SANGFOR

Sangfor NGAF

Endpoint App Control Configuration Guide

Product Version	8.0.39
Document Version	01
Released on	Aug. 26, 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.

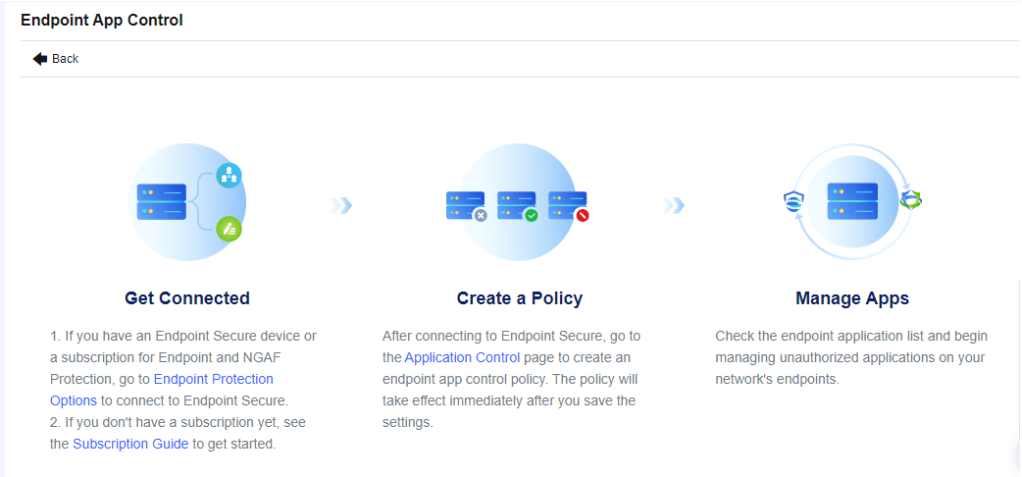
Change Log

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

Contents

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.



