



SANGFOR

Sangfor NGAF

Endpoint App Control Configuration Guide

Product Version 8.0.39

Document Version 01

Released on Aug. 26, 2021



Copyright © Sangfor Technologies Inc. 2021. All rights reserved.

Unless otherwise stated or authorized, Sangfor Technologies Inc. (hereinafter referred to as "Sangfor") and its affiliates reserve all intellectual property rights, including but not limited to copyrights, trademarks, patents, and trade secrets, and related rights to text, images, pictures, photographs, audio, videos, charts, colors, and layouts as presented in or concerning this document and content therein. Without prior written consent of Sangfor, this document and content therein must not be reproduced, forwarded, adapted, modified or displayed or distributed by any other means for any purpose.

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.

Change Log

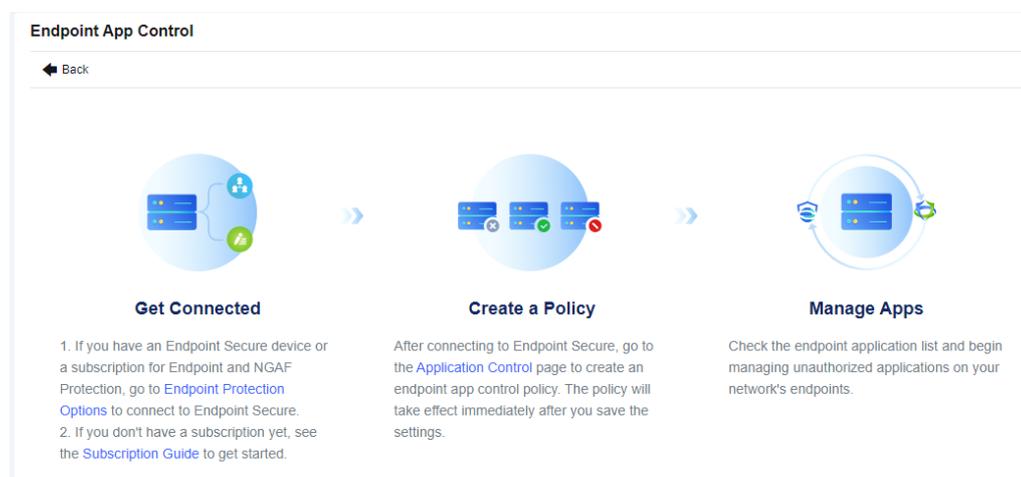
Date	Change Description
Aug. 26, 2021	This is the first release of this document.

Contents

Change Log.....	2
1 Introduction.....	4
2 Application Scenario.....	4
2.1 Block Proxy Tools.....	4
2.1.1 Configuration Steps.....	4
2.1.2 Testing Result.....	7
2.2 Block Custom Application.....	7
2.2.1 Configuration Steps.....	7
2.2.2 Testing Result.....	10
3 Precaution.....	11

1 Introduction

Endpoint App control is a function used to track and control applications from the endpoint application list to prevent employees from using those apps during office hours, improving productivity and reducing network security risks.



2 Application Scenario

2.1 Block Proxy Tools

An enterprise does not allow their employee to use proxy tools. When the user uses proxy tools like Psiphon, the application will not be able to run. To implement this function, you need to add an endpoint app control policy in NGAF.

2.1.1 Configuration Steps

Step 1. Make sure that your NGAF device is connected to Endpoint Secure Manager. To connect NGAF to Endpoint Secure Manager, go to **SOC > Next-Gen Security > Endpoint Protection > Endpoint Protection Options**.



Endpoint Secure

Endpoint Secure integrates the power of AI with Engine-Zero, cloud-based engine and reputation database. When integrated with NGAF, Endpoint Secure delivers a comprehensive, highly coordinated and automated defense platform for continuous detection, rapid response, and multi-layered protection.

