved. ning 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.

SecureAPlus	Settings			×
Ouniversal AVOuniversal AV </th <th>Antivirus Offline an Virus sign Antiviru D Enab Enab Enab</th> <th>Exclusions Is Information Itivirus engine: ClamAV G Nature version: 20836, W Is Settings: De Offline Antivirus De Universal AV De Real-time Scannir</th> <th>Included File Types 0.98.7 Ved Aug 26 04:51:25 201</th> <th>5 Cancel</th>	Antivirus Offline an Virus sign Antiviru D Enab Enab Enab	Exclusions Is Information Itivirus engine: ClamAV G Nature version: 20836, W Is Settings: De Offline Antivirus De Universal AV De Real-time Scannir	Included File Types 0.98.7 Ved Aug 26 04:51:25 201	5 Cancel
🛒 Store 👃 Account	🔒 LockCube 🔥 Abo	out 🏠 Home	Copyright © SecureAge Te	chnology. All rights reserved.

- 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.)

SecureAPlus	s Settings			×
	Antivirus	Exclusions	Included File Types	0
Oniversal AV	Antiviru: Offline ant	s Information tivirus engine: ClamAV 0	.98.7	
Application Secu Whitelisting	reAPlus			
Scan Setting:	ClamAV will remain	in the memory until the	machine is rebooted.	
Update			ОК	Cancel
Manage User Rights				
🛒 Store 💧 Account	LockCube Abo	ut 🏠 Home	Copyright © SecureAge Tec	hnology. All rights reserved.

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

SecureAPlus	×			
	Antivirus	Exclusions	Included File Types	0
Ouniversal AVOuniversal AV </th <th>Antiviru Offline an Virus sign Antiviru □ Enab ☑ Enab</th> <th>s Information tivirus engine: ClamAV G ature version: 20836, W s Settings: le Offline Antivirus le Universal AV le Real-time Scannir</th> <th>0.98.7 Ved Aug 26 04:51:25 2015 ng Apply</th> <th>Cancel</th>	Antiviru Offline an Virus sign Antiviru □ Enab ☑ Enab	s Information tivirus engine: ClamAV G ature version: 20836, W s Settings: le Offline Antivirus le Universal AV le Real-time Scannir	0.98.7 Ved Aug 26 04:51:25 2015 ng Apply	Cancel
🛒 Store 💄 Account	LockCube 🔥 Abo	ut 🏠 Home	Copyr (1) SecureAPlu Real-time scan	IS 🔌 🗙 erved. Ining 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.

SecureAPlus Settings				×
Universal AV Control Application Whitelisting Control Scan Settings Control Update Control Manage User Rights Control Manage User Rights	Antivirus Offline an Virus sigr Antiviru S Enab Enab	Exclusions Is Information Itivirus engine: ClamAV O nature version: 20836, W Is Settings: De Offline Antivirus De Universal AV De Real-time Scannin	Included File Types	Cancel
🛒 Store 👃 Account	CLockCube 🔨 Abo	out 🏠 Home	Copyright © SecureAge Techn	ology. All rights reserved.

- 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.

Universal AV Antivirus Information Application Offline antivirus engine: ClamAV 0.98.7 Virus signature version: 20836, Wed Aug 26 04:51:25 2015 Antivirus Settings: Scan Settings Update Manage		Antivirus	Exclusions	Included File Types	(
Update Apply Cancel Manage	Universal AV Application Whitelisting	Antivirus Offline ant Virus signa Antivirus ☑ Enabl ☑ Enabl	s Information ivirus engine: ClamAv ature version: 20836, s Settings: le Offline Antivirus e Universal AV	/ 0.98.7 Wed Aug 26 04:51:25 2015	
	Update Manage	🗆 Enabl	e Real-time Scann	ning Apply	Cancel

Copyright © SecureAge Technology Pte Ltd. All rights reserved.

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.

SecureAPlus	Settings			×
Oniversal AV	Antivirus Antiviru	Exclusions us Information	Included File Types	0
Application Whitelisting	Offline ar Virus sign Antiviru S Enab	ntivirus engine: ClamAV (nature version: 20836, W us Settings: Dle Offline Antivirus).98.7 /ed Aug 26 04:51:25 2015	
Scan Settings	🗹 Enat	ole Universal AV ole Real-time Scannir	Apply	Cancel
Manage User Rights			Арріу	Cancer
🛒 Store 🕹 Account	🔒 LockCube 🔥 Abo	out 🏠 Home	Copyright © SecureAge Techno	ology. All rights reserved.

- 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.

SecureAPlus	Settings			>	
	Antivirus	Exclusions	Included File Types	0	
🔊 Universal AV	Antiviru	s Information			
Application	Offline an Virus sign	tivirus engine: ClamAV ature version: 20836,	0.98.7 Wed Aug 26 04:51:25 2015		
Whitelisting	Antiviru				
Scan Settings	Enable Offline Antivirus Frable Universal AV				
, Octain Section go	 Enable Chiversa Av Enable Real-time Scanning 				
Update			(and)	Connect	
			Арріу	Cancel	
Manage User Rights					
Store 💄 Account		out 🏠 Home		s 🔌 X erved.	
			Real-time scan	ning is enabled.	
				- 🌛 😼 🕯	

4.3.1.5 Application Whitelisting only

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

SecureAPlus	×			
Image Universal AVImage Universal AVImage UpdateImage User Rights	Antivirus Offline an Virus sign Antiviru Enab Enab	Exclusions Is Information htivirus engine: ClamAV C nature version: 20836, W Is Settings: Dele Offline Antivirus Dele Universal AV Dele Real-time Scannin	Included File Types	Cancel
🛒 Store 👃 Account	Abo	out 🏠 Home	Copyright © SecureAge Te	chnology. All rights reserved.

- 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.)

SecureAPlu	s Settings			×
	Antivirus	Exclusions	Included File Types	0
Universal AV	Antivirus Offline ant	s Information ivirus engine: ClamAV 0	0.98.7	
Application Sect Whitelisting	IreAPlus	in the memory until the	machine is rebooted.	
Update			OK	Cancel
Store & Account	LockCube About	ut 🏠 Home	Copyright © SecureAge Techr	nology. All rights reserved.

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

SecureAPlus	Settings			×
	Antivirus	Exclusions	Included File Types	0
Conversal AV Conversal AV Conversal AV Application Whitelisting Scan Settings	Antiviru Offline an Virus sign Antiviru Enab Enab	s Information tivirus engine: ClamAV (ature version: 20836, V s Settings: le Offline Antivirus le Universal AV le Real-time Scanni	0.98.7 Ved Aug 26 04:51:25 2015	
Update Update Manage User Rights			Apply	Cancel
🛒 Store 👃 Account	🔒 LockCube 🔥 Aba	ut 🏠 Home	Copyr SecureAPlu Real-time scan	S X erved. ning 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.

SecureAPlus S	Settings			×
Ouniversal AVOuniversal AV </th <th>Antivirus Offline an Virus sign Antiviru S Enab Enab Enab</th> <th>Exclusions s Information tivirus engine: ClamAV (ature version: 20836, V s Settings: le Offline Antivirus le Universal AV le Real-time Scannin</th> <th>D.98.7 Ved Aug 26 04:51:25 2015</th> <th>Cancel</th>	Antivirus Offline an Virus sign Antiviru S Enab Enab Enab	Exclusions s Information tivirus engine: ClamAV (ature version: 20836, V s Settings: le Offline Antivirus le Universal AV le Real-time Scannin	D.98.7 Ved Aug 26 04:51:25 2015	Cancel
🛒 Store 👃 Account 🕯	LockCube 🔨 Abo	ut 🏫 Home	Copyright © SecureAge Techno	ology. All rights reserved.

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

	Antivirus	Exclusions	Included File Types	6	
Oniversal AV	Antiviru Offline an Virus sign	is Information tivirus engine: ClamAV ature version: 20836, N	0.98.7 Wed Aug 26 04:51:25 2015		
whitelisting	Antivirus Settings: Enable Offline Antivirus				
🕮 Scan Settings	 Enable Universal AV Enable Real-time Scanning 				
Update			Apply	Cancel	
Manage User Rights					
🚽 Store 💄 Account 🕯	LockCube 🔨 Abo	out 🏠 Home	Copyr 🔞 SecureAPlus	🔌 🗶 erved	

4.3.1.7 Offline Antivirus with real-time protection

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

SecureAPlus	×			
	Antivirus	Exclusions	Included File Types	0
Application	Antiviru Offline ar Virus sign	us Information htivirus engine: ClamAV (nature version: 20836, V).98.7 Ved Aug 26 04:51:25 201	5
Whitelisting	Antiviru 🗹 Enat	us Settings: ble Offline Antivirus ble Universal AV]	
Update	🗹 Enat	ble Real-time Scannii	Apply	Cancel
Manage User Rights				
🛒 Store 💄 Account	CLOCKCube Abo	out 🏠 Home	Copyright © SecureAge Ted	chnology. All rights reserved.

