Sangfor IAG

Anti-proxy and ES Correlation Configuration Guide

Product Version	13.0.19
Document Version	01
Released on	Sep. 23, 2021

Disclaimer

Products, services or features described in this document, whether wholly or in part, may be not within your purchase scope or usage scope. The products, services or features you purchase must be subject to the commercial contract and terms as agreed by you and Sangfor. Unless otherwise provided in the contract, Sangfor disclaims warranties of any kind, either express or implied, for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Unless otherwise agreed, this document is used for reference only, and all statements, information, and recommendations therein do not constitute any express or implied warranties.

Technical Support

For technical support, please visit: https://www.sangfor.com/en/about-us/contact-us/technical-support

Send information about errors or any product related problem to tech.support@sangfor.com.

About This Document

This document describes the anti-proxy IAG and ES correlation Configuration Guide.

Intended Audience

This document is intended for:

- Network design engineers
- O&M personnel

Note Icons

English Icon	Description
⚠DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
⚠WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
⚠CAUTION	Indicates a hazardous situation, which if not avoided, could result in minor or moderate injury.
⚠NOTICE	Indicates a hazardous situation, which if not avoided, could result in settings failing to take effect, equipment damage, or data loss. NOTICE addresses practices not related to personal injury.
NOTE	Calls attention to important information, best practices, and tips. NOTE addresses information not related to personal injury or equipment damage.

Change Log

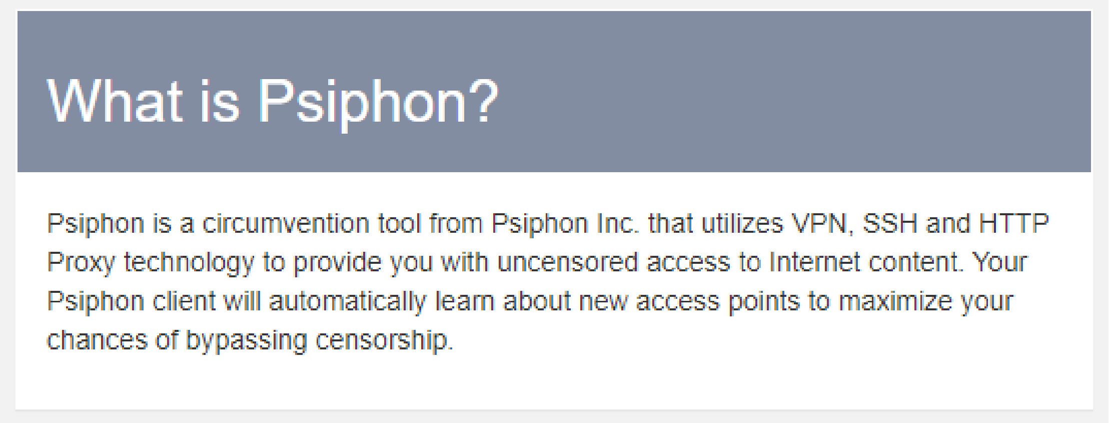
Date	Change Description
Sep. 23, 2021	This is the first release of this document.

Contents

1 Introduction

Many users use VPN tools to access applications that are not allowed by network administrators, such as pornographic websites and the dark web. In addition, the use of VPN tools can lead to information leakage and behaviors that cannot be audited. For network administrators, these VPN tools need to be blocked.

Traditionally, the general anti-proxy method blocks the domain name and IP associated with the proxy tool in the dimension of network traffic, but the effect is usually minimal. As some proxy software tools claim, the traffic is disguised as standard SSH, HTTP Protocol, and DNS protocol to bypass the detection of security software. Some proxy software deployed on the server on the public cloud, blocking its IP will cause the normal website to be blocked. Therefore, we need a better way to prevent proxy tools, through the linkage of IAG and ES, directly block the operation of proxy tools related processes.



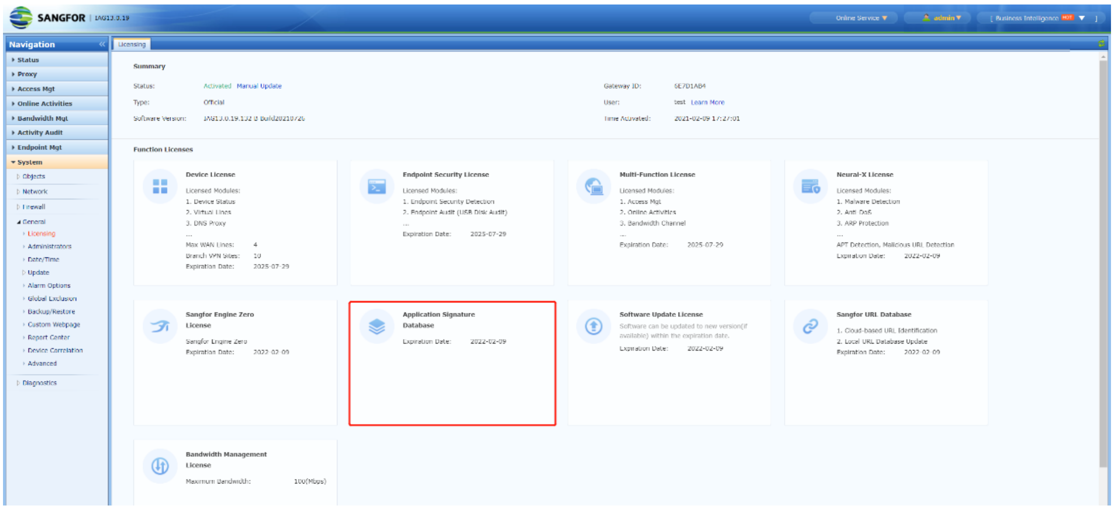
What is Psiphon?

Psiphon is a circumvention tool from Psiphon Inc. that utilizes VPN, SSH and HTTP Proxy technology to provide you with uncensored access to Internet content. Your Psiphon client will automatically learn about new access points to maximize your chances of bypassing censorship.

2 Configure Policy in IAG

2.1 Check License and Database

1. Check whether IAG has enabled application control License. The Anti Proxy function needs to use the application control rule base, which requires the relevant authorization to be turned on.