Integration Settings

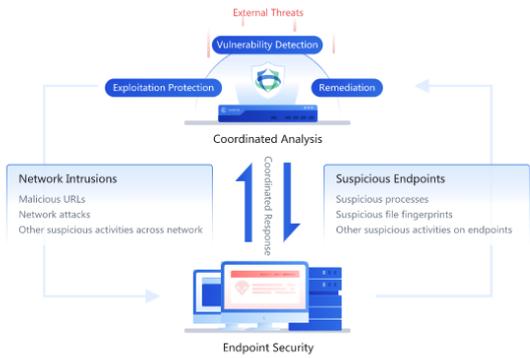
- Endpoint Secure and NGAF
- Endpoint Secure and Platform-X (coming s...)

Endpoint Secure Manager

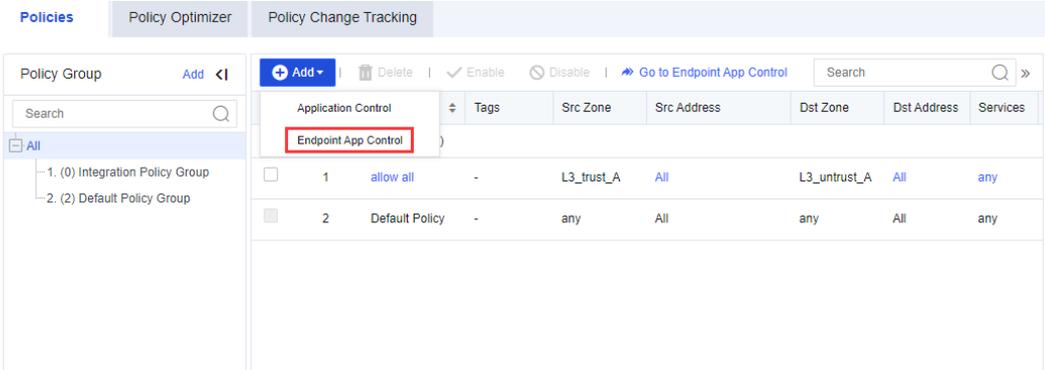
- For Endpoint Secure Manager
- For networks with more than 500 endpoints

Endpoint and NGAF Protection [How to Subscribe?](#)

Integrate NGAF with Endpoint Secure to share security information, visualize threats and enhance threat response across your network.



Step 2. After Endpoint Secure Manager success connected with NGAF, configure an endpoint app control policy in NGAF. Go to **Policies > Access Control > Application Control**. Click **Add** and select **Endpoint App Control** to configure the policy.



Application Control	Tags	Src Zone	Src Address	Dst Zone	Dst Address	Services
Endpoint App Control						
1 allow all	-	L3_trust_A	All	L3_untrust_A	All	any
2 Default Policy	-	any	All	any	All	any

Edit Endpoint App Control Policy

Name:

Status: Enabled Disabled

Description:

Policy Group: Integration Policy Group

Tags:

Endpoints:

Applications:

Schedule: All week

Action: Allow Block

NGAF will push down the policy to Endpoint Secure immediately after you save the settings. Within 5 to 10 minutes, the selected applications will be blocked on all selected endpoints.

Name: Set the name of the endpoint app control policy.

Status: Set the policy as **Enabled** or **Disabled**.

Description: Set the description of the endpoint app control policy

Policy Group: By default, all endpoint app control policies will belong to the Integration Policy Group.

Tags: Select the policy tag. This parameter is optional and can be set for displaying a specified zone or filtering.

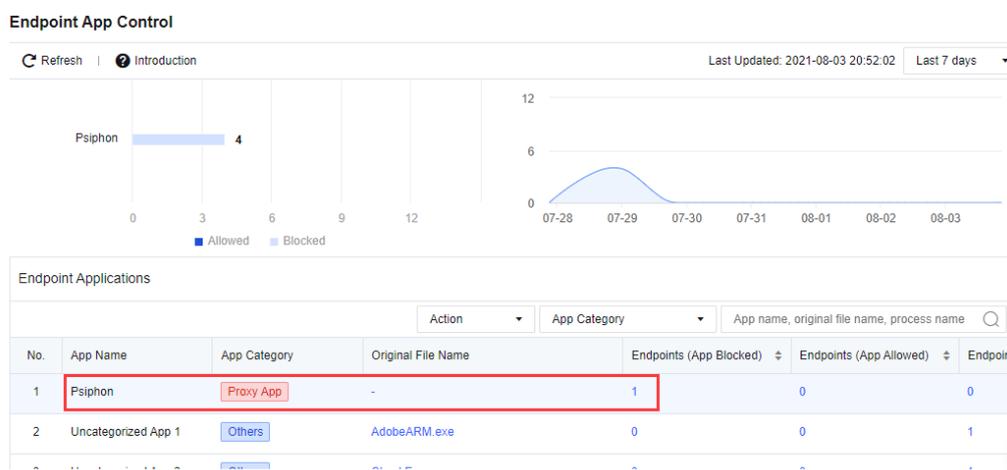
Endpoints: Select the endpoint's IP to be controlled.

