



SANGFOR



Endpoint Secure

Best Practices for Scenarios_Endpoint Secure Security Policy Implement Guide for Host

Version 3.2.22



Change Log

Date	Change Description
Mar 16, 2021	Document release.
May 17, 2021	Document update.

CONTENT

Chapter 1 Scenario	1
Chapter 2 Overview	1
Chapter 3 Identify the Security Risks of Host	1
3.1 Security & Integrity Check	1
3.1.1 Security & Integrity Check	1
3.1.2 Deal with Non-conformities	1
3.2 System Vulnerability Check	3
3.2.1 Vulnerability Check	3
3.2.2 Dealing with Vulnerabilities	3
3.3 Scan Virus	4
3.3.1 Scan Virus	4
Chapter 4 Host Security Policy Implementation Guidance	4
4.1 Basic Policy	4
4.2 Anti Virus	5
4.3 Realtime Protection	6
4.4 Trust Files	7
4.5 Vulnerability Fix	7
4.6 Alarm Policy	8

Chapter 1 Scenario

Chapter 2 Overview

This document is suitable for Endpoint Secure to guide the implementation of the Endpoint Secure security policy in the context of protecting the host security. The document includes two parts: identifying host security risks and implementing host security policies. Identifying host security risks guides users on how to identify client security risks in advance, makes users aware of the security risks and impacts of host, and guides users to deal with security risks; implement host The security policy refers to which security policy should be configured by Endpoint Secure and how to configure the security policy in order to ensure the subsequent security of the host.

Chapter 3 Identify the Security Risks of Host

Identifying host security risks is to guide users how to identify client security risks in advance, make users aware of the security risks and impacts of the host, and guide users to deal with security risks. This chapter guides users to identify client security risks in advance and deal with them from three parts: baseline check, system vulnerability check, and virus killing.

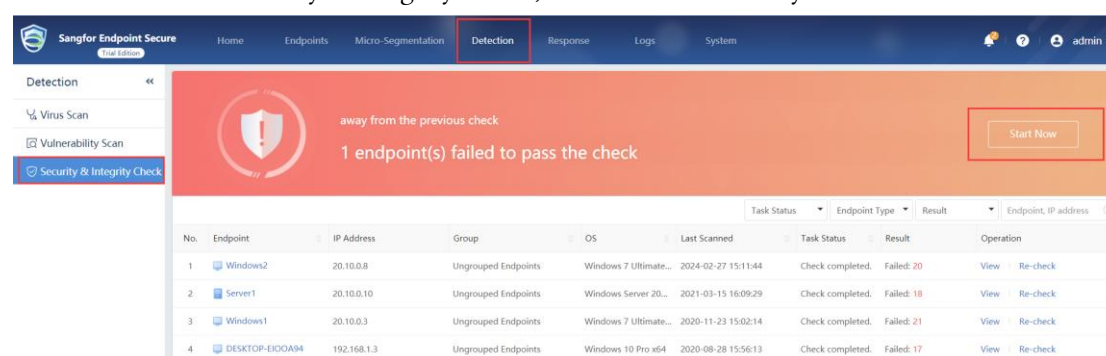
Note that if there are many hosts, it is recommended to choose 1 or 2 hosts to guide users on how to identify host security risks and how to deal with them.

3.1 Security & Integrity Check

Security & Integrity Check is a compliance check for windows and linux systems according to security compliance requirements, helping customers find non-compliant endpoints' and non-compliant items in the intranet, and provide repair suggestions.