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

SecureAPlus S	Settings			×
	Antivirus	Exclusions	Included File Types	0
Application Whitelisting	Antiviru Offline an Virus sign Antiviru S Enab	s Information tivirus engine: ClamAV ature version: 20836, V s Settings: le Offline Antivirus	0.98.7 Ved Aug 26 04:51:25 2015	
Update	🗆 Enab	ie Universal AV le Real-time Scanni	ng Apply	Cancel
Manage User Rights				
🛒 Store 👃 Account 🕻	LockCube 🔨 Abo	ut 🏠 Home	Copyr SecureAPI Real-time sca	US X erved. nning 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** <u>2.1</u> 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.

SecureAPlus Settings					
	Antivirus	Exclusions	Included File Types	0	
Oniversal AV	Specify the fil	es or folders to be	excluded from scan	ning:	
Application Whitelisting	Name			Add	
Scan Settings				Remove	
Update			Apply	Cancel	
Manage User Rights	Tips Universal A Similarly, Se and exclude	V will not upload and cureAPlus Offline Anti d new program files.	scan excluded progra virus will not scan excl	m files in the cloud. uded document files	
🛒 Store 👃 Account	🔒 LockCube 🔥 Abo	ut 🏠 Home	Copyright © SecureAge Te	chnology. All rights reserved.	

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

Select a file or folder:	X
 Computer Floppy Disk Drive (A:) Local Disk (C:) DVD RW Drive (D:) 	
	OK Cancel

It will be displayed under the list of exclusions.

SecureAPlus	Settings			×
	Antivirus	Exclusions	Included File Types	0
S Universal AV	Specify the fil	es or folders to be	excluded from scann	ing:
Application Whitelisting	C:\Users\Admin\D	esktop\Test		Add
Scan Settings				Remove
Update			Apply	Cancel
Manage User Rights	— 🕖 Tips Universal A Similarly, Se and excluded	V will not upload and cureAPlus Offline Anti d new program files.	l scan excluded program ivirus will not scan excluc	files in the cloud. ded document files
🛒 Store 💄 Account 🕯	LockCube 🔨 Abo	ut 🏠 Home	Copyright © SecureAge Tech	nology. All rights reserved.

• 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.

	Antivirus	Exclusions	Included File Types	8
🔗 Universal AV	Specify the file	es or folders to be	e excluded from scannin	g:
Application Whitelisting	C:\Users\Admin\D	esktop\Test		Add
😁 Scan Settings				Remove
Update			Apply	Cancel
Manage User Rights	- O Tips Universal AV Similarly, Ser and excluded	/ will not upload an cureAPlus Offline An d new program files.	d scan excluded program fi tivirus will not scan excluded	es in the cloud. d document files

• 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.

SecureAge Antivirus					
SecureAge					
S Threat detected!					
Win32/Tnega.XAAI!suspicious					
Detected by: AVG, BitDefender, ESET, TotalDefense					
File: c:\users\sijie\desktop\mailpv.exe					
What action would you like to perform to this file?					
Quarantine					
Delete					
Allow once					
🔘 Ignore					
Remember my answer throughout this session.					

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.



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 <u>2.1</u> 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.

	Antivirus	Exclusions	Included File Types	(
🔊 Universal AV	Succify the file	ovtonsions to be	included in the course	ing hu
	Note: Separate mul	ltiple file extensions	with semicolon (;):	ing by:
Application	Offline Anti	ivirus		
Whitelisting	.zip;.rar			Add
	Extension			Remove
Scan Settings				
-				
Update 💦			Apply	Cancel
	7 Tine		орриу	Cancer
Anage Manage	Universal AV	scans .dll, .exe, .ja	r and .msi files in the clou	ud and SecureAPlus
User Rights	Offline Antivi	irus scans new prog he PC. You can also	ram files, .pdf, .docx, .doc, add in other file extensions	.xlsx, .xls, .pptx and

 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.

SecureAPlus	Settings			×
	Antivirus	Exclusions	Included File Types	0
Ouniversal AV	Specify the file Note: Separate mo	e extensions to be in ultiple file extensions wi	ncluded in the scan ith semicolon (;):	ning by:
Application Whitelisting	Offline And	tivirus ion, e.g.: .doc;.pdf)		Add
Scan Settings	Extension .zip .rar			Remove
Update			Apply	Cancel
Manage User Rights	- O Tips Universal A' Offline Antiv .ppt files at	V scans .dll, .exe, .jar a virus scans new progra the PC. You can also ad	and .msi files in the clo m files, .pdf, .docx, .doc d in other file extension	oud and SecureAPlus , .xlsx, .xls, .pptx and s for scanning.
🛒 Store 👃 Account	LockCube 🔨 Abo	ut 🏠 Home	Copyright © SecureAge Te	chnology. All rights reserved.

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.

Specify the file Note: Separate mu	extensions to be i ultiple file extensions w	ncluded in the scanni vith semicolon (;):	ng by:
Offline Ant	tivirus		
(enter file extensi	on, e.g.: .doc;.pdf)		Add
Extension			Remove
.zip			
		Apply	Cancel
- 🧭 Tips	√ scans .dll, .exe, .jar	and .msi files in the clou	d and SecureAPlus
	Specify the file Note: Separate mu Offline Ant (enter file extensi Extension .zip .rar	Specify the file extensions to be in Note: Separate multiple file extensions w Offline Antivirus (enter file extension, e.g.: .doc;.pdf) Extension .zip .rar	Specify the file extensions to be included in the scanni Note: Separate multiple file extensions with semicolon (;): Offline Antivirus (enter file extension, e.g.: .doc;.pdf) Extension .zip .rar Apply

 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.

	Antivirus	Exclusions	Included File Types	(
Oniversal AV	Specify the file Note: Separate mul Offline Anti	extensions to be i tiple file extensions w virus	ncluded in the scan ith semicolon (;):	ning by:
Whitelisting	(enter file extensio	n, e.g.: .doc;.pdf)		Add
	Extension			Remove
Scan Settings				
Update			Apply	Cancel
Manage User Rights	Universal AV Offline Antivi .ppt files at th	scans .dll, .exe, .jar rus scans new progra ne PC. You can also ac	and .msi files in the clo m files, .pdf, .docx, .doo d in other file extensior	oud and SecureAPlus ;, .xlsx, .xls, .pptx and is for scanning.

4.4 Update

4.4.1 Software

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

- Start SecureAPlus. Please refer to **Section** <u>2.1</u> 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.

SecureAPlus	Settings		×			
	Software	Virus Signature	0			
Universal AV	Softwar	e Update and Setting	Update			
Application Whitelisting	Current	Version: 3.4.1.1				
Scan Settings	Notify me for new update					
Update	► Ma	nual update	Apply Cancel			
Manage User Rights	Apply Cancel Tips Select an option that best meet your future software update's requirement. Alternatively, click on the "Update" button to manually check and update to the latest SecureAPlus version now.					
🛒 Store 🛛 🐣 Account	LockCube Abo	out 🏫 Home Copy	right © SecureAge Technology. All rights reserved.			

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.

😌 User Account	Control	—
😨 Do yo chang	u want to allow the follow es to this computer?	wing program to make
Ø	Program name: Update Sec Verified publisher: SecureAge File origin: Hard drive	ureAPlus • Technology Pte Ltd on this computer
Show detai	ls	Yes No
	Chang	e when these notifications appear

It will start to download the new update.

SecureAPlu	s Software Update	
Sec	JreAge	1.
SHILL REAL	Download Downloading SecureAPlusSetup_v1.0.27.ex Please wait	e.
21446656	of 95113944 bytes	22%

 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**.

SecureAPI	us Software Upo	Jate	×
Sec	ureAg	e 🥢	1.
	Softwar	e Update	
There is It is rec	s an update av ommended tha	ailable for SecureAPlus. at you always install the lates	t updates.
Opti	ions	Download & Install	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:

- SecureAPlus Settings × 0 Software **Virus Signature** Universal AV Software Update and Setting Update Current Version: 2.3.2.1 Application Whitelisting Automatic update **Scan Settings** Notify me for new update Manual update Update Apply Cancel 💋 Tips Manage Select an option that best meet your future software update's requirement. **User Rights** Alternatively, click on the "Update" button to manually check and update to the latest SecureAPlus version now. 🛒 Store 💄 Account 🔥 About 🏾 🏠 Home Copyright © SecureAge Technology. All rights reserved.
- 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.

SecureAPlus Softv	Age	
📀 Up t	to date	
Your software	is up to date.	
	OK	

• 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.

👕 SecureAPlus Beta v3.0.0 Setup	
Installing Please wait while SecureAPlus Beta v3.0.0 is being installed.	4000
Extract: saappctl.inf 100% Extract: SATrustCtx.dll 100% Extract: Application Whitelisting.exe 100% Extract: Process Protector.exe 100% Extract: saappsvc.exe 100% Extract: sanotifier.exe 100% Extract: SearchSvc.exe 100% Extract: saappctl.sys 100% Extract: FinishInstallation.exe 100% Extract: SASystemScan.exe	
SecureAge Technology	Cancel

 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.

👕 SecureAPlus Beta v3.0.0 Setup	
Installation Complete Setup was completed successfully.	4 6 24
Completed	
👕 SecureAPlus Beta v3.0.0 Setup	23
Your computer needs to be restarted for the new updates to t Do you want to reboot the system now?	ake effect.
Yes	No
SecureAge Technology < Back Close	Cancel

4.4.2 Virus Signature

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

- Start SecureAPlus. Please refer to **Section** <u>2.1</u> 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.