Summary

Status: Activated Manual Update

Type: Official

Software Version: IAG13.0.19.132 B Build20210726

Gateway ID: 5E7D1AB4

User: test Learn More

Time Activated: 2021-02-09 17:27:01

Function Licenses

Device License
Licensed Modules:
1. Device Status
2. Virtual Lines
3. DNS Proxy
...
Max WAN Lines: 4
Branch VPN Sites: 10
Expiration Date: 2025-07-29

Endpoint Security License
Licensed Modules:
1. Endpoint Security Detection
2. Endpoint Audit (USB Disk Audit)
...
Expiration Date: 2025-07-29

Multi-Function License
Licensed Modules:
1. Access Mgt
2. Online Activities
3. Bandwidth Channel
...
Expiration Date: 2025-07-29

Neural-X License
Licensed Modules:
1. Malware Detection
2. Anti DoS
3. ARP Protection
...
APT Detection, Malicious URL Detection
Expiration Date: 2022-02-09

Sangfor Engine Zero License
Sangfor Engine Zero
Expiration Date: 2022-02-09

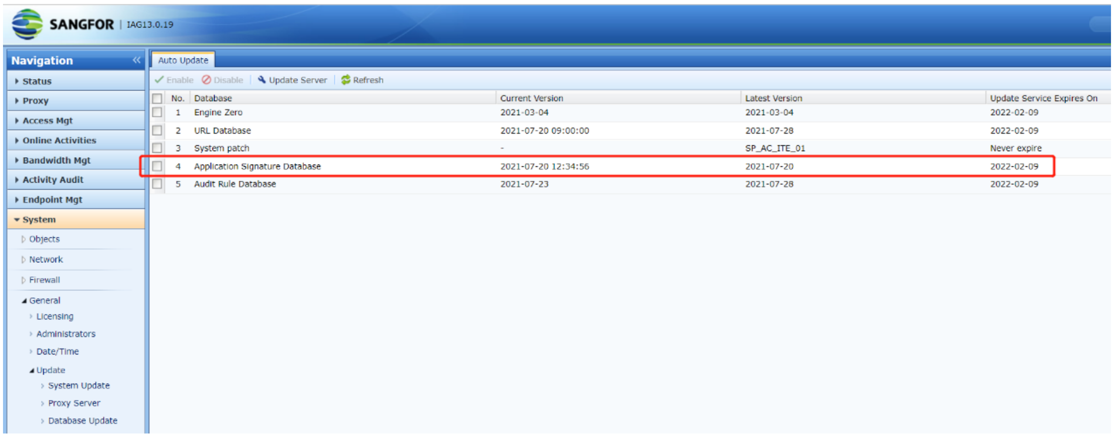
Application Signature Database
Expiration Date: 2022-02-09

Software Update License
Software can be updated to new version(if available) within the expiration date.
Expiration Date: 2022-02-09

Sangfor URL Database
1. Cloud-based URL Identification
2. Local URL Database Update
Expiration Date: 2022-02-09

Bandwidth Management License
Maximum Bandwidth: 100(Mbps)

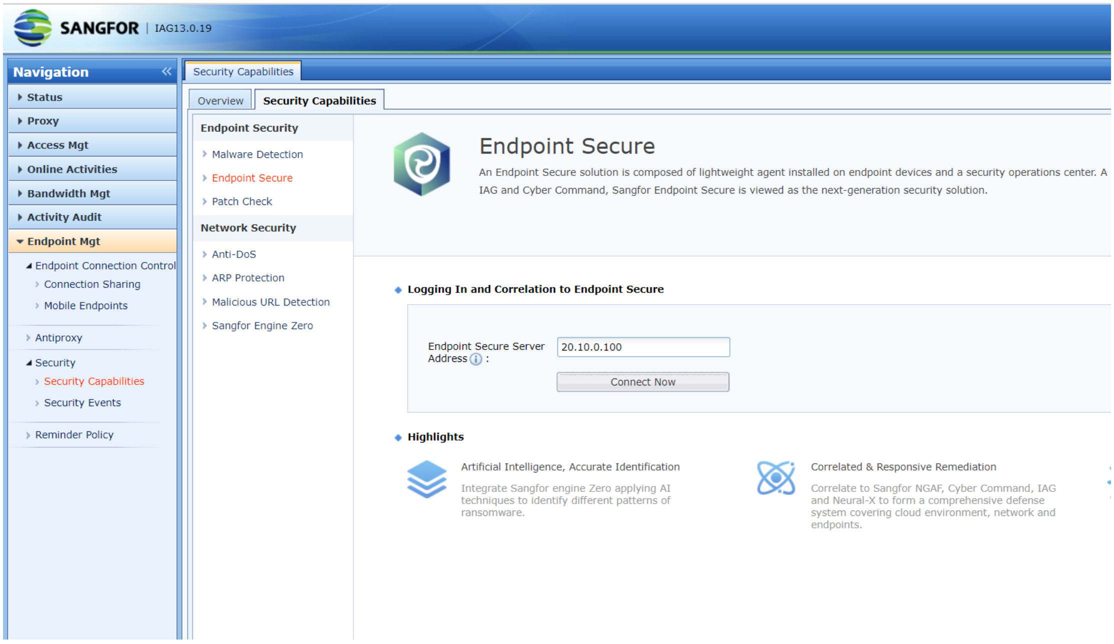
2. Check whether the rule database has been updated to the latest date. The latest rule database will help to achieve a better Anti Proxy effect.



□	No.	Database	Current Version	Latest Version	Update Service Expires On
□	1	Engine Zero	2021-03-04	2021-03-04	2022-02-09
□	2	URL Database	2021-07-20 09:00:00	2021-07-28	2022-02-09
□	3	System patch	-	SP_AC_ITE_01	Never expire
□	4	Application Signature Database	2021-07-20 12:34:56	2021-07-20	2022-02-09
□	5	Audit Rule Database	2021-07-23	2021-07-28	2022-02-09

2.2 Correlate IAG with Endpoint Secure

1. Connect IAG to Endpoint Secure.



Endpoint Secure

An Endpoint Secure solution is composed of lightweight agent installed on endpoint devices and a security operations center. A IAG and Cyber Command, Sangfor Endpoint Secure is viewed as the next-generation security solution.

