impero education pro

Sophos Anti-Virus and EdPro Chrome Browser extension guide Impero Education Pro 2017 KBA-01331-K1Q0R7

DISCLAIMER - Any changes made as outlined are carried out as your own risk, we cannot accept responsibility for any System & Network changes made and outcomes thereafter. We have tested the following scenarios within this guide with no issues. If you are unsure we recommend that you apply the following changes in an isolated environment as this is not our software. Sophos have confirmed the steps below do not present a security risk to end users using Sophos products



Introduction

It has been reported that when using the Impero Education Pro Chrome Browser extension in combination with a Sophos anti-virus installation this could lead to EdPro **NOT** logging or blocking content.

This can be seen within the chrome console for the background page, evidenced by an error connecting to localhost. In combination with Sophos we have agreed the process below to rectify the issue, without presenting any security risk to end users of Sophos Anti-Virus.

Sophos client application

<u>Step 1</u>

Open the Sophos Enterprise Console and navigate to Anti-Virus and HIPS** (Bottom Left) and right Click and select View/Edit Policy;

🖓 📿 Updating			
Anti-virus and HIPS			
····· <mark>P Def</mark>	Create Policy		
Applica Applica Data co Device	Rename Policy		
	Duplicate Policy		
	View/Edit Policy		
⊡ (∕) Tampe —	Delete Policy		
Hold Rep Co	View Groups Using Policy		
	Reset Policy to Factory Defaults		

Please see the Additional Information section at the bottom for further information ******

<u>Step 2</u>

In the Policy window, you will need to select the Authorization button at the top, which will open another window;

	rus and HIPS Policy - Default
Authorization	ı
Messaging.	
Sophos Live Prote	ection
On-access scanning	
Enable on-access	scanning Configure
Enable behavior r	nonitoring Configure
Web protection	
lock access to malici	ious websites: On 🗸
Download scanning:	As on-access scanning V
Scheduled scanning	
Set up and manage s	scheduled scans:
Name 🎝 New scheduled :	scan
Add	Edit Remove
Add Extensions and Exc	Edit Remove
Add Extensions and Exc Changes to "Exclusio system scan" and de computers.	Edit Remove dusions ns" or "Extensions" settings also affect the "Full fault on-demand scans on the individual
Add Extensions and Exc Changes to "Exclusio system scan" and de computers.	Edit Remove dusions ons" or "Extensions" settings also affect the "Full fault on-demand scans on the individual

<u>Step 3</u>

Within the Authorization Manager you will need to navigate to the Websites tab and click the add button.

	Anti-Vir	us and HIP	S Policy - De	fault X]
	Authorization.				
	Αι	uthorizatio	n Manager	×	
	Adware and DU	A.c.	Puffer	Querflow	
	Suspicious Files	Suspicio	us Behavior	Websites	1
	Ta annuart bladúar af a		ومسال معر لرام معر	,	
w:	address to the list of au	thorized webs	ites by clicking 'Ad	ld'.	
tu:	Authorized websites:				
m				Add	
: 16					
A				Edit	
A				Remove	
A					
A					
A					
A					
R					
в					
D	The "Authorized website	s" setting app	lies only to Windo	ws.	
D					
D b			OK	Cancel	
					:
DH	computers.				Y
DH			ОК	Cancel	D
DH4					Y

Step 4

Once clicking the add button you will need to select the IP Address Radio button and enter the following 127.0.0.1 and click okay.

	Anti-Virus and HIPS Policy - Default		
	Authorization		
	Authorization Manager 🛛 🗶		
	Adware and PUAs Buffer Overflow		
	Suspicious Files Suspicious Behavior Websites		
View:	Add an Authorized Website		
Status	Address format:		
Com			
A 🖉	○ IP address with subnet mask		
⊐ ø A	● IP address		
⇒× A ■× A	Example: 192.168.0.1		
A	127 . 0 . 0 . 1		
≕ A ⊒ s A			
X A			
l ⇒ x Al	OK Cancel		
🖳 ві			
D D	The "Authorized websites" setting applies only to Windows.		
- X D			
S D	OK Cancel		
S DH3	computers.		
💐 DH:	OK Cancel		

Additional Information

** This will need to be applied to every Anti-Virus and HIPS Policies that you have setup, which can be seen in Step 1.

Sophos Central

Step 1

Login to the Central website and add the settings to the Global Scanning Exclusions.

You can add this setting in the Global Scanning Exclusions for Sophos:

Go to Global Settings > Global Scanning Exclusions



<u>Step 2</u>

Add a New scanning exclusion. Make sure that the type is set to "Website" and add 127.0.0.1 as the IP address. You can add a comment as well if you wish.

This Website Has Been B × Sophos Central ×					
← → C Sophos Ltd. [GB] https://central.sophos.com/manage/config/settings/scanning-exclusions					
SOPHOS	ImperoServer.exe File or folder (W	Real-time and scheduled	Real-time and scheduled		
Admin	ImperoServerBn File or folder (W	Edit Scanning Exclusion ×			
Overview	ImperoServerSV File or folder (W	EXCLUSION TYPE Website (Windows/Mac)			
Alerts	ImperoUtilities .e File or folder (W	VALUE * (IP ADDRESS) [127.0.0.1]			
💾 Logs & Reports	ImperoWinlogon	You can exclude a domain name or IP address (e.g. google.com, 192.168.0.1)			
📌 People	File or folder (W	COMMENT			
🖵 Devices	lnssatt.exe File or folder (W	Impero Chrome Extension			
🗱 Global Settings	lnsscomm.exe				
Protect Devices	File or folder (W				
MY PRODUCTS	mantle.exe File or folder (W	Update Cancel			
Endpoint Protection	NRControlViewer.	dll Real-time and scheduled			
Server Protection	File or folder (Win	dows)			
SOPHOS CENTRAL	update.exe File or folder (Win	dows)			
Explore Products	127.0.0.1 Website (Windows	s/Mac)	Impero Chrome Extension		

Step 3

Make sure that once you have added this exclusion, you click Save at the top of the page. You may need to restart the Chrome browser for the extension to start working once this change has been made.

SOPHOS CENTRAL Admin	Global Scanning Exclusions System Settings / Global Scanning Exclusions	Help 🕶	
Overview			Save Cancel
Dashboard	Exclude files, websites and applications from scanning	g for threats.	
Alerts	Note: These exclusions will apply to all your users (an	d their computers) and servers. If you want them to appl	ly only to certain users or servers, use the scanning exclusions
🟥 Logs & Reports	in the policies instead.		
👤 People			Add Exclusion
Devices	EXCLUDE	ACTIVE FOR	COMMENT
Global Settings	C:\Program Files (x86)\GFI\LanGuard 11 Agent\ File or folder (Windows)	Real-time and scheduled	
▲ Protect Devices	C:\Program Files (x86)\Impero Solutions Ltd\ File or folder (Windows)	Real-time and scheduled	×
Endpoint Protection	C:\Program Files\GFI\LanGuard 11 Agent\ File or folder (Windows)	Real-time and scheduled	- <u>*</u> :
Server Protection	C:\Program Files\Impero Solutions Ltd\ File or folder (Windows)	Real-time and scheduled	×
SOPHOS CENTRAL Explore Products	httpd.exe File or folder (Windows)	Lating and the second s	×
	imperoclient.exe File or folder (Windows)	the second secon	×

info@imperosoftware.com www.imperosoftware.co.uk www.imperosoftware.com +44 (0) 1509 611341 UK 877-883-4370 USA