SecureAPlus	Settings	×
	Software Virus Signature	0
Universal AV	Virus Signature Update and Setting	Update
Application Whitelisting	Virus signature version: 20846, Fri Aug 28 12:37:34 2015 ✓ Automatic daily update Manual update	
Scan Settings	Virus Signature Server: database.clamav.net Proxy Server: Port:	
Update	Retrieve System Proxy Settings Apply	Cancel
Manage User Rights	— V Tips Click on the "Update" button to manually update the virus signature option that best meet your future virus signature update's Configure the proxy server if the virus signature fails to update.	e or select an requirement.
🛒 Store 👃 Account	LockCube 🔨 About 🏫 Home Copyright © SecureAge Technology	. All rights reserved.

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.

_	Software	Virus Signature		
🔊 Universal AV	Virus Si	gnature Update and	Setting Updat	е
Application Whitelisting	Virus sig	tomatic daily update	 Aug 28 12:37:34 2015 Manual update 	
🕮 Scan Settings	Scan Settings			
Update	Proxy S Retrie	erver: ve System Proxy Sett	ings	
Manage User Rights	- 💋 Tips	e "Update" button to mai it best meet your futu the proxy server if the vir	nually update the virus signature or sele ure virus signature update's requirer us signature fails to update.	ect an ment.

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

SecureAPlus	Settings		×
	Software	Virus Signature	0
Oniversal AV	Virus Si	gnature Update and S	Setting
Application Whitelisting	Virus sign	nature version: 20846, Fri A tomatic daily update	Aug 28 12:37:34 2015
Scan Settings	Virus Si Proxy S	gnature Server: data	base.clamav.net Port:
Update	Retriev	ve System Proxy Settin	ngs Apply Cancel
Manage User Rights	- ⊘ Tips Click on the option tha Configure t	"Update" button to manu t best meet your future he proxy server if the viru:	ually update the virus signature or select an e virus signature update's requirement. s signature fails to update.
🛒 Store 🕹 Account	🔒 LockCube 🔥 Abo	out 🏫 Home C	opyright © SecureAge Technology. All rights reserved.

• 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.

SecureAge Antivirus Signatures Update	
SecureAge	
main.dd is up to date (version: 55, sigs: 2424225, f-level: 60, builder: neo)	
daily.dd is up to date (version: 20846, sigs: 1547069, f-level: 63, builder: neo) bytecode.dd is up to date (version: 268, sigs: 47, f-level: 63, builder: anvilleg)	
Done.	
OK	

Vote:

- 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.

User Accounts		×			
Users Advanced					
Use the list below to grant or deny users access to your computer, and to change passwords and other settings.					
Users must enter a user name and password to use this computer.					
Users for this computer:					
User Name	Group				
🔏 admin	Administrators; Users				
Schloe	Administrators				
Password for admin To change your Password.	Add Remove Properties r password, press Ctrl-Alt-Del and select Change Reset Password				
	OK Cancel Apply	/			

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

	Trusted Accounts	
Universal AV	Specify list of users who have the ri	ights to modify the whitelist:
Application Whitelisting	Trusted Groups Administrators Add Add	Trusted Users SYSTEM ICE ERVICE Remove
Scan Settings	Administrators Backup Operators Cryptographic Operators	
Update	Distributed COM Users Event Log Readers Guests IIS_IUSRS Network Configuration Operators	Apply Cancel
Manage User Rights	Performance Log Users Performance Monitor Users Power Users Remote Desktop Users Replicator Users	unts will have the rights to : of each program file and 3) run staller.

 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.)

-	Trusted Accounts		
Universal AV	Specify list of users who have the righ	ts to modify the whitelist:	
Application Whitelisting	Administrators Add S Add S Add S	Trusted Users Ad VSTEM ICE ERVICE Remo	d ove
😁 Scan Settings	LOCAL SERVICE NETWORK SERVICE SYSTEM	•	
Update		Apply Cance	I
Manage User Rights	Tips Those users who are listed here as trust 1) add new whitelist, 2) modify the trus any installation software that is trusted	ed accounts will have the rights to : it level of each program file and 3) as an installer.	run

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 <u>4.5.1.2</u>Manage 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



• .

- 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.

🌆 Computer Management			- • •		
File Action View Help					
 Computer Management (Local System Tools O Task Scheduler Event Viewer S Shared Folders Local Users and Groups 	Name Administrators Backup Operators Cryptographic Operat Distributed COM Users	Description Administrators have complete an Backup Operators can override se Members are authorized to perfor Members are allowed to launch, a	Actions Groups More Actions		
 Users Groups Performance Device Manager Storage Disk Management Services and Applications 	 Event Log Readers Guests IIS_IUSRS Network Configuratio Performance Log Users Performance Monitor Power Users Remote Desktop Users Replicator Users 	Members of this group can read e Guests have the same access as m Built-in group used by Internet Inf Members in this group can have s Members of this group may sche Nembers of this group can acces Power Users are included for back Members in this group are grante Supports file replication in a dom Users are prevented from making			
< <u> </u>					

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

🌆 Computer Management			
File Action View Help			
🗢 🤿 🖄 🖬 🙆 🔒 👔			
 Computer Management (Local System Tools O Task Scheduler I Event Viewer S Shared Folders Scal Users and Groups Users 	Name Administrators Backup Operators Cryptographic Operat Distributed COM Users Event Log Readers	Description Administrators have complete an Backup Operators can override se Members are authorized to perfor Members are allowed to launch, a Members of this group can read e	Actions Groups More Actions
Groups > N Performance Device Manager * Storage Disk Management > Services and Applications	GUESTS IS_IUSRS Network Configuratio Performance Log Users Performance Monitor Power Users	Built-in group used by Internet Inf Built-in group used by Internet Inf Members in this group can have s Members of this group may sche Power Users are included for back	
	 Remote Desktop Users Replicator Users 	Members in this group are grante Supports file replication in a dom Users are prevented from making New Group	
	L	Refresh Export List View • Arrange Icons • Line up Icons	
		Help	
Creates a new local group.			

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

New Group		? 💌
Group name:	SecureAge	
Description:	For SecureAge Only	
Members:		
Add	Remove	
Help	Create	Close

 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.

New Group			? <mark>×</mark>
Group name:			
Description:			
Members:			
Add	Remove		
Help		Create	Close

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

😓 Computer Management						
File Action View Help	File Action View Help					
🗢 🧼 🖄 📰 🙆 😖 🛛						
 Computer Management (Local System Tools Task Scheduler Event Viewer Shared Folders Local Users and Groups Operformance Device Manager Storage Disk Management Services and Applications 	Name Administrators Backup Operators Cryptographic Operat Distributed COM Users Cryptographic Operat Distributed COM Users Fuests IS_IUSRS Network Configuratio Performance Log Users Performance Monitor Power Users Remote Desktop Users Replicator Users SecureAge	Description Administrators have complete an Backup Operators can override se Members are authorized to perfor Members of this group can read e Guests have the same access as m Built-in group used by Internet Inf Members in this group can have s Members of this group may sche Members of this group can acces Power Users are included for back Members in this group are grante Supports file replication in a dom Users are prevented from making For SecureAge Only		Actions Groups Actions		
	L			1		

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.

New User					? <mark>-×</mark>
User name:	Sijie				
Full name:					
Description:					
Password:		•••••			
Confirm password	:	•••••			
User must cha	nge pa	issword at next	logon		
User cannot ch	nange	password			
Password never	er expi	res			
Account is disa	abled				
Help				Create	Close

 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.

New User	? 🔀
User name:	
Full name:	
Description:	
Password:	
Confirm password:	
🔽 User must change	assword at next logon
User cannot chang	e password
Password never ex	bires
Account is disable	
Help	Create

• 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** <u>2.1</u> 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.

SecureAPlus	Settings	×
	Trusted Accounts	0
Application Whitelisting	Specify list of users who have the rights to more Trusted Groups Trust Administrators Add	dify the whitelist: ted Users
Scan Settings	Remove LOCAL SERVIC	CE Remove
Lpdate		Apply Cancel
Manage User Rights	 Tips Those users who are listed here as trusted accounts 1) add new whitelist, 2) modify the trust level of e any installation software that is trusted as an installation 	s will have the rights to : ach program file and 3) run ler.
🛒 Store 👃 Account	About A Home Copyright © Secu	reAge Technology. All rights reserved.

 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.

SecureAPlus Settings ×					
	Trusted Accounts		0		
Universal AV	Specify list of users who ha	ve the rights to modify the whi	telist:		
Application Whitelisting	Administrators	Add SYSTEM LOCAL SERVICE NETWORK SERVICE	Add Remove		
Scan Settings					
Update		Apply	Cancel		
Manage User Rights	— O Tips Those users who are listed 1) add new whitelist, 2) mo any installation software the	here as trusted accounts will have the odify the trust level of each program f at is trusted as an installer.	rights to : file and 3) run		
🛒 Store 🕹 Account	🔨 About 🛛 🏠 Home	Copyright © SecureAge Technolog	y. All rights reserved.		

 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.