Logging In and Correlation to Endpoint Secure

Endpoint Secure Server Address: 20.10.0.100

Highlights

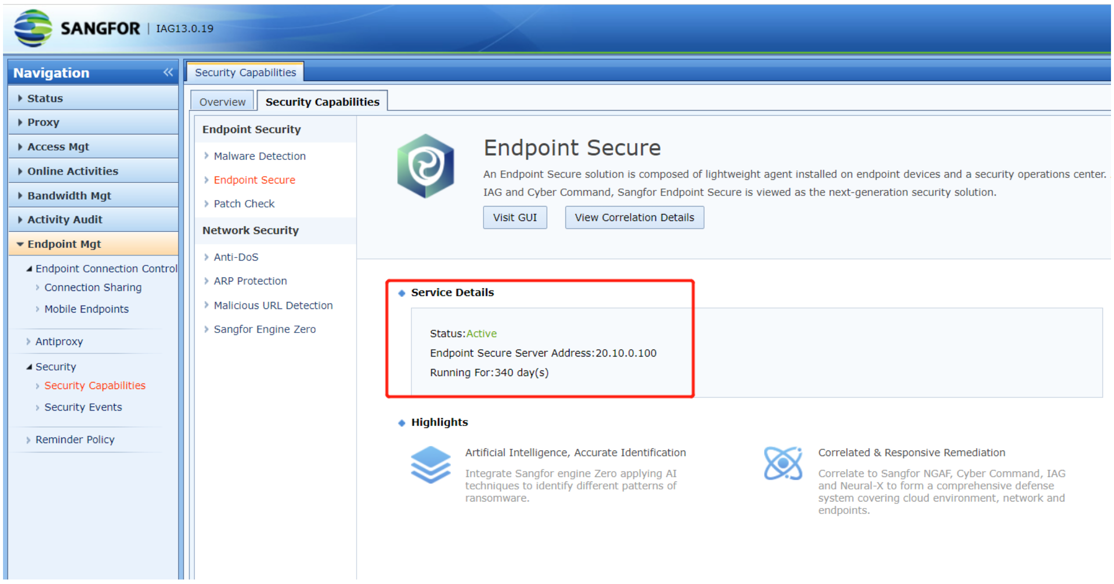
Artificial Intelligence, Accurate Identification

Integrate Sangfor engine Zero applying AI techniques to identify different patterns of ransomware.

Correlated & Responsive Remediation

Correlate to Sangfor NGAF, Cyber Command, IAG and Neural-X to form a comprehensive defense system covering cloud environment, network and endpoints.

2. If IAG correlates with Endpoint Secure successfully, you can view the endpoints in IAG and the connection status.



Endpoint Secure

An Endpoint Secure solution is composed of lightweight agent installed on endpoint devices and a security operations center. IAG and Cyber Command, Sangfor Endpoint Secure is viewed as the next-generation security solution.

Service Details

Status:Active

Endpoint Secure Server Address:20.10.0.100

Running For:340 day(s)

Highlights

Artificial Intelligence, Accurate Identification

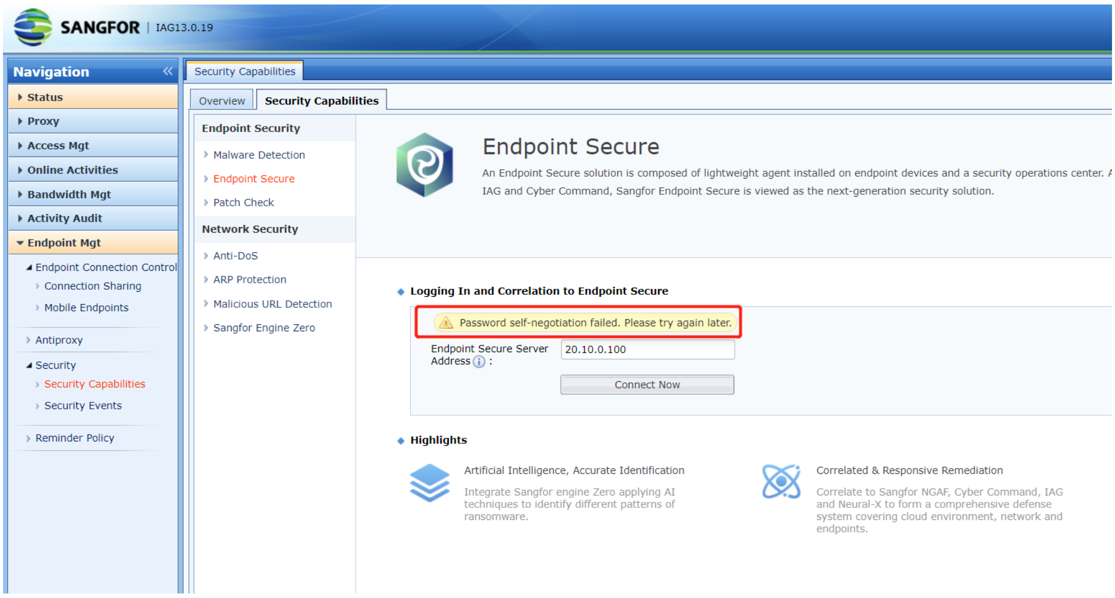
Integrate Sangfor engine Zero applying AI techniques to identify different patterns of ransomware.

Correlated & Responsive Remediation

Correlate to Sangfor NGAF, Cyber Command, IAG and Neural-X to form a comprehensive defense system covering cloud environment, network and endpoints.

2.2.1 Precaution on IAG connect to ES

1. When IAG connects to Endpoint Secure, the following error message may appear. It is because the device access permission is not enabled on Endpoint Secure.



Endpoint Secure

An Endpoint Secure solution is composed of lightweight agent installed on endpoint devices and a security operations center. A

IAG and Cyber Command, Sangfor Endpoint Secure is viewed as the next-generation security solution.

Logging In and Correlation to Endpoint Secure

Password self-negotiation failed. Please try again later.