3.1.1 Security & Integrity Check

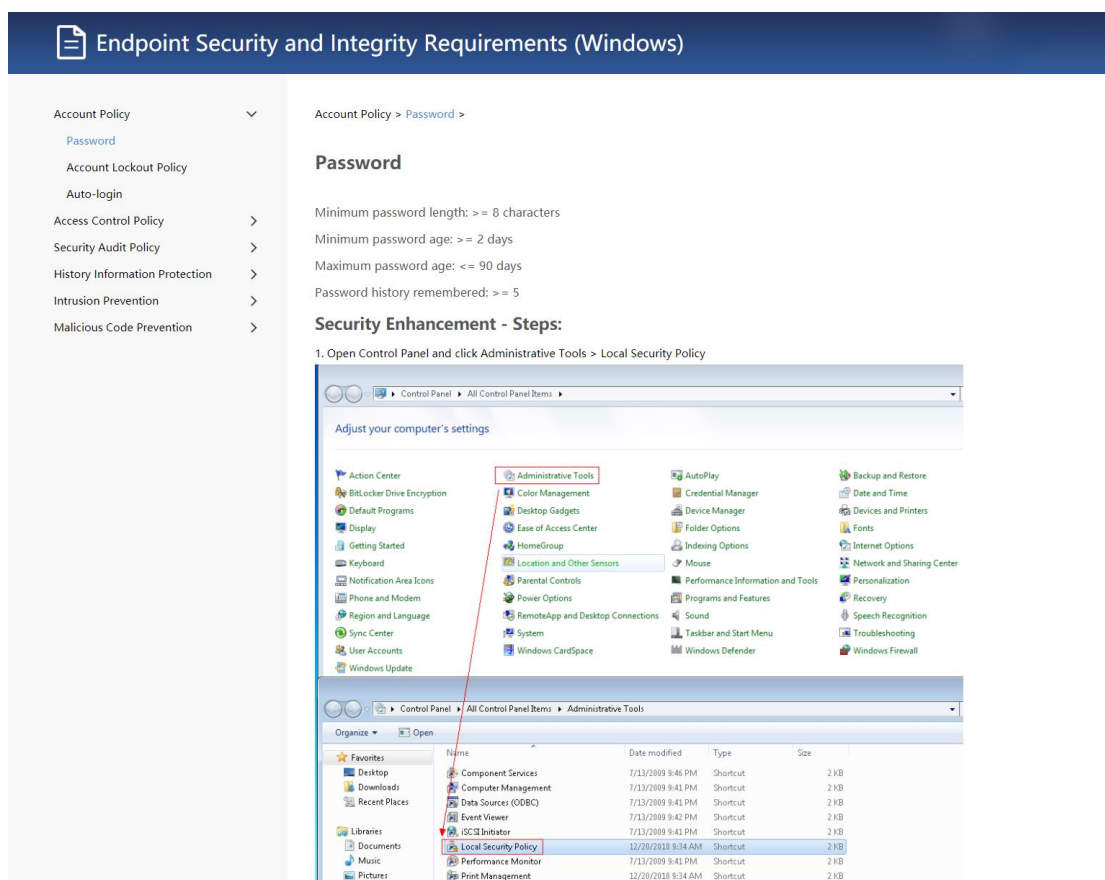
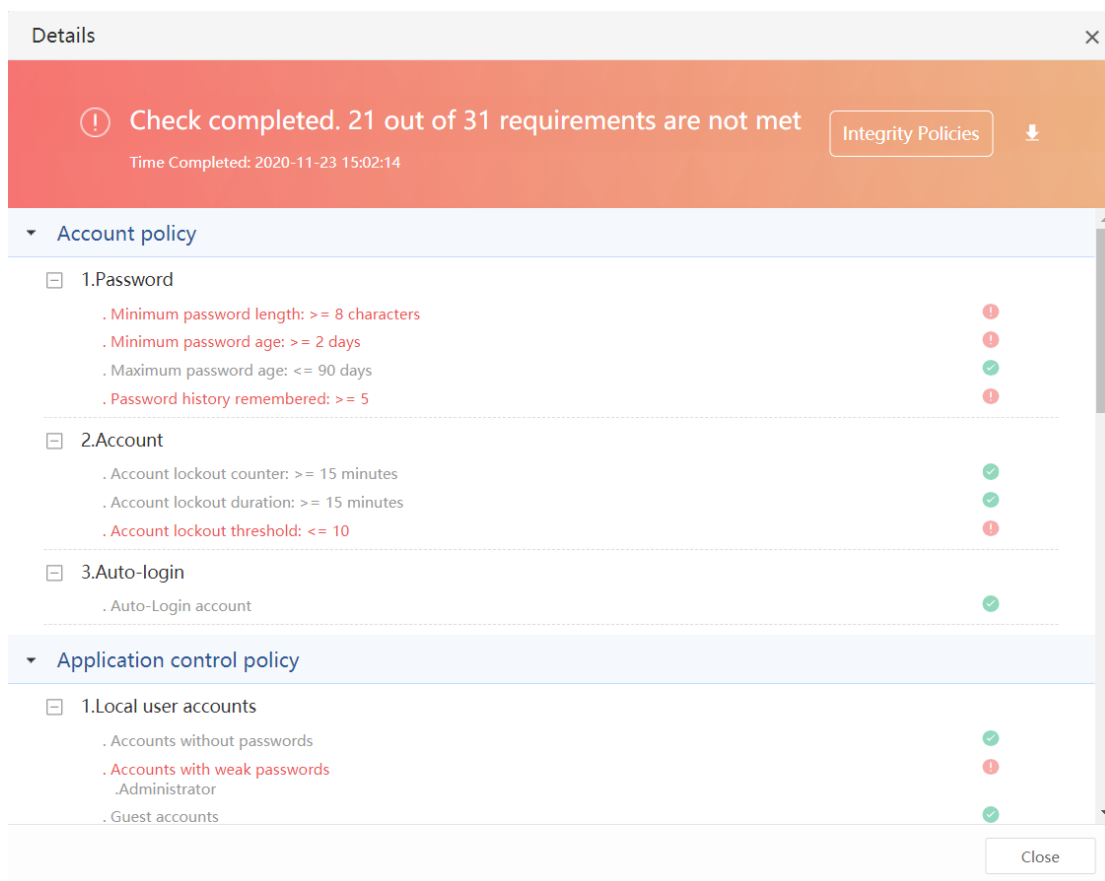
Go to Detection-> Security & Integrity Check, Perform basic security checks on the host.