Add		—
Administrators Backup Operators Cryptographic Operator Distributed COM Users Event Log Readers Guests IIS_IUSRS Network Configuration (O Performance Log Users Performance Monitor Us Power Users Remote Desktop Users Replicator	s Operators Jers	
SecureAge Users		
Add		×
SecureAge		•
	ОК	Cancel

SecureAPlus	Settings			×
	Trusted Accounts			0
Universal AV	Specify list of users w	ho have the r	ights to modify the whi	telist:
Application Whitelisting	Trusted Groups Administrators SecureAge	Add Remove	Trusted Users SYSTEM LOCAL SERVICE NETWORK SERVICE	Add Remove
Scan Settings				
Update			Apply	Cancel
Manage User Rights	 —	e listed here as tr t, 2) modify the ware that is trust	usted accounts will have the trust level of each program ed as an installer.	rights to : file and 3) run
🛒 Store 🕹 Account	🔨 About	c	Copyright © SecureAge Technolog	gy. All rights reserved.

• 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.

SecureAPlus	Settings		×
Oniversal AV Application Whitelisting Scan Settings	Trusted Accounts Specify list of users who have to Trusted Groups Administrators Addinistrators Addiniestrators Addiniestrator	the rights to modify the whit Trusted Users SYSTEM LOCAL SERVICE NETWORK SERVICE	elist: Add Remove
Update Update Manage User Rights	- O Tips Those users who are listed here 1) add new whitelist, 2) modify any installation software that is	Apply e as trusted accounts will have the r y the trust level of each program fi s trusted as an installer.	Cancel ights to : le and 3) run
🛒 Store 🕹 Account	🔨 About 🛛 🏠 Home	Copyright © SecureAge Technology	. All rights reserved.

• 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.

SecureAPlus	Settings			×
Universal AV	Trusted Accounts Specify list of users who	have the r	ights to modify the whi	? itelist:
Application Whitelisting	Trusted Groups Administrators	Add Remove	Trusted Users SYSTEM LOCAL SERVICE NETWORK SERVICE	Add Remove
Update Update Manage User Rights	Tips Those users who are lis 1) add new whitelist, 2 any installation softwar	ted here as tr) modify the e that is trust	Apply usted accounts will have the trust level of each program ed as an installer.	Cancel rights to : file and 3) run
🛒 Store 🛛 👃 Account	About 🏠 Home	c	copyright © SecureAge Technolog	gy. All rights reserved.

 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.

dd	— ×
sijie	.
LOCAL SERVICE NETWORK SERVICE SYSTEM	

• 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.

SecureAPlus	Settings	×
	Trusted Accounts	0
Oniversal AV	Specify list of users who have the rights to modify Trusted Groups Trusted U	the whitelist:
Whitelisting	Administrators Add SYSTEM SecureAge Remove NETWORK SERVICE	Add Remove
Scan Settings	spie	
Update		ly Cancel
Manage User Rights	 Tips Those users who are listed here as trusted accounts will 1) add new whitelist, 2) modify the trust level of each any installation software that is trusted as an installer. 	have the rights to : program file and 3) run
🛒 Store 👃 Account	About A Home Copyright © SecureAge	Technology. All rights reserved.

• 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** <u>2.1</u> for the steps to start SecureAPlus.
- In the SecureAPlus window, click on the Complete Scan icon.

SecureAPlus v3.4.1.1			_ × _
		Interactive Mod You will be prompted w and run a program that the trusted list.	e vhether to trust is not found in Change Mode ►
 ✓ Security Features: Running ✓ Software Update: Up-to-date Last Complete Scan: 2015/08/28 	Settings	Complete Scan	Quarantine & History
More details 🕨	Update	License Extension	P Help
Premium Trial			Enter license code
🛒 Store 👃 Account 🔒 LockCube 🔥 About		Copyright © SecureAge Tech	nology. All rights reserved.

• 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.

SecureAPlus	Status	_ ×
Complete Scan Complete Scan About Complete Scan	Scanning Results Universal AV Status Your computer is free from malware! Number of Infected Files 1. Currently on my PC: 0 2. I have ignored: 0 Executable Files Requested by Server Today Number of successfully uploaded executable files: 0 Total file size uploaded: 0 Bytes	B
	Disable Upload Complete Scan Retrieve Last	Scan
Store 💄 Account	LockCube About About Copyright © SecureAge Technology, All right	ts reserved.

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.

SecureAPlus	s Status	_ ×
	Scanning Results	0
Complete Scan <td>Universal AV Status Your computer is free from malware! Number of Infected Files 1. Currently on my PC: 0 2. I have ignored: 0 Executable Files Requested by Server Today Number of successfully uploaded executable files: 0 Total file size uploaded: 0 Bytes</td> <td>b</td>	Universal AV Status Your computer is free from malware! Number of Infected Files 1. Currently on my PC: 0 2. I have ignored: 0 Executable Files Requested by Server Today Number of successfully uploaded executable files: 0 Total file size uploaded: 0 Bytes	b
	Disable Upload Complete Scan Retrieve Last	Scan
🛒 Store 👃 Account	Copyright © SecureAge Technology. All rights	reserved.

• The uploading will be disabled.

SecureAPlus	s Status .	_ ×
Complete Scan About Complete Scan License	Scanning Results Universal AV Status Your computer is free from malware! Number of Infected Files 1. Currently on my PC: 0 2. I have ignored: 0 Executable Files Requested by Server Today Number of successfully uploaded executable files: 0 Total file size uploaded: 0 Bytes	
	Enable Upload Complete Scan Retrieve Last Sc	an
🛒 Store 🛛 👃 Account	Copyright © SecureAge Technology. All rights re	served.

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

• Click on Enable Upload button.

SecureAPlus	Status	- ×
Complete Scan Complete Scan About Complete Scan License	Scanning Results Universal AV Status Your computer is free from malware! Number of Infected Files 1. Currently on my PC: 0 2. I have ignored: 0 Executable Files Requested by Server Today Number of successfully uploaded executable files: 0 Total file size uploaded: 0 Bytes	0
	Enable Upload Complete Scan Retrieve Last Sca	in
🛒 Store Account	Enable Upload Complete Scan Retrieve Last Sca	in erved.

• The uploading will be enabled.

SecureAPlus	s Status	_ ×
	Scanning Results	0
Complete ScanAboutComplete ScanComplete ScanComplete Scan	Universal AV Status Your computer is free from malware! Number of Infected Files 1. Currently on my PC: 0 2. I have ignored: 0 Executable Files Requested by Server Today Number of successfully uploaded executable files: 0 Total file size uploaded: 0 Bytes Disable Upload Complete Scan Retrieve Late	Log Log ast Scan
🛒 Store 💧 Account	LockCube About About Copyright © SecureAge Technology. All r	ights reserved.

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.

SecureAPlus	s Status	_ ×
	Scanning Results	0
Complete Scan <td>Universal AV Status Your computer is free from malware! Number of Infected Files 1. Currently on my PC: 0 2. I have ignored: 0 Executable Files Requested by Server Today Number of successfully uploaded executable files: 0 Total file size uploaded: 0 Bytes Disable Upload Complete Scan Retrieve</td> <td>ew Log ete Log e Last Scan</td>	Universal AV Status Your computer is free from malware! Number of Infected Files 1. Currently on my PC: 0 2. I have ignored: 0 Executable Files Requested by Server Today Number of successfully uploaded executable files: 0 Total file size uploaded: 0 Bytes Disable Upload Complete Scan Retrieve	ew Log ete Log e Last Scan
🛒 Store 🕹 Account	LockCube About About Copyright © SecureAge Technology.	All rights reserved.

• The progress of the scanning will be shown.

SecureAPlus	Status	_ × _
Complete Scan Complete Scan About Complete Scan License	Scanning Results Universal AV Status Searching for new hashes Number of Infected Files 1. Currently on my PC: 0 2. I have ignored: 0 Executable Files Requested by Server Today Number of successfully uploaded executable files: 0 Total file size uploaded: 0 Bytes 1 of 511507 Disable Upload Complete Scan	View Log Delete Log 0%
🛒 Store 💄 Account	LockCube About About Copyright © SecureAge Technolo	ogy. All rights reserved.

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

SecureAPlus	Status _	- ×
	Scanning Results	0
Complete Scan	Universal AV Status Your computer is free from malware!	
About	Number of Infected Files View Log 1. Currently on my PC: 0 2. I have ignored: 0	
Verse License	Executable Files Requested by Server Today Number of successfully uploaded executable files: 0 Total file size uploaded: 0 Bytes	
	Disable Upload Complete Scan Retrieve Last Sca	n
🛒 Store 🕹 Account	About 🏠 Home Copyright © SecureAge Technology. All rights res	erved.
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.

SecureAPlus	Status	_ ×
	Scanning Results	0
Complete Scan <th>Universal AV Status Your computer is free from malware! Number of Infected Files 1. Currently on my PC: 0 2. I have ignored: 0 Executable Files Requested by Server Today Number of successfully uploaded executable files: 0 Total file size uploaded: 0 Bytes</th> <th>I</th>	Universal AV Status Your computer is free from malware! Number of Infected Files 1. Currently on my PC: 0 2. I have ignored: 0 Executable Files Requested by Server Today Number of successfully uploaded executable files: 0 Total file size uploaded: 0 Bytes	I
	Disable Upload Complete Scan Retrieve Last S	can
🛒 Store 🛛 👃 Account	About A Home Copyright © SecureAge Technology. All rights	reserved.