Endpoint Secure Server Address ⓘ : 20.10.0.100

Highlights

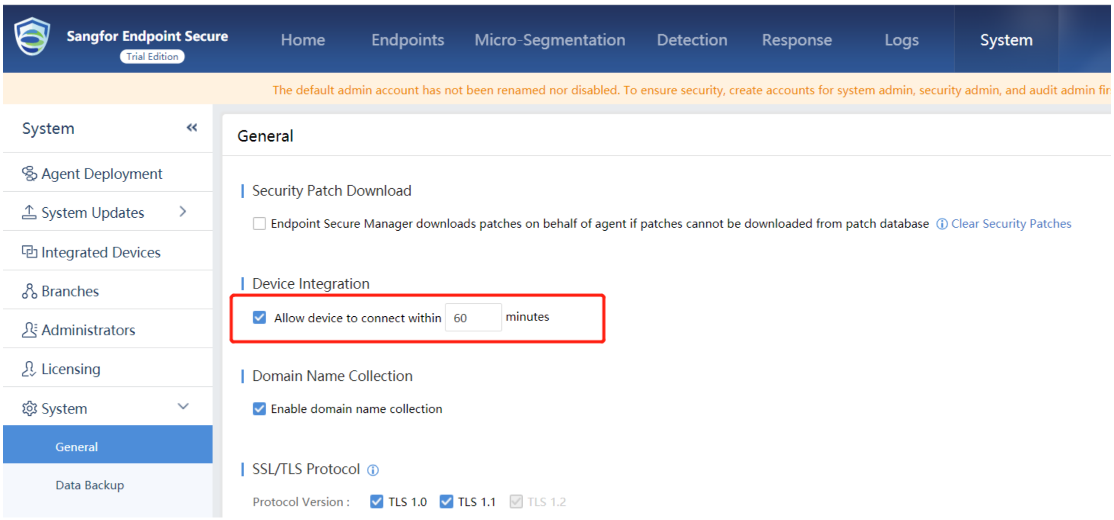
Artificial Intelligence, Accurate Identification

Integrate Sangfor engine Zero applying AI techniques to identify different patterns of ransomware.

Correlated & Responsive Remediation

Correlate to Sangfor NGAF, Cyber Command, IAG and Neural-X to form a comprehensive defense system covering cloud environment, network and endpoints.

2. It requires enabling the **Device Integration** option on Endpoint Secure.



The default admin account has not been renamed nor disabled. To ensure security, create accounts for system admin, security admin, and audit admin fir

General

Security Patch Download

□ Endpoint Secure Manager downloads patches on behalf of agent if patches cannot be downloaded from patch database

Device Integration

☑ Allow device to connect within 60 minutes

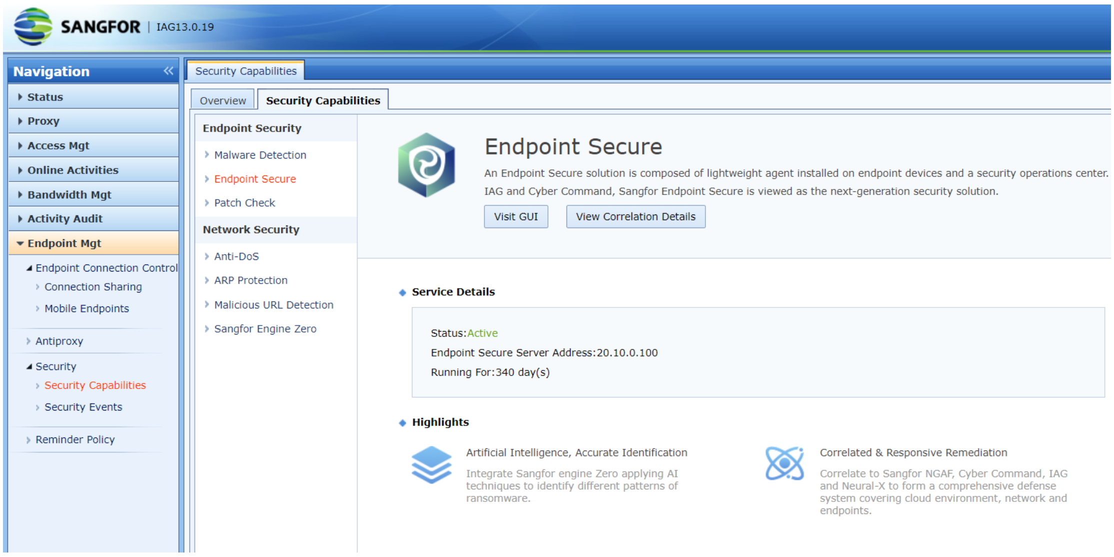
Domain Name Collection

☑ Enable domain name collection

SSL/TLS Protocol ⓘ

Protocol Version : ☑ TLS 1.0 ☑ TLS 1.1 ☑ TLS 1.2

3. Then access **Endpoint Secure** from IAG.



Endpoint Secure

An Endpoint Secure solution is composed of lightweight agent installed on endpoint devices and a security operations center. IAG and Cyber Command, Sangfor Endpoint Secure is viewed as the next-generation security solution.

Service Details

Status:Active
Endpoint Secure Server Address:20.10.0.100
Running For:340 day(s)

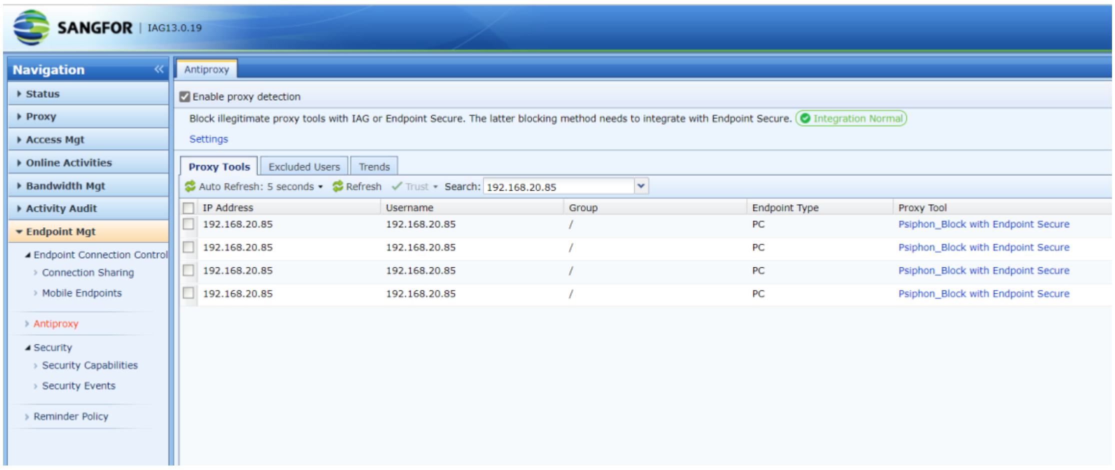
Highlights

Artificial Intelligence, Accurate Identification
Integrate Sangfor engine Zero applying AI techniques to identify different patterns of ransomware.