No.	Endpoint	IP Address	Group	OS	Last Scanned	Task Status	Result	Operation
1	Windows2	20.10.0.8	Ungrouped Endpoints	Windows 7 Ultimate...	2024-02-27 15:11:44	Check completed.	Failed: 20	View Re-check
2	Server1	20.10.0.10	Ungrouped Endpoints	Windows Server 20...	2021-03-15 16:09:29	Check completed.	Failed: 18	View Re-check
3	Windows1	20.10.0.3	Ungrouped Endpoints	Windows 7 Ultimate...	2020-11-23 15:02:14	Check completed.	Failed: 21	View Re-check
4	DESKTOP-EJQOA94	192.168.1.3	Ungrouped Endpoints	Windows 10 Pro x64	2020-08-28 15:56:13	Check completed.	Failed: 17	View Re-check

3.1.2 Deal with Non-conformities

Reinforce the non-compliant items in the system security check results according to the security compliance setting document provided by Endpoint Secure, as shown in the following figure:

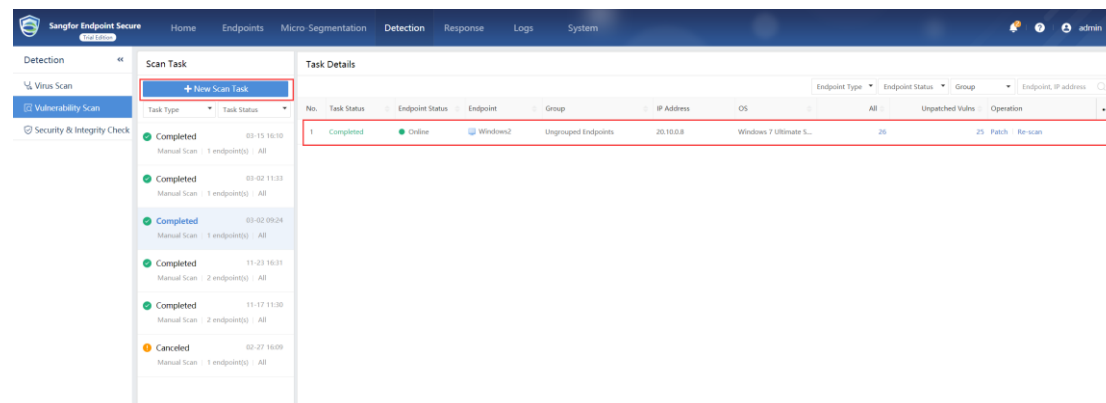


3.2 System Vulnerability Check

Help users identify high-risk vulnerabilities in hosts and provide repair suggestions.