• The last scan result will be retrieved and displayed.

SecureAPlus	Status _	×
Complete Scan Complete Scan About Conse	Scanning Results Universal AV Status Retrieving the scan result from the server Number of Infected Files 1. Currently on my PC: 0 2. I have ignored: 0 Executable Files Requested by Server Today Number of successfully uploaded executable files: 0 Total file size uploaded: 0 Bytes	2
	Disable Upload Complete Scan Retrieve Last Scan	
🛒 Store 👃 Account	About 🏠 Home Copyright © SecureAge Technology. All rights reser	ved.

5.4 View Universal AV's Log

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

• Click on View Log button.

SecureAPlus	- Status	- ×
	Scanning Results	0
Complete Scan <td>Universal AV Status Your computer is free from malware! Number of Infected Files 1. Currently on my PC: 0 2. I have ignored: 0 Executable Files Requested by Server Today Number of successfully uploaded executable files: 0 Total file size uploaded: 0 Bytes</td> <td></td>	Universal AV Status Your computer is free from malware! Number of Infected Files 1. Currently on my PC: 0 2. I have ignored: 0 Executable Files Requested by Server Today Number of successfully uploaded executable files: 0 Total file size uploaded: 0 Bytes	
	Disable Upload Complete Scan Retrieve Last Sca	n
🛒 Store 👃 Account	LockCube 🔨 About 🏠 Home Copyright © SecureAge Technology. All rights res	erved.

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

UniversalAV - Notepad	_ 0	×
File Edit Format View Help		
File Edit Format View Help 2015-08-26 09:50:34 Scan result file: C:\ProgramData\SecureAge Technology\SecureAge\Universelled: C:\ProgramData\SecureAge Technology\SecureAge\Universeled: C:\SecureAge D:0:03 8 Number of hashes: 8818	ge\Univers salAV\VsjO jojabe-465 salAV\2015 034_VsjOja c:\Progra ist\to be 034_VsjOja ed status ist\to be -support.v eAge\Whit whitelist jojabe-465 gy\SecureA ile: "C:\P	
2015-08-26 10:08:59 Waiting for search engine. 2015-08-26 10:09:00 Search engine is not running vet.		
2015-08-26 10:09:14 Search engine is running, but it is not ready to accept any re	equest yet	-
< <u> </u>	P.	

5.5 Delete Universal AV's Log

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

• Click on **Delete Log** button.

SecureAPlus	Status .	_ ×
Complete Scan Complete Scan Complete Scan Complete Scan	Scanning Results Universal AV Status Your computer is free from malware! Number of Infected Files 1. Currently on my PC: 0 2. I have ignored: 0 Executable Files Requested by Server Today Number of successfully uploaded executable files: 0 Total file size uploaded: 0 Bytes Disable Upload Complete Scan Retrieve Last Sc	an
🛒 Store 💧 Account	LockCube About A Home Copyright © SecureAge Technology. All rights re	eserved.

• The Universal AV log file contents will be deleted.

SecureAPlus	Status -	- ×
Complete Scan About Cense	Scanning Results Universal AV Status Your computer is free from malware! Numbe 1. Curren 2. I have Executa Number Total file OK	
	Enable Upload Complete Scan Retrieve Last Sca	IN
🛒 Store 👃 Account	About 🏠 Home Copyright © SecureAge Technology. All rights res	erved.

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** <u>2.1</u> for the steps to start SecureAPlus.
- In the SecureAPlus window, click on the Quarantine & History icon.

SecureAPlus v3.4.1.1			_ × _
		Interactive Mod You will be prompted w and run a program that the trusted list.	e ⁄hether to trust is not found in Change Mode ►
 ✓ Security Features: Running ✓ Software Update: Up-to-date Last Complete Scan: 2015/08/28 	Settings	Complete Scan	Quarantine & History
More details ►	Update	License Extension	P Help
Premium Trial			Enter license code
🛒 Store 👃 Account 🔒 LockCube 🔥 About		Copyright © SecureAge Tech	nology. All rights reserved.

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

😯 User Account	t Control	×		
Do you want to allow the following program to make changes to this computer?				
٢	Program name: Quaran Verified publisher: Secure File origin: Hard dr	tine Age Technology Pte Ltd ive on this computer		
Show detai	ils	Yes No		
	<u>cı</u>	ange when these notifications appear		

• The SecureAge Antivirus Quarantine & History window will launch.

🕖 SecureAge Antivirus Quarantine & History					
	ge ·			1.	
Item	File name	Date	Detected by		
Win.Trojan.Ramnit-1484	c:\\$recyde.bin\s-1-5-21-2477740147-125	2014-03-19 10:36:57	ClamAV		
Select All Unselect All]	Restore][Remove	Exit

6.1 Quarantine List

To view the quarantine list, follow the steps below:

- Start SecureAPlus. Please refer to **Section** <u>2.1</u> 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.

SecureAge Antivirus Quarantine & History	the s			
Secure Age			1.	
History Quarantine	Date	Detected by		
Ignored	2014-03-19 10:36:57	ClamAV		
Select All Unselect All	Restore		Remove	Exit

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.
SecureAPlus User Guide

	ge		. //.	
Item	File name	Date	Detected by	
<u> </u> win. Trojan. Ramnit-1484	c: \\$recycle.bin\\$-1-5-21-2477740147-125	2014-03-19 10:36:57	LiamAv	
Select All Unselect All]	Restore	Remove	Exit

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

Evit

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.

SecureAge Antivirus Quara	antine & History			
SecureAg	ge		. //:	
Quarantine	•			
Item	File name	Date	Detected by	
Win.Trojan.Ramnit-1484	c:\\$recycle.bin\\$-1-5-21-2477740147-125	2014-03-19 10:36:57	ClamAV	
Select All Unselect All]	Restore	Remove	Exit

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

) SecureAge Antivirus Quarantine & History				
		-	61	
ecure	Age		1-11-	
Duarantine	•			
Item	File name	Date	Detected by	

Copyright © SecureAge Technology Pte Ltd. All rights reserved.

6.2 History List

To view the history, follow the steps below:

- Start SecureAPlus. Please refer to **Section** <u>2.1</u> 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.

SecureAge Antivirus Quar	antine & History		6	1.	X
History History Quarantine Ignored W32.Virut.Gen.D-163 Win.Trojan.Ramnit-1484 Trojan.PDFex	C: \Users \admin \Desktop \ace. dll c: \users \admin \desktop \ece. exe c: \users \admin \desktop \ace. dll C: \Users \admin \Desktop \virus.pdf	Date 2014-01-28 09:21:02 2014-01-28 09:20:12 2013-11-21 07:46:23 2013-05-21 15:22:51	Action Quarantined Quarantined Allowed Quarantined	Detected by ClamAV ClamAV ClamAV ClamAV	Status Successful. Successful. Successful. Successful.
Select All Unselect All				Remove	Exit

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.

SecureAPlus User Guide

	antine & History			1.	X
History	▼ File name	Date	Action	Detected by	Status
Vin.Trojan.Ramnit-1484 W32.Virut.Gen.D-163 Win.Trojan.Ramnit-1484 Trojan.PDFex	C: \Users\admin\Desktop\ace.dll c: \users\admin\desktop\excel.exe c: \users\admin\desktop\ace.dll C: \Users\admin\Desktop\virus.pdf	2014-01-28 09:21:02 2014-01-28 09:20:12 2013-11-21 07:46:23 2013-05-21 15:22:51	Quarantined Quarantined Allowed Quarantined	ClamAV ClamAV ClamAV ClamAV	Successful. Successful. Successful. Successful.
	Ш				۲
Select All Unselect All]			Remove	Exit

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

SecureAge Antivirus Quara	antine & History	-lo-	-	_	
	ge		(. ,	1.	
Item	File name	Date	Action	Detected by	Status
UV32.Virut.Gen.D-163 Win.Trojan.Ramnit-1484 Trojan.PDFex	c: Jusers Jadmin Jdesktop Jexcel. exe c: Jusers Jadmin Jdesktop Jace. dll C: JUsers Jadmin JDesktop Jvirus, pdf	2014-01-28 09:20:12 2013-11-21 07:46:23 2013-05-21 15:22:51	Quarantined Allowed Quarantined	ClamAV ClamAV ClamAV	Successful. Successful. Successful.
Select All Unselect All	.m.			Remove	Exit

6.3 Ignored List

To view the ignored list, follow the steps below:

- Start SecureAPlus. Please refer to **Section** <u>2.1</u> 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.

SecureAge Antivirus Quarantine & History	
SecureAge	1.
Ignored History Quarantine Ignored	
Select All Unselect All	Remove from ignore list Exit

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.

SecureAPlus User Guide

O SecureAge Antivirus Quarantine & History	
\wedge	
SecureAge	····
[Ignored •	
File name	
(♥) c: users ladmin idesktop lace. di	
Select All Unselect All	Remove from ignore list Exit

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

SecureAge Antivirus Quarantine & History	
	///·
SecureAge	· /· ·
JeculeAge	
Ignored 🔹	
File name	
Select All Unselect All	Remove from ignore list Exit

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** <u>2.1</u> 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.