Correlated & Responsive Remediation
Correlate to Sangfor NGAF, Cyber Command, IAG and Neural-X to form a comprehensive defense system covering cloud environment, network and endpoints.

2.3 Configure Endpoint App Control Policy

1. Navigate to **Endpoint Mgt** Page and go to **Antiproxy** module, click Enable Proxy Detection.



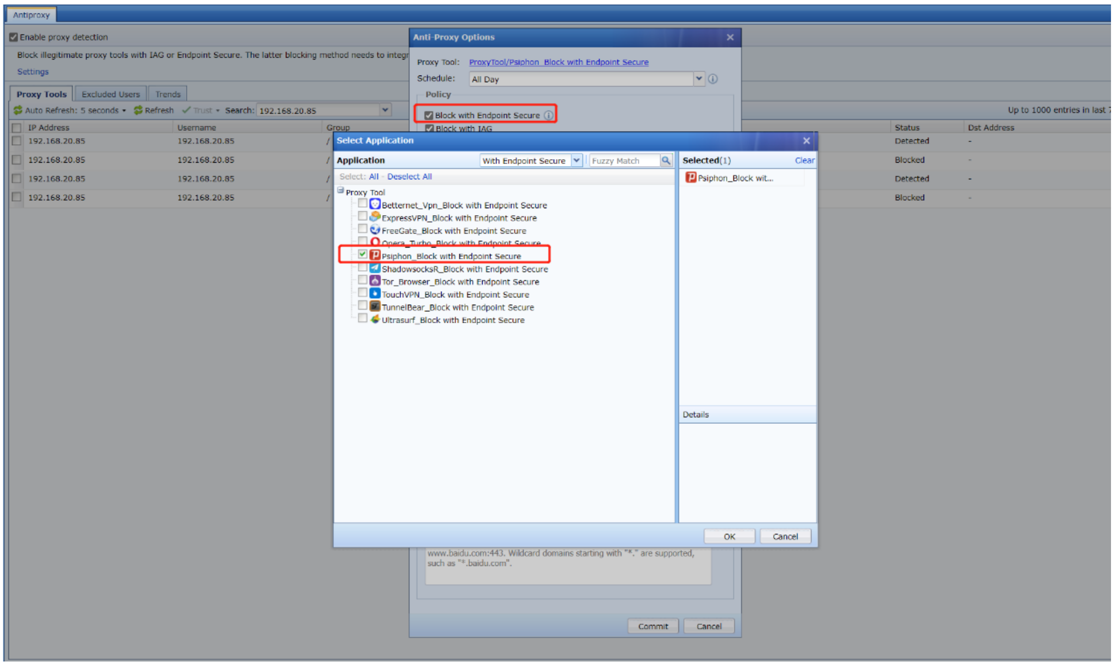
☑ Enable proxy detection

Block illegitimate proxy tools with IAG or Endpoint Secure. The latter blocking method needs to integrate with Endpoint Secure. ✓ Integration Normal

Search: 192.168.20.85

□	IP Address	Username	Group	Endpoint Type	Proxy Tool
□	192.168.20.85	192.168.20.85	/	PC	Psiphon_Block with Endpoint Secure
□	192.168.20.85	192.168.20.85	/	PC	Psiphon_Block with Endpoint Secure
□	192.168.20.85	192.168.20.85	/	PC	Psiphon_Block with Endpoint Secure
□	192.168.20.85	192.168.20.85	/	PC	Psiphon_Block with Endpoint Secure

2. Select the App that you want to block.



☑ Enable proxy detection

Block illegitimate proxy tools with IAG or Endpoint Secure. The latter blocking method needs to integr

Search: 192.168.20.85

Up to 1000 entries in last 7

IP Address	Username	Group	Status	Dst Address
192.168.20.85	192.168.20.85	/	Detected	-
192.168.20.85	192.168.20.85	/	Blocked	-
192.168.20.85	192.168.20.85	/	Detected	-
192.168.20.85	192.168.20.85	/	Blocked	-

Anti-Proxy Options

Proxy Tool: ProxyTool/Psiphon_Block with Endpoint Secure

Schedule: All Day

Policy

☑ Block with Endpoint Secure

☑ Block with IAG

www.baidu.com:443. Wildcard domains starting with "*." are supported, such as "*.baidu.com".