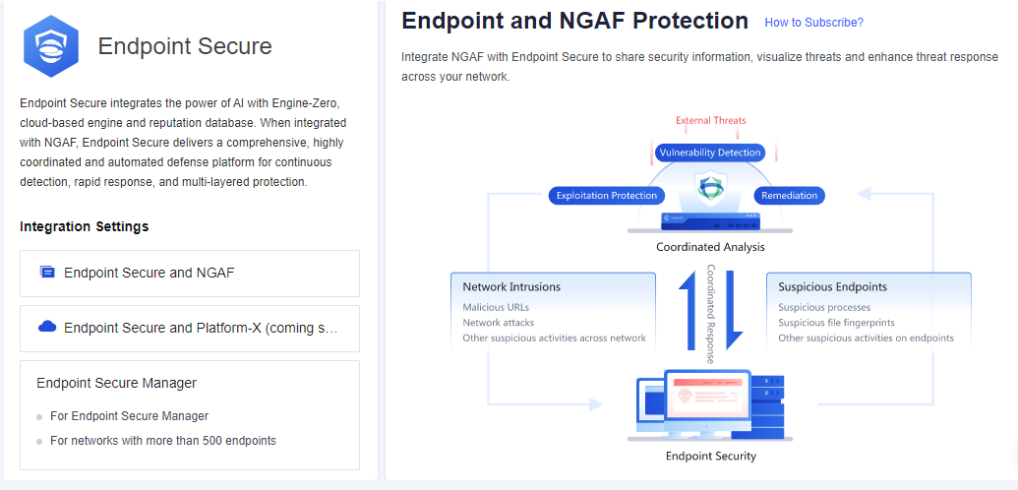
2 Application Scenario

2.1 Block Proxy Tools

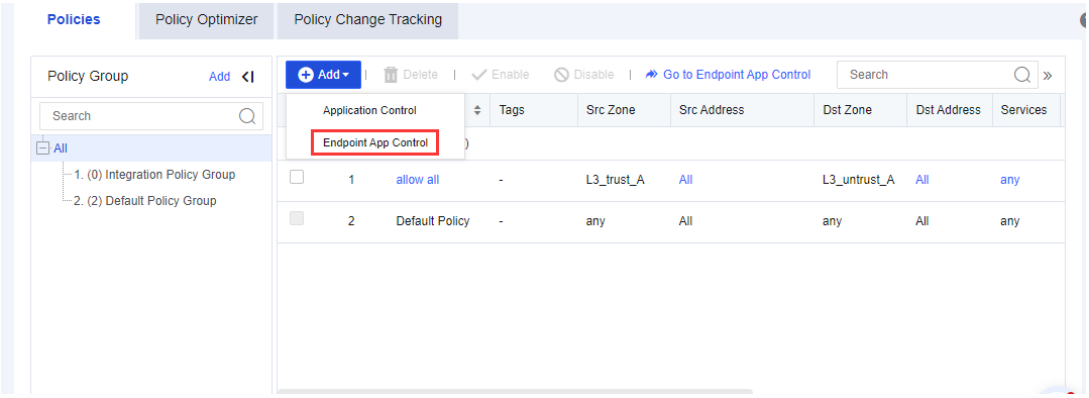
An enterprise does not allow their employee to use proxy tools. When the user uses proxy tools like Psiphon, the application will not be able to run. To implement this function, you need to add an endpoint app control policy in NGAF.

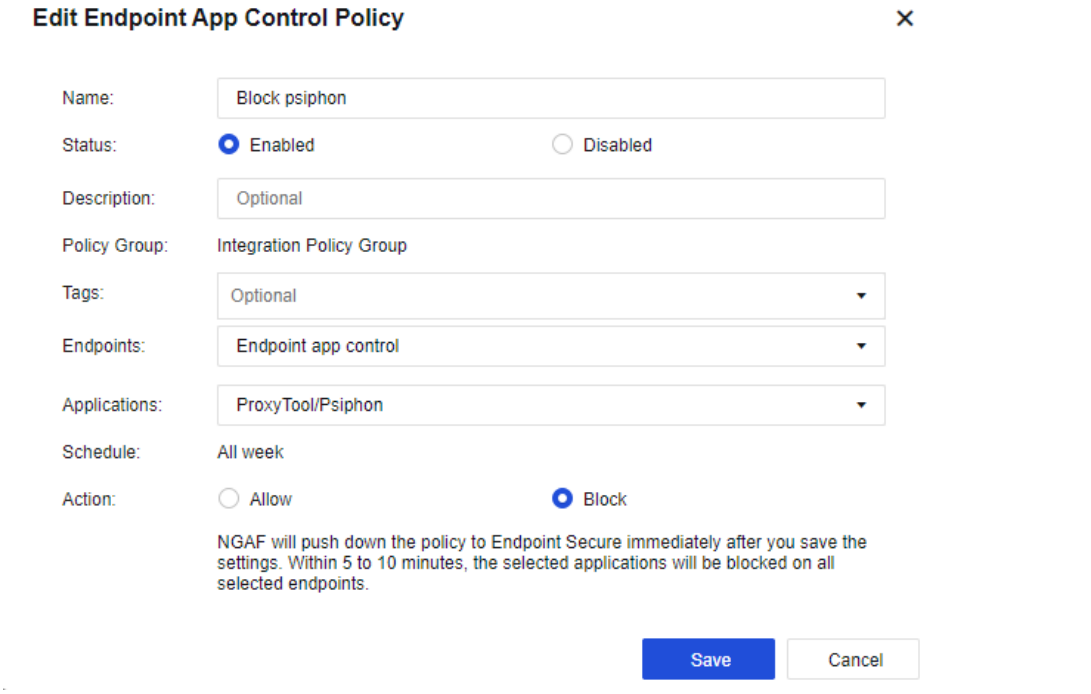
2.1.1 Configuration Steps

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**.



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.





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.