Applications: Select the applications that are needed to control.

Schedule: By default, the policy will run all week.

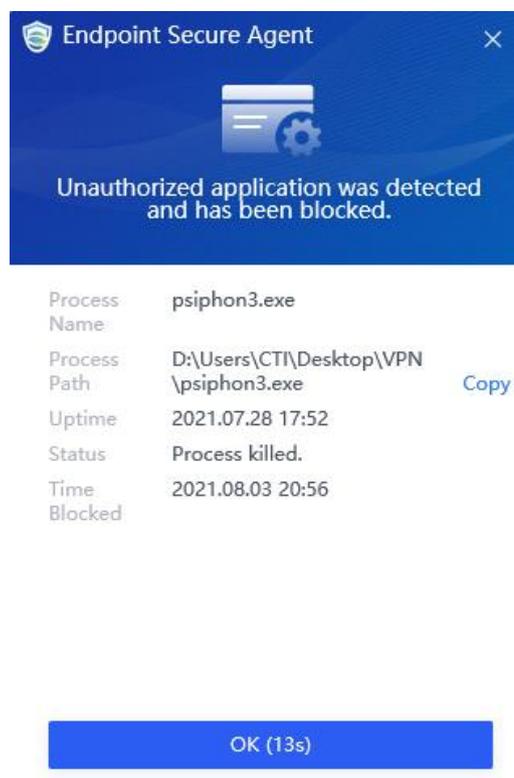
Action: Set the policy to **Allow** or **Block**.

Step 3. After 5 to 10 minutes, go to **SOC > Specialized Protection > Endpoint App Control** to view the endpoint app control status for the endpoint.



2.1.2 Testing Result

Step 1. Run the Psiphon application in the endpoint. ES agent will block the Psiphon application for running and prompt the alert.



2.2 Block Custom Application

An enterprise does not allow their employee to use certain applications. When the user uses those applications, the application will not be able to run. To implement this function, you need to add an endpoint app control policy in NGAF and ensure the agent has collected the application signatures from the PC.

2.2.1 Configuration Steps

Step 1. Make sure that your NGAF device is connected to Endpoint Secure Manager. To connect NGAF to Endpoint Secure Manager, go to **SOC > Next-Gen Security > Endpoint Protection > Endpoint Protection Options**.



Endpoint Secure

Endpoint Secure integrates the power of AI with Engine-Zero, cloud-based engine and reputation database. When integrated with NGAF, Endpoint Secure delivers a comprehensive, highly coordinated and automated defense platform for continuous detection, rapid response, and multi-layered protection.

Integration Settings

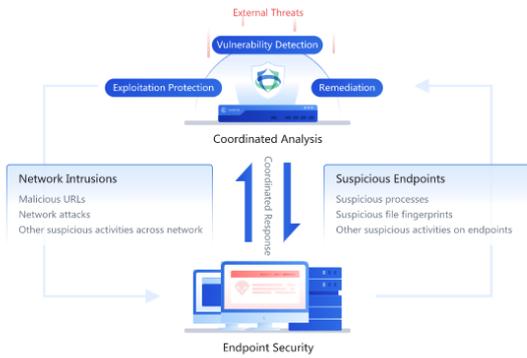
- Endpoint Secure and NGAF
- Endpoint Secure and Platform-X (coming s...

Endpoint Secure Manager

- For Endpoint Secure Manager
- For networks with more than 500 endpoints

Endpoint and NGAF Protection [How to Subscribe?](#)

Integrate NGAF with Endpoint Secure to share security information, visualize threats and enhance threat response across your network.