Select Application

Application: With Endpoint Secure | Fuzzy Match

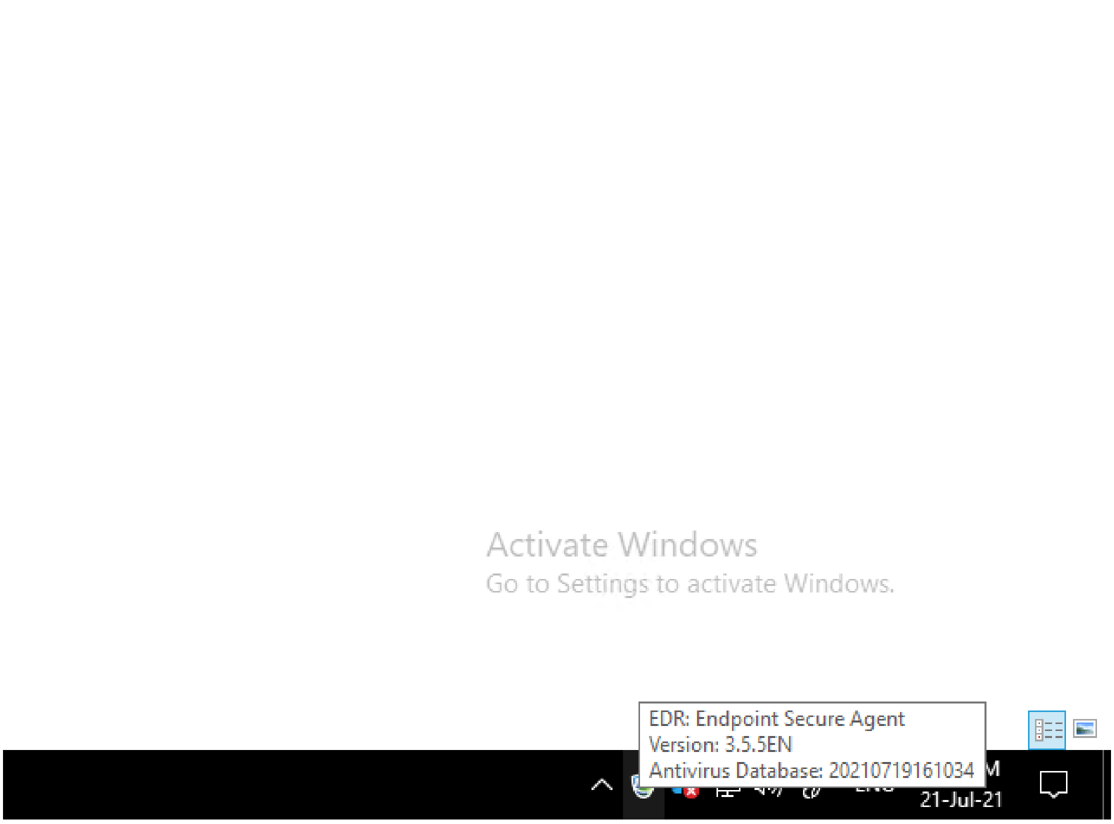
Proxy Tool

- □ Betternet_Vpn_Block with Endpoint Secure
- □ ExpressVPN_Block with Endpoint Secure
- □ FreeGate_Block with Endpoint Secure
- □ Opera_Turbo_Block with Endpoint Secure
- ☑ Psiphon_Block with Endpoint Secure
- □ ShadowsocksR_Block with Endpoint Secure
- □ Tor_Browser_Block with Endpoint Secure
- □ TouchVPN_Block with Endpoint Secure
- □ TunnelBear_Block with Endpoint Secure
- □ Ultrasurf_Block with Endpoint Secure

Selected(1): Psiphon_Block wit...

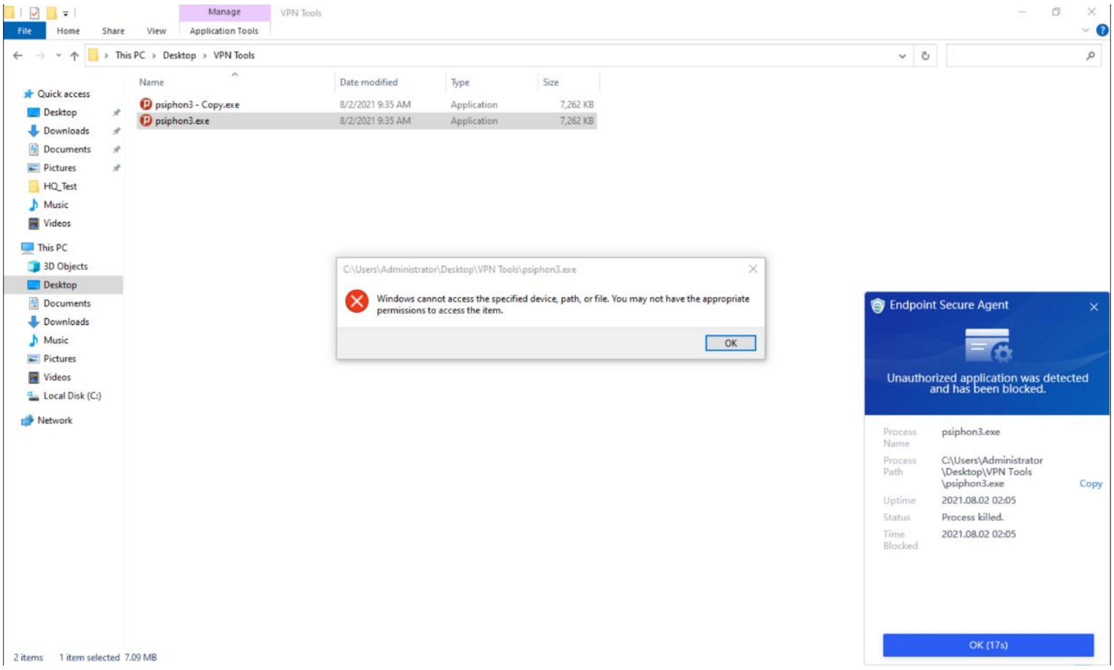
2.4 Run Proxy Tools on PC

1. It is required to ensure the PC's Endpoint Secure Agent is running.



EDR: Endpoint Secure Agent
Version: 3.5.5EN
Antivirus Database: 20210719161034

2. Run the Proxy tool. You can see that the Proxy tool cannot run Endpoint Secure Agent and displays warning information.



Name	Date modified	Type	Size
psiphon3 - Copy.exe	8/2/2021 9:35 AM	Application	7,262 KB
psiphon3.exe	8/2/2021 9:35 AM	Application	7,262 KB

C:\Users\Administrator\Desktop\VPN Tools\psiphon3.exe

Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item.

Endpoint Secure Agent

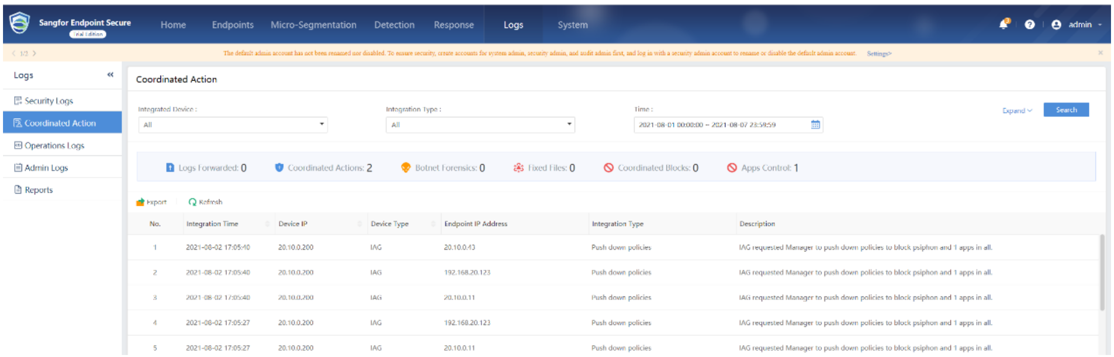
Unauthorized application was detected and has been blocked.