Application Whitelisting	
General Restricted Applications Trusted Certif	icate Script Status
Export whitelist to a file	Import whitelist from a file
Compact Whitelist Database	View log
	OK Cancel Apply

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.

🗐 Windows Fax and Scan
🖑 Windows Update
🛹 XPS Viewer
Accessories
퉬 Games
Maintenance
Microsoft Office
SecureAge
Application Whitelisting
SecureAPlus
🚱 Uninstall SecureAPlus
퉬 Startup
◀ Back
Search programs and files
🚱 🧭 🚞

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.

Application Whitelisting	
General Festricted Applications Trusted Certificate Script	Status
Export whitelist to a file	port whitelist from a file
Compact Whitelist Database	View log
ОК	Cancel Apply

Export whitelist to a file

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

• Click on **Export whitelist to a file...** button.

Applicatio	on Whitelisting				
General	Restricted Applications	Trusted Certifi	cate Script	Status	
	Export whitelist to a file	ə	Imp	ort whitelist from	n a file
	Compact Whitelist Data	base		View log	
			ОК	Cancel	Apply

• 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.

Application Whitelisting	
General Restricted Applications Trusted Certi	ficate Script Status
Export whitelist to a file	Import whitelist from a file
Compact Whitelist Database	View log
L	OK Cancel Apply

• 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

Applicatio	n Whitelisting		
General	Restricted Applications Trusted Certifi	cate Script Status	
	Export whitelist to a file	Import whitelist from	a file
	Compact Whitelist Database	View log	
		OK Cancel	Apply

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



SecureAPlus Compact Whitelist	_ ×
File: c:\windows\winsxs\x86_microsoft-windows-sgnt-extension-agent_3:	Lbf3\evntagnt.dll
	16%
	Cancel

<u>View Log</u>

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

• Click on **View Log** button

Application Whitelisting					
General Restricted Applications Trustee	d Certificate	Script	Status		
Export whitelist to a file		Imp	ort whitelist fr	om a file	
Compact Whitelist Database			View log	9	
		ОК	Cano	el A	pply

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

🕘 whitelist - Notepad
File Edit Format View Help
2015-08-11 09:32:27 Initial whitelist, Set trust level to 1, file c:\program files\secureag
2015-08-11 09:32:27 Logged on user: Admin
2015-08-11 09:32:29 Initial whitelist, set trust level to 2, file c:\windows\system3\sycho
2015-08-11 09:32:29 Initial whitelist, Set trust level to 2, file c:\windows\system32\sycho
2015-08-11 09:32:29 Initial whitelist, set trust level to 1, file c:\windows\system32\windows
2015-08-11 09:32:29 Initial whitefist, set trust level to 1, file c:\windows\systems2\crvnt
2015-08-11 09:32:30 Initial whitelist, set trust level to 1, file c:\windows\system32\crypt
2015-08-11 09:32:30 Initial whitelist, set trust level to 1, file c:\windows\system32\rsaen
2015-08-11 09:32:30 Initial Whitelist, Set trust level to 1, Tile C:\Windows\system32\kerne
2015-08-11 09:32:30 Initial whitelist. Set trust level to 1, file c:\windows\system22\apic
2015-08-11 09:32:30 Initial whitelist, Set trust level to 1, file c:\windows\system32\kerne
2015-08-11 09:32:30 Initial whitelist, set trust level to 1, file c:\program files\secureag
2015-08-11 09:32:30 Initial whitelist, set trust level to 1, file c:\windows\explorer.exe
2015-08-11 09:32:30 Initial whitelist, set trust level to 1, file c:\windows\system32\gdi32
2015-08-11 09:32:30 Initial whitelist, Set trust level to 1, file c:\windows\system32\user3
2015-08-11 09:32:31 Initial whitelist, set trust level to 1, file c:\windows\system32\lpk.d
2015-08-11 09:32:31 Initial whitefist, set trust level to 1, file c:\windows\system3\rasma
2015-08-11 09:32:31 Initial whitelist, set trust level to 1, file c:\windows\system32\usp10
2015-08-11 09:32:31 Initial whitelist, set trust level to 1, file c:\windows\system32\msvcr
2015-08-11 09:32:31 Initial whitelist, Set trust level to 1, file c:\windows\system32\winnin
2015-08-11 09:32:31 Initial whitefist, set trust level to 1, file c:\windows\systems2\secho
2015-08-11 09:32:32 Initial whitelist, Set trust level to 1, file c:\windows\system32\rpcrt
2015-08-11 09:32:32 Initial whitelist, set trust level to 1, file c:\windows\system32\urlmo
2015-08-11 09:32:32 Initial whitelist, set trust level to 1, file c:\windows\system32\ole32
2015-08-11 09:32:32 Initial whitelist, set trust level to 1, file c:\windows\system32\(rept
2015-08-11 09:32:32 Initial whitelist, Set trust level to 1, file c:\windows\system32\msasn
2015-08-11 09:32:33 Initial whitelist, Set trust level to 1, file c:\windows\system32\iertu +
۲ m ا

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.

plicatio	n Whitelisting				
Genera	Restricted Application	ns ¹ rusted Cer	tificate Script	Status	
The ap internet files that	plications listed below n t or removable media that at are created by these a restricted applications:	nay download, e at may potential applications will	extract, or copy fil y harm your syste not be automatic	es from external em. Hence, any ally trusted.	sources such as new executable
File n	ame				
7z.ex	e				
7zfm.	exe				
7zg.e	xe				=
acron	d32.exe				
chron	ne.exe				
clamo	d.exe				
cmd.e	exe				
dllhos	st.exe				
drago	on.exe				
excel	.exe				
explo	rer.exe				
fdm.e	xe				
firefo	c.exe				
ftp.ex	e				
git.ex	e				
lexplo	ore.exe				*
A	Add Edit	Remove			
			ОК	Cancel	Apply

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.

Application Whitelisting		X
General Restricted Applications Trusted Certific	cate Script Status	
The applications listed below may download, extr internet or removable media that may potentially h files that are created by these applications will no List of restricted applications:	act, or copy files from exte namn your system. Hence, t be automatically trusted.	ernal sources such as any new executable
File name		
7z.exe 7zfm.exe 7zg.exe acrord32.exe chrome.exe clamd.exe cmd.exe dllhost.exe dllhost.exe dragon.exe excel.exe explorer.exe fdm.exe firefox.exe ftp.exe git.exe		
iexplore.exe		-
Add Edit Remove]	
	OK Can	cel Apply
estricted Application		×
File name:		
		Browse
The file name can be a file name only, without pat	h, or a full path file name.	

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

OK

Cancel

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.

Application Whitelisting	
General Restricted Applications Trusted Certificate Script Status	
The applications listed below may download, extract, or copy files from extern internet or removable media that may potentially harm your system. Hence, an files that are created by these applications will not be automatically trusted. List of restricted applications:	al sources such as y new executable
File name	
firefox.exe	
ftp.exe	
git.exe	
iexplore.exe	
ieuser.exe	
ieinstal.exe	=
infonath exe	
msaccess exe	
mspub.exe	
notepad.exe	
notepad++.exe	
orbitdm.exe	
outlook.exe	
opera.exe	
opera64.exe	-
Add Edit Remove	
OK Cance	Apply
Restricted Application	x
File name:	
notepad.exe	Browse
The file name can be a file name only, without path, or a full path file name.	
OK	Cancel

• 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.

Application Whitelisting	
General Restricted Applications Trusted Certificate Script Status	
The applications listed below may download, extract, or copy files from exten- internet or removable media that may potentially harm your system. Hence, an files that are created by these applications will not be automatically trusted. List of restricted applications:	al sources such as y new executable
File name	*
firefox.exe	
ftp.exe	
git.exe	
iexplore.exe	
ieuser.exe	
ieinstal.exe	=
infdefaultinstall.exe	
infopath.exe	
msaccess.exe	
mspub.exe	
notepad.exe	
notepad++.exe	
orbitdm.exe	
opera 6/ eve	
uperdut.exe	*
Add Edit Remove	
OK Cance	Apply

 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.

pplication Whitelisting				×		
General Restricted Application	Trusted Certifica	te cript Stat	tus			
List of trusted certificates:						
Certificate name	Valid from	Valid To	Thumbprint			
Intel(R) Software Developme	8/28/2006	8/27/2009	42E6955A5E92	=		
Absolute Software Corp.	11/9/2006	11/10/2009	66F722F7492BF			
Acer Incorporated	9/3/2010	9/13/2013	4A83D5D989CF			
Acresso Software Inc.	3/18/2008	3/18/2011	09595DCD9CB4			
Acronis, Inc	9/3/2009	9/24/2012	023CEA9D29FE			
Acronis, Inc	8/22/2008	9/25/2009	790C2D762BF4			
Adobe Systems Incorporated	9/24/2012	10/1/2015	0DA4BF5A428C			
Adobe Systems Incorporated	9/19/2012	9/19/2013	547150A979468			
Adobe Systems Incorporated	9/5/2009	10/3/2012	A2D24C470848			
Adobe Systems Incorporated	11/5/2009	12/10/2010	C066E010388F			
Adobe Systems Incorporated	11/1/2006	12/10/2007	F02CC68ED1D5			
Adobe Systems Incorporated	12/15/2010	12/14/2012	FDF01DD3F37C			
Adobe Systems Incorporated.	11/16/2010	11/15/2012	C9278717706F1			
Adobe Systems, Incorporated	4/17/2012	4/18/2014	05EA784DF481			
Adobe Systems, Incorporated	9/19/2006	11/5/2009	39A129ABFB62			
Adobe Systems, Incorporated	10/9/2002	10/31/2003	4AC7F6FBDA79			
Adobe Systems, Incorporated	9/27/2012	9/27/2013	5E7953BBC20C			
Adobe Systems, Incorporated	9/20/2012	9/20/2013	70D566DF844F	-		
Add Remove Refresh						
		ОК	Cancel Ap	ply		

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.