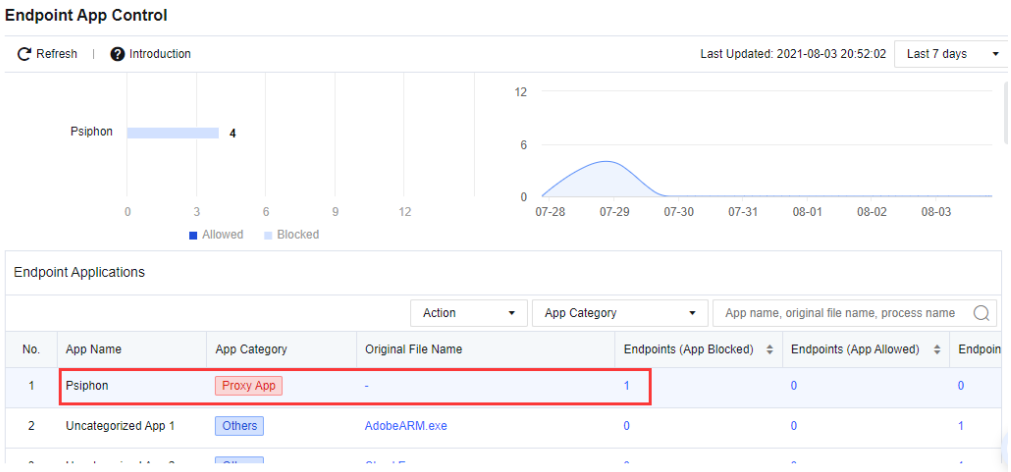
Endpoints: Select the endpoint's IP to be controlled.

Applications: Select the applications that are needed to control.

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

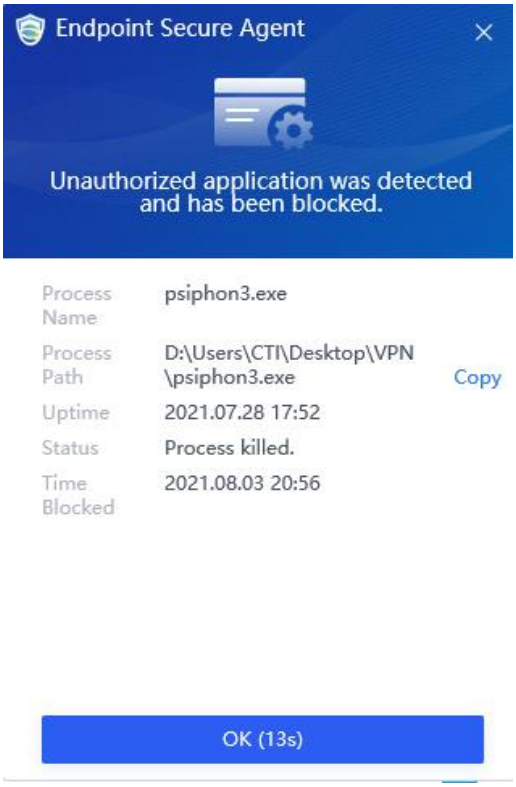
Action: Set the policy to **Allow** or **Block**.

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.