Process Name	psiphon3.exe
Process Path	C:\Users\Administrator\Desktop\VPN Tools\psiphon3.exe
Uptime	2021.08.02 02:05
Status	Process killed.
Time Blocked	2021.08.02 02:05

3 View Logs

3.1 View Agent Logs in MGR

1. You can see the **Coordinated Action Logs** of the IAG policy in the **ES MGR log**.



The default admin account has not been renamed nor disabled. To ensure security, create accounts for system admin, security admin, and audit admin first, and log in with a security admin account to rename or disable the default admin account. Settings>

Coordinated Action

Integrated Device : All

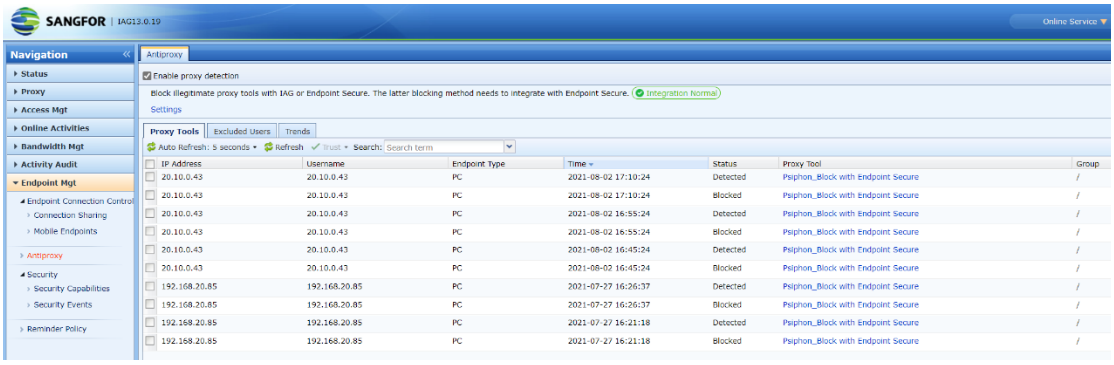
Integration Type : All

Time : 2021-08-01 00:00:00 ~ 2021-08-07 23:59:59

Logs Forwarded: 0 Coordinated Actions: 2 Botnet Forensics: 0 Fixed Files: 0 Coordinated Blocks: 0 Apps Control: 1

No.	Integration Time	Device IP	Device Type	Endpoint IP Address	Integration Type	Description
1	2021-08-02 17:05:40	20.10.0.200	IAG	20.10.0.43	Push down policies	IAG requested Manager to push down policies to block psiphon and 1 apps in all.
2	2021-08-02 17:05:40	20.10.0.200	IAG	192.168.20.123	Push down policies	IAG requested Manager to push down policies to block psiphon and 1 apps in all.
3	2021-08-02 17:05:40	20.10.0.200	IAG	20.10.0.11	Push down policies	IAG requested Manager to push down policies to block psiphon and 1 apps in all.
4	2021-08-02 17:05:27	20.10.0.200	IAG	192.168.20.123	Push down policies	IAG requested Manager to push down policies to block psiphon and 1 apps in all.
5	2021-08-02 17:05:27	20.10.0.200	IAG	20.10.0.11	Push down policies	IAG requested Manager to push down policies to block psiphon and 1 apps in all.

2. You can View the Proxy Tools Running Logs in IAG.

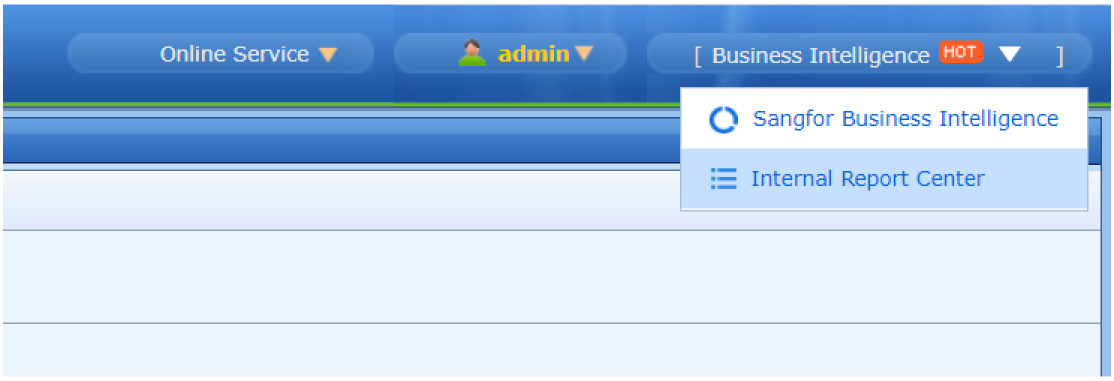


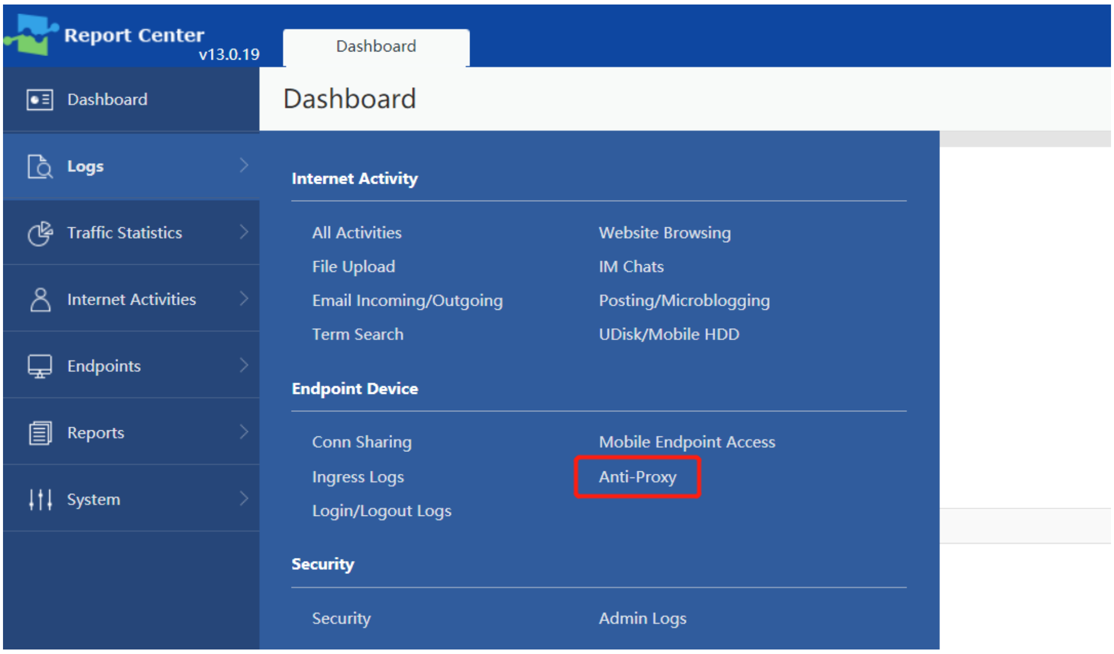
☑ Enable proxy detection

Block illegitimate proxy tools with IAG or Endpoint Secure. The latter blocking method needs to integrate with Endpoint Secure. Integration Normal