0.10.1	17 F 17	V.F.I.T.	The last of the la
Certificate name	valid from	Valid 10	
Intel(R) Software Developme	8/28/2006	8/27/2009	42E6955A5E92
Absolute Software Corp.	11/9/2006	11/10/2009	66F722F7492BF
Acer Incorporated	9/3/2010	9/13/2013	4A83D5D989CF
Acresso Software Inc.	3/18/2008	3/18/2011	09595DCD9CB4
Acronis, Inc	9/3/2009	9/24/2012	023CEA9D29FE
Acronis, Inc	8/22/2008	9/25/2009	790C2D762BF4
Adobe Systems Incorporated	9/24/2012	10/1/2015	0DA4BF5A428C
Adobe Systems Incorporated	9/19/2012	9/19/2013	547150A979468
Adobe Systems Incorporated	9/5/2009	10/3/2012	A2D24C470848
Adobe Systems Incorporated	11/5/2009	12/10/2010	C066E010388F
Adobe Systems Incorporated	11/1/2006	12/10/2007	F02CC68ED1D5
Adobe Systems Incorporated	12/15/2010	12/14/2012	FDF01DD3F37C
Adobe Systems Incorporated.	11/16/2010	11/15/2012	C9278717706F1
Adobe Systems, Incorporated	4/17/2012	4/18/2014	05EA784DF481
Adobe Systems, Incorporated	9/19/2006	11/5/2009	39A129ABFB62
Adobe Systems, Incorporated	10/9/2002	10/31/2003	4AC7F6FBDA79
Adobe Systems, Incorporated	9/27/2012	9/27/2013	5E7953BBC20C
Adobe Systems, Incorporated	9/20/2012	9/20/2013	70D566DF844F 👻
Add Remove			Refresh
		ОК	Cancel Apply
0.00		x	

•	The newly	added	trusted	certificate	will	be	added	to	the	list.	Then	click	on	Apply
	button to ap	oply the	change	s made.										

Cancel

OK

Certificate validity date:

From file...

* Field must not be empty.

* Thumbprint:

1/ 1/2000 - To 1/ 1/2000 -

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

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

plication Whitelisting	T . 10			×		
General Restricted Applications Trusted Certificate Script Status						
List of trusted certificates:						
Certificate name	Valid from	Valid To	Thumbprint	-		
Intel(R) Software Developme	8/28/2006	8/27/2009	42E6955A5E92	=		
Absolute Software Corp.	11/9/2006	11/10/2009	66F722F7492BF			
Acer Incorporated	9/3/2010	9/13/2013	4A83D5D989CF			
Acresso Software Inc.	3/18/2008	3/18/2011	09595DCD9CB4			
Acronis, Inc	9/3/2009	9/24/2012	023CEA9D29FE			
Acronis, Inc	8/22/2008	9/25/2009	790C2D762BF4			
Adobe Systems Incorporated	9/24/2012	10/1/2015	0DA4BF5A428C			
Adobe Systems Incorporated	9/19/2012	9/19/2013	547150A979468			
Adobe Systems Incorporated	9/5/2009	10/3/2012	A2D24C470848			
Adobe Systems Incorporated	11/5/2009	12/10/2010	C066E010388F			
Adobe Systems Incorporated	11/1/2006	12/10/2007	F02CC68ED1D5			
Adobe Systems Incorporated	12/15/2010	12/14/2012	FDF01DD3F37C			
Adobe Systems Incorporated.	11/16/2010	11/15/2012	C9278717706F1			
Adobe Systems, Incorporated	4/17/2012	4/18/2014	05EA784DF481			
Adobe Systems, Incorporated	9/19/2006	11/5/2009	39A129ABFB62			
Adobe Systems, Incorporated	10/9/2002	10/31/2003	4AC7F6FBDA79			
Adobe Systems, Incorporated	9/27/2012	9/27/2013	5E7953BBC20C			
Adobe Systems, Incorporated	9/20/2012	9/20/2013	70D566DF844F	-		
Add Remove			Refresh	1		
		ок	Cancel Ap	ply		

 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.

Application Whitelisting				X			
General Restricted Applications	Trusted Certificat	te Script Stat	us				
List of trusted certificates:							
Certificate name	Valid from	Valid To	Thumbprint	-			
Intel(R) Software Developme	8/28/2006	8/27/2009	42E6955A5E92	=			
Absolute Software Corp.	11/9/2006	11/10/2009	66F722F7492BF				
Acer Incorporated	9/3/2010	9/13/2013	4A83D5D989CF				
Acresso Software Inc.	3/18/2008	3/18/2011	09595DCD9CB4				
Acronis, Inc	9/3/2009	9/24/2012	023CEA9D29FE				
Acronis, Inc	8/22/2008	9/25/2009	790C2D762BF4				
Adobe Systems Incorporated	9/24/2012	10/1/2015	0DA4BF5A428C				
Adobe Systems Incorporated	9/19/2012	9/19/2013	547150A979468				
Adobe Systems Incorporated	9/5/2009	10/3/2012	A2D24C470848				
Adobe Systems Incorporated	11/5/2009	12/10/2010	C066E010388F				
Adobe Systems Incorporated	11/1/2006	12/10/2007	F02CC68ED1D5				
Adobe Systems Incorporated	12/15/2010	12/14/2012	FDF01DD3F37C				
Adobe Systems Incorporated.	11/16/2010	11/15/2012	C9278717706F1				
Adobe Systems, Incorporated	4/17/2012	4/18/2014	05EA784DF481				
Adobe Systems, Incorporated	9/19/2006	11/5/2009	39A129ABFB62				
Adobe Systems, Incorporated	10/9/2002	10/31/2003	4AC7F6FBDA79				
Adobe Systems, Incorporated	9/27/2012	9/27/2013	5E7953BBC20C				
Adobe Systems, Incorporated	9/20/2012	9/20/2013	70D566DF844F	-			
Add Remove			Refresh				
		ОК	Cancel Ap	ply			

• 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.

Application Whitelisting	
General Restricted Applications Truste Script interpreter and the file extensions t	d Certificate Script Itatus
Interpreter	Extensions
cmd.exe cscript.exe java.exe javaw.exe msiexec.exe powershell.exe wscript.exe wusa.exe	.bat .cmd ijs jse .vbe .vbs .wsc .wsf .wsh .class jar jnlp .msi .ps1 .psc1 js jse .vbe .vbs .wsc .wsf .wsh .msu
Add Edit Re	move
	OK Cancel Apply

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.

Application Whitelisting					x
General Restricted Applications	Trusted Certifica	te Script	Status		
Script interpreter and the file exte	nsions that are as	sociated to t	the script:		
Interpreter	Ð	tensions			
cmd.exe	.b	at I.cmd			
cscript.exe	.js	.jse .vbe .vb	s .wsc .wsf .wsh	n	
java.exe	.C	ass .jar			
javaw.exe	.c	ass .jar			
javaws.exe	.jr	p			
msiexec.exe	n.	si			
powershell.exe	.p	s1 .psc1			
wscnpt.exe	.]5	.jsel.vbel.vb	s[.wsc[.wst[.wst	1	
wusa.exe	n.	su			
Add Edit	Remove				
	(ОК	Cancel	App	ly

SecureAPlus User Guide

Script	×
Script interpreter:	Browse
Script interpreter For example: java	can be either a file name only, without path, or a full path file name. .exe, or c:\windows\system32\java.exe
File extensions:	*
Please separate m Use '* (an asteris	ultiple extensions using ' ', for example: .exe .dll .sys <, without quote), to include all extensions.
	OK Cancel

• 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.

Application Whitelisting	
General Restricted Applications Trusted Certi Script interpreter and the file extensions that are	ficate Script Status associated to the script:
Interpreter	Extensions
cmd.exe	.bat .cmd
cscript.exe	.jsl.jsel.vbel.vbsl.wscl.wsfl.wsh
java.exe	.class .jar
javaw.exe	.class .jar
javaws.exe	jnlp
msiexec.exe	.msi
powershell.exe	.ps1l.psc1
wscript.exe	.jsl.jsel.vbel.vbsl.wscl.wsfl.wsh
wusa.exe	.msu
Add Edit Remove	
	OK Cancel Apply

Script	
Script interpreter:	cscript.exe Browse
Script interpreter ca For example: java.	an be either a file name only, without path, or a full path file name. exe, or c:\windows\system32\java.exe
File extensions:	js .jse .vbe .vbs .wsc .wsf .wsh
Please separate mu Use '*' (an asterisk,	Itiple extensions using ' ', for example: .exe .dll .sys , without quote), to include all extensions.
	OK Cancel

 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.