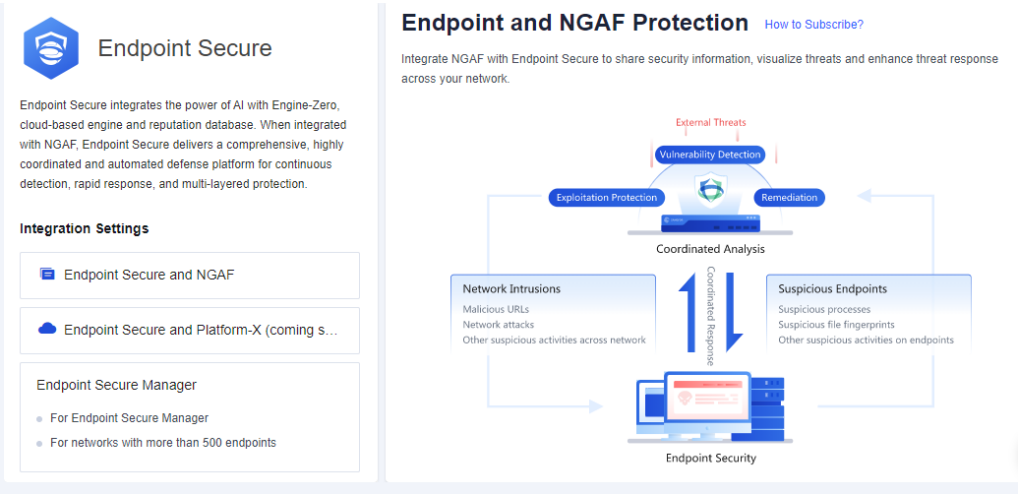


2.2 Block Custom Application

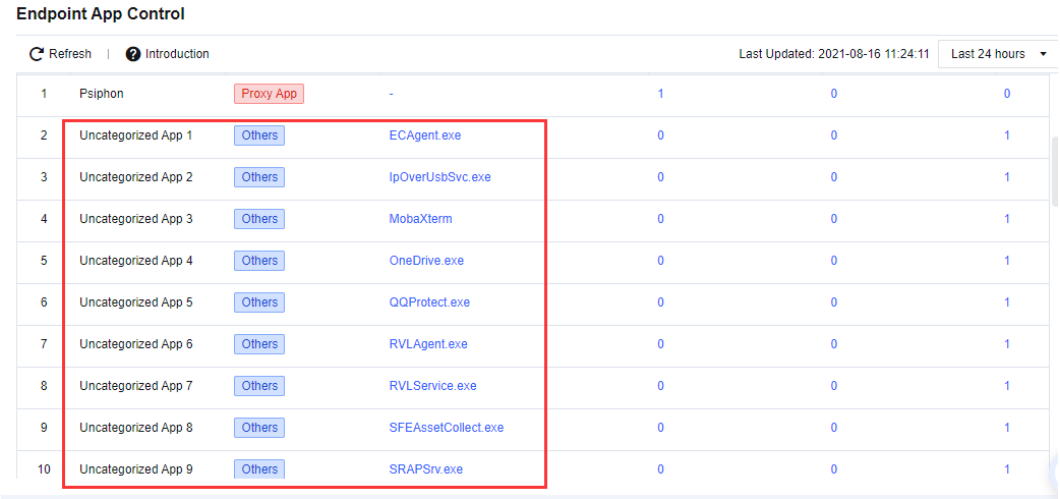
An enterprise does not allow their employee to use certain applications. When the user uses those applications, the application will not be able to run. To implement this function, you need to add an endpoint app control policy in NGAF and ensure the agent has collected the application signatures from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

2.2.1 Configuration Steps

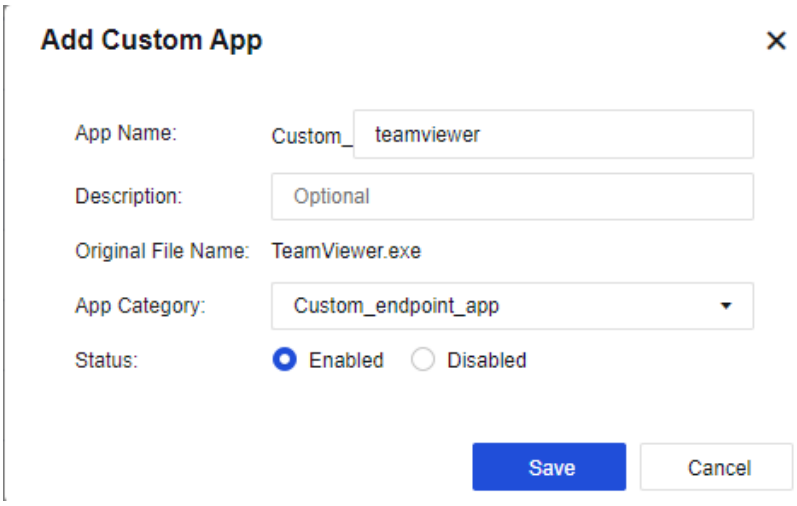
Step 1. Make sure that your NGAF device is connected to Endpoint Secure Manager. To connect NGAF to Endpoint Secure Manager, go to **SOC** > **Next-Gen Security** > **Endpoint Protection** > **Endpoint Protection Options**.