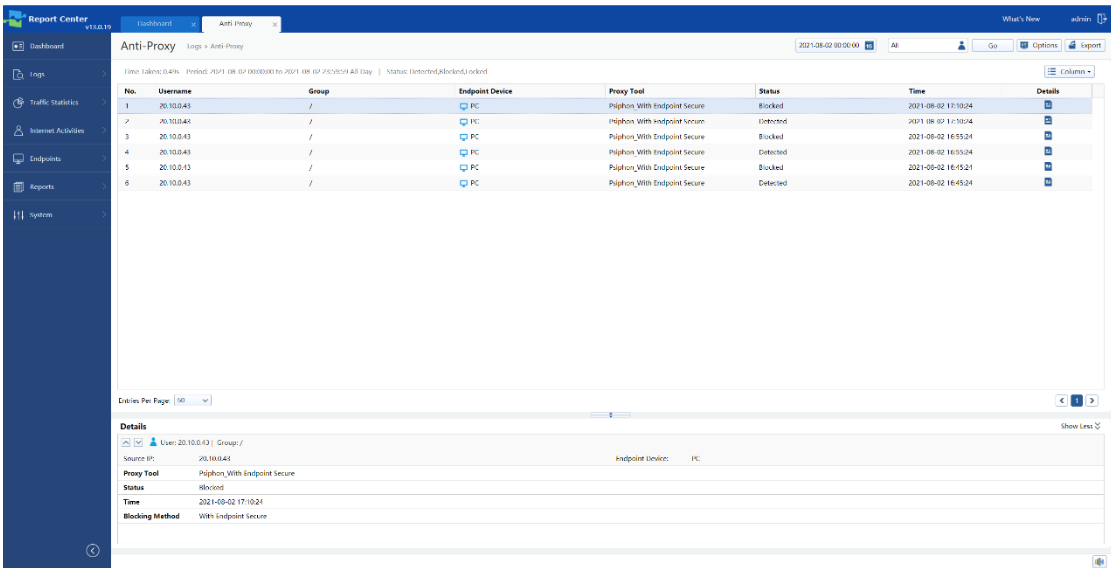
Auto Refresh: 5 seconds Search: Search term

□	IP Address	Username	Endpoint Type	Time	Status	Proxy Tool	Group
□	20.10.0.43	20.10.0.43	PC	2021-08-02 17:10:24	Detected	Psiphon_Block with Endpoint Secure	/
□	20.10.0.43	20.10.0.43	PC	2021-08-02 17:10:24	Blocked	Psiphon_Block with Endpoint Secure	/
□	20.10.0.43	20.10.0.43	PC	2021-08-02 16:55:24	Detected	Psiphon_Block with Endpoint Secure	/
□	20.10.0.43	20.10.0.43	PC	2021-08-02 16:55:24	Blocked	Psiphon_Block with Endpoint Secure	/
□	20.10.0.43	20.10.0.43	PC	2021-08-02 16:45:24	Detected	Psiphon_Block with Endpoint Secure	/
□	20.10.0.43	20.10.0.43	PC	2021-08-02 16:45:24	Blocked	Psiphon_Block with Endpoint Secure	/
□	192.168.20.85	192.168.20.85	PC	2021-07-27 16:26:37	Detected	Psiphon_Block with Endpoint Secure	/
□	192.168.20.85	192.168.20.85	PC	2021-07-27 16:26:37	Blocked	Psiphon_Block with Endpoint Secure	/
□	192.168.20.85	192.168.20.85	PC	2021-07-27 16:21:18	Detected	Psiphon_Block with Endpoint Secure	/
□	192.168.20.85	192.168.20.85	PC	2021-07-27 16:21:18	Blocked	Psiphon_Block with Endpoint Secure	/





3. Go to **Report Center**. You can view the detailed logs.



Time Taken: 0.49s Period: 2021-08-02 00:00:00 to 2021-08-02 23:59:59 All Day | Status: Detected,Blocked,Locked

No.	Username	Group	Endpoint Device	Proxy Tool	Status	Time	Details
1	20.10.0.43	/	PC	Psiphon_With Endpoint Secure	Blocked	2021-08-02 17:10:24	
2	20.10.0.43	/	PC	Psiphon_With Endpoint Secure	Detected	2021-08-02 17:10:24	
3	20.10.0.43	/	PC	Psiphon_With Endpoint Secure	Blocked	2021-08-02 16:55:24	
4	20.10.0.43	/	PC	Psiphon_With Endpoint Secure	Detected	2021-08-02 16:55:24	
5	20.10.0.43	/	PC	Psiphon_With Endpoint Secure	Blocked	2021-08-02 16:45:24	
6	20.10.0.43	/	PC	Psiphon_With Endpoint Secure	Detected	2021-08-02 16:45:24	

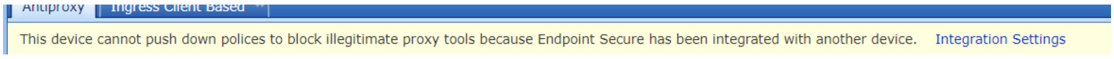
Details

User: 20.10.0.43 | Group: /

Source IP:	20.10.0.43	Endpoint Device:	PC
Proxy Tool	Psiphon_With Endpoint Secure		
Status	Blocked		
Time	2021-08-02 17:10:24		
Blocking Method	With Endpoint Secure		

4 Precaution

1. The version of both Endpoint Secure Manager and Endpoint Agent must be 3.5.5 EN or above.
2. Only one instance of IAG can be running at any given time.



This device cannot push down polices to block illegitimate proxy tools because Endpoint Secure has been integrated with another device.

3. Endpoint Secure Manager can run alongside one instance of IAG (Anti-Proxy Enabled) and multiple instances of NGAF (Anti-Proxy Disabled).
4. Require port 443 communication between IAG and Endpoint Secure Manager.
5. Anti-proxy and ES Correlation doesn’t support on windows server platform, it only support on windows-pc with windows 7 and above.

SANGFOR