Application Whitelisting						
General Restricted Applications Trusted Ce	ertificate Script Status					
and eve	hatland					
cscript eve	islisel yhel yhel wech weft weh					
iava exe	dassi jar					
java.exe	classijar					
javaws.exe	inlp					
msiexec.exe	.msi					
powershell.exe	.ps1 .psc1					
wscript.exe	.jsl.jsel.vbel.vbsl.wscl.wsfl.wsh					
wusa.exe	.msu					
Add Edit Remov	e					
	OK Cancel Apply					

 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.

Application Whitelisting		
General Restricted Applications	Trusted Certificate Script Status	
Initial full system scan:	Done (2014-07-04 08:43:25).	
Application whitelisting service:	Running.	
Application whitelisting driver:	Running.	
	UK Cano	Appiy

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.

🐼 setup64.exe		4/10/2013.8:21.PM	Ar	pilic .	
•		Open		Þ	
ate modified: 4/10/2013	۲	Run as administrator			
Size: 2.37 MB		Troubleshoot compatibility			
	6	Scan "setup64.exe"			
		Trust Level	►	\checkmark	Trusted Application
		Show all trust level			Trusted Installer
Y		Share with	×		Not Trusted

 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.

SA		Open
		Share with Restore previous versions Include in library
		Scan "SA" Trust Level →
		Show all trust level
	(() () ()	Add to archive Add to "SA.rar" Compress and email Compress to "SA.rar" and email
		Send to
		Copy Create shortcut Delete
		Rename Properties

SecureAPlus User Guide

cureAge Application Whitelistir	ng		
Filename	Full path filename	Trust level	
readme.txt	c: \users \windows7en	1 (Trusted application)	
sa.ico	c:\users\windows7en	0 (Not trusted)	
saconfig.ini	c:\users\windows7en	0 (Not trusted)	
sage50014.exe	c:\users\windows7en	1 (Trusted application)	
sage_cacert.der	c:\users\windows7en	1 (Trusted application)	
secureage installation guide.pdf	c:\users\windows7en	0 (Not trusted)	
secureageca 1.crl	c:\users\windows7en	1 (Trusted application)	
securedata admin guide.pdf	c:\users\windows7en	0 (Not trusted)	
securedatacfg.exe	c:\users\windows7en	1 (Trusted application)	
securedata_2pp.pdf	c:\users\windows7en	0 (Not trusted)	
setup.exe	c:\users\windows7en	1 (Trusted application)	
			ОК

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 <u>7.2.1</u> 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 <u>7.2.3</u> 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 <u>untrusted</u> executable file is being run and it is being launched by <u>Windows Explorer</u>, Application Whitelisting will notify for further actions as below:

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



Vote:

- 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 <u>unsigned</u> files which are <u>not trusted</u> 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.

SecureAge Application Whitelisting
SecureAge
Untrusted: winwordc.exe
This file is not signed.
Universal AV status: Clean
The file is blocked. Do you want to unblock?
Unblock Block More >>

 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.

SecureAge Application Whitelisting
SecureAge
Untrusted: wwlibc.dll
Unable to verify digital signature.
The file is blocked. Do you want to unblock?
Unblock Block << Less
The above file is launched by the following process: winwordc.exe (PID: 7744) Remember my answer for this entire process.

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



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 <u>trusted applications</u> 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.

SecureAge Application Whitelisting
SecureAge
Process: 7z938.exe (pid: 4848) This process is not signed.
Universal AV status: Clean
This process seems to be performing installation. Do you want to trust this process as a trusted installer?
Yes No << Less
Do this for this session only.
Note: An executable file has just been created by this process. By setting this process as a trusted installer, all the executable files, which are created by this process, will be automatically trusted.
This process is not an installer. Remember my answer permanently.
The executable file that was created by this process:
7z.dl
This file is not signed.
Universal AV status: Clean
Trust this file only. Do not set the process as a trusted installer.

- 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 <u>7.2</u> – 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.
Vote:

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.

•	Open Run as administrator Troubleshoot compatibility Scan "7z938.exe"			
	Trust Level	•		Trusted Application
	Share with	×	~	Trusted Installer
	Pin to Taskbar			Not Trusted
	Pin to Start Menu			
	Restore previous versions			
	Send to	•		
	Cut			
	Cut			
	Сору			
	Copy Create shortcut			
	Copy Create shortcut Delete			

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 <u>not trusted</u> with <u>no hashes exist in the Universal AV</u> and are being executed, Application Whitelisting will notify for further actions as below:



- ► 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.

SecureAge Application Whitelisting	
SecureAge	
Untrusted script: test.bat	
No digital signature.	
VirusTotal: Unknown	Send to VirusTotal
The file is blocked. Do you want to unblock? Unblock Block More >>	



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

SecureAge Application Whitelisting	
SecureAge	
Untrusted script: test.bat	
No digital signature.	
VirusTotal detection ratio: 0/55	
The file is blocked. Do you want to unblock?	
Unblock Block More >>	

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.

bare with		
Restore previous versions	•	
nclude in library Scan "SecureAge"	•	
Frust Level	+	Trusted Application
ihow all trust level Add to archive Add to "SecureAge.rar" Compress and email Compress to "SecureAge.rar" and email		Trusted Installer Not Trusted
iend to Cut Copy Create shortcut	•	
	Add to archive Add to archive Compress and email Compress to "SecureAge.rar" and email Compress to "SecureAge.rar" and email Compress to archive Compress to "SecureAge.rar" and email Compress to a social and email and email Compress to a social and email and email Compress to a social and email	Add to archive Add to archive Compress and email Compress to "SecureAge.rar" and email Seend to Cut Copy Create shortcut Delete

 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.

cureAge Application V	Vhitelisting		
Filename	Full path filename	Trust level	
sawhitelist.dat secureaplussetup.exe	c: \users \sijie \desktop \secu c: \users \sijie \desktop \secu	1 (Trusted application) 1 (Trusted application)	
			ОК

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:

📀 Scan complete. No threats detected.

 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.

SecureAPlus User Guide

me elapsed: 00:00:06				ОК
les scanned: 33			<	<less< th=""></less<>
umber of program files unknow	in to Universal AV: 0			
Scan complete. 8 threat(s)	detected			
Virus name	File name	Detected by	Action taken	Status
Trojan.DyrezaKD.2195	C:\Users\John\Desktop\Office Files\	Emsisoft, McAfee, AVG, BitDefender, ESET, Norman		
Backdoor.Win32.Andro	C:\Users\John\Desktop\Office Files\	Emsisoft, McAfee, AVG, BitDefender, ESET, Norman		
Trojan.MSIL.Injector (A)	C:\Users\John\Desktop\Office Files\	Emsisoft, McAfee, AVG, BitDefender, ESET, QuickHeal		
Backdoor.Win32.Andro	C:\Users\John\Desktop\Office Files\	Emsisoft, McAfee, AVG, BitDefender, ClamAV, ESET		
Trojan-Downloader.Win	C:\Users\John\Desktop\Office Files\	Emsisoft, McAfee, BitDefender, ClamAV, ESET, Quic		
Trojan.Win32.Agent (A)	C:\Users\John\Desktop\Office Files\	Emsisoft, McAfee, BitDefender, ESET, Norman, Quic		
Trojan.GenericKD.2194	C:\Users\John\Desktop\Office Files\	Emsisoft, McAfee, AVG, BitDefender, ESET, Norman		
Trojan.Win32.Injector (A)	C:\Users\John\Desktop\Office Files\	Emsisoft, McAfee, AVG, BitDefender, ESET, Quid:H		

• Choose Quarantine or Remove the infected files.

ine elected 00.00.06						ОК
me elapsed: 00:00:06						
iles scanned: 33					<	<less< td=""></less<>
lumber of program files unknov	vn to Univer	sal AV: 0				
Scan complete. 8 threat(s)	detected					
Virus name	File name	Detected by			Action taken	Status
Trojan.DyrezaKD.2195	C:\Users\	SecureAPlus Virus Scapper	- 23 -	fender, ESET, Norman	Remove	Succe
Backdoor.Win32.Andro	C:\Users\			ender, ESET, Norman	Remove	Succe
Trojan.MSIL.Injector (A)	C:\Users\			fender, ESET, QuickHeal	Remove	Succe
Backdoor.Win32.Andro	C:\Users\	All selected items are successfully rer	moved.	fender, ClamAV, ESET	Remove	Succe
Trojan-Downloader.Win	C:\Users\	· · · · · · · · · · · · · · · · · · ·		, ClamAV, ESET, Quic	Remove	Succe
Trojan.Win32.Agent (A)	C: Users			, ESET, Norman, Quic	Remove	Succe
Trojan.GenericKD.2194	C: Users	·	04	fender, ESET, Norman	Remove	Succe
Trojan.Win32.Injector (A)	C:\Users\	۱	UK	fender, ESET, QuickH	Remove	Succe
				9		
					1	

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** <u>4.31</u> 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** <u>4.31</u> 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