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



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.



App Name: Set the application name.

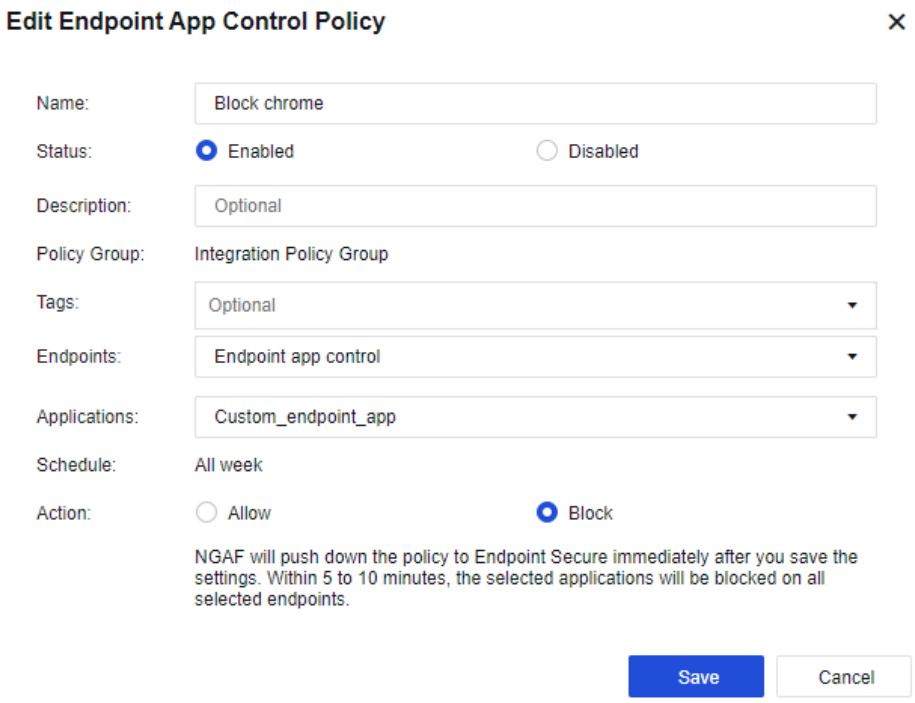
Description: Set the description of the custom application.

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.



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.

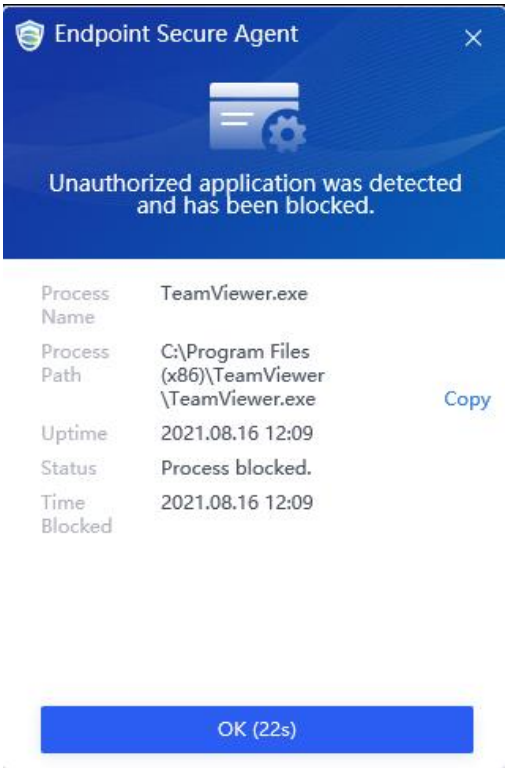
Schedule: By default, the policy will run all week.

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.



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