Step 2. Go to **SOC > Specialized Protection > Endpoint App Control** to check the application signature collected from the ES agent.

Endpoint App Control

Refresh | Introduction Last Updated: 2021-08-16 11:24:11 Last 24 hours

1	Psiphon	Proxy App	-	1	0	0
2	Uncategorized App 1	Others	ECAgent.exe	0	0	1
3	Uncategorized App 2	Others	IpOverUsbSvc.exe	0	0	1
4	Uncategorized App 3	Others	MobaXterm	0	0	1
5	Uncategorized App 4	Others	OneDrive.exe	0	0	1
6	Uncategorized App 5	Others	QQProtect.exe	0	0	1
7	Uncategorized App 6	Others	RVLAgent.exe	0	0	1
8	Uncategorized App 7	Others	RVLService.exe	0	0	1
9	Uncategorized App 8	Others	SFEAssetCollect.exe	0	0	1
10	Uncategorized App 9	Others	SRAPSRV.exe	0	0	1

Step 3. Click **Add Custom App** to create the custom endpoint application that needed to block according to the list. For example, select teamviewer.exe as a custom application.

Endpoint App Control

Refresh | Introduction Last Updated: 2021-08-16 11:24:11 Last 24 hours

14	Uncategorized App 13	Others	SangforUDProtectEx.exe	0	0	1	Add Custom App
15	Uncategorized App 14	Others	SecurityDesktopService.exe	0	0	1	Add Custom App
16	Uncategorized App 15	Others	TeamViewer.exe	0	0	1	Add Custom App
17	Uncategorized App 16	Others	TeamViewer_Service.exe	0	0	1	Add Custom App
18	Uncategorized App 17	Others	TlWorker.exe	0	0	1	Add Custom App
19	Uncategorized App 18	Others	VDAGENT.exe	0	0	1	Add Custom App

Add Custom App ✕

App Name: Custom_

Description:

Original File Name: TeamViewer.exe

App Category:

Status: Enabled Disabled

App Name: Set the application name.

Description: Set the description of the custom application.

Original File Name: File name collected by ES agent.

App Category: Set the application category.

Status: Set whether to **Enabled** or **Disabled** the custom endpoint application.

Step 4. After Endpoint Secure is connected, configure an endpoint app control policy. Go to **Policies > Access Control > Application Control** to configure the policy. Select the custom app that was created earlier.

Edit Endpoint App Control Policy ✕

Name:

Status: Enabled Disabled

Description:

Policy Group: Integration Policy Group

Tags:

Endpoints:

Applications:

Schedule: All week

Action: Allow Block

NGAF will push down the policy to Endpoint Secure immediately after you save the settings. Within 5 to 10 minutes, the selected applications will be blocked on all selected endpoints.

Name: Set the name of the endpoint app control policy.

Status: Set the policy as **Enabled** or **Disabled**.

Description: Set the description of the endpoint app control policy

Policy Group: By default, all endpoint app control policies will belong to the Integration Policy Group.

Tags: Select the policy tag. This parameter is optional and can be set for displaying a specified zone or filtering.

Endpoints: Select the endpoint's IP to be controlled.

Applications: Select the applications that are needed to control.

Schedule: By default, the policy will run all week.

Action: Set the policy to **Allow** or **Block**.

Step 1. After 5 to 10 minutes, go to **SOC > Specialized Protection > Endpoint App Control** to view the endpoint app control status for the endpoint.

2.2.2 Testing Result

Run the Teamviewer application in the endpoint. ES agent will block the application for running and prompt the alert.



Process Name	TeamViewer.exe	
Process Path	C:\Program Files (x86)\TeamViewer\TeamViewer.exe	Copy
Uptime	2021.08.16 12:09	
Status	Process blocked.	
Time Blocked	2021.08.16 12:09	

OK (22s)

3 Precaution

1. Endpoint App control requires the Endpoint Secure in version 3.5.5 and above.
2. The policy set in NGAF may not take effect instantly. You may need to wait for 5-10mins.
3. You can create the custom application according to the Endpoint App Control list only.
4. The Windows process will not be collected by the ES agent and send to NGAF.
5. The ES agent will not block the application consist of Sangfor signature.



SANGFOR