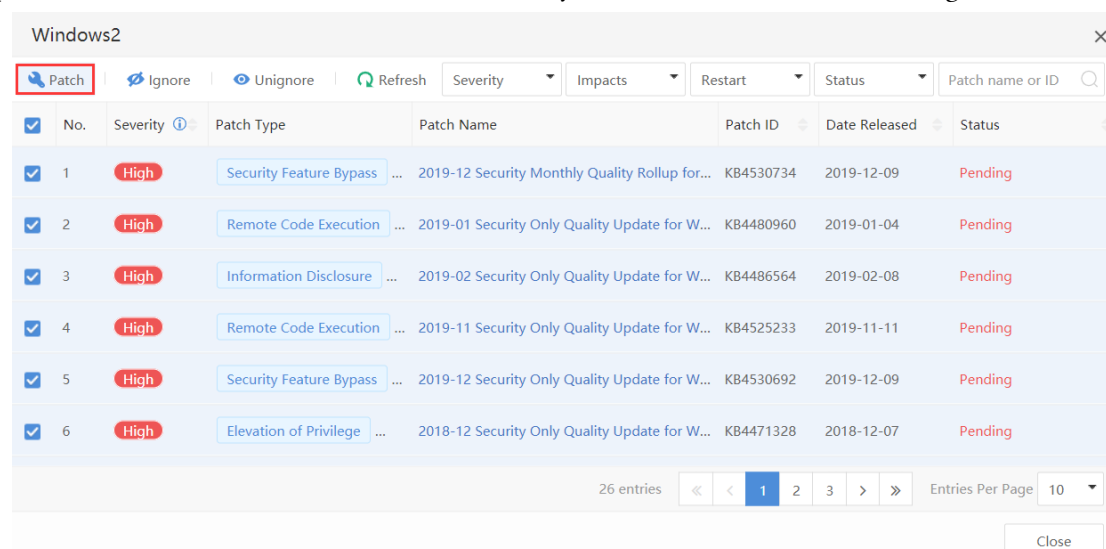
3.2.1 Vulnerability Check

Go to Detection-> Vulnerability Scan path, Check hosts for vulnerabilities.

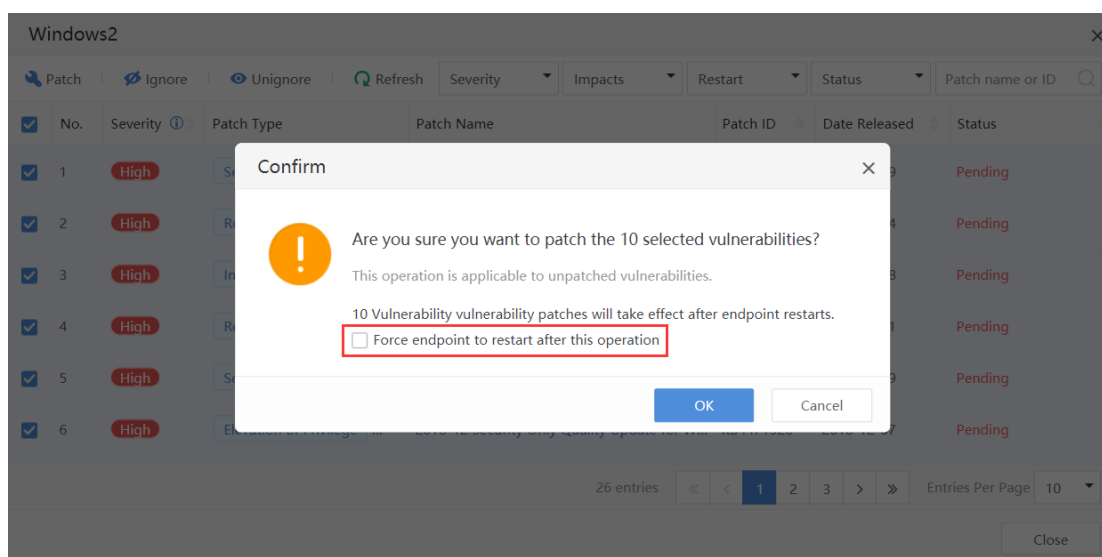


3.2.2 Dealing with Vulnerabilities

Repair the unfixed vulnerabilities in the vulnerability check results, as shown in the figure below:



Note that after clicking "Patch", it is recommended not to check "Force endpoint to restart after this operation" for patches that can only take effect after restarting the computer, as shown in the figure below:



3.3 Scan Virus

Perform a full investigation and killing of hosts, discover and deal with threat files in advance.

3.3.1 Scan Virus

Organizations or departments with the same business environment will promote implementation according to the following ideas.

Find a test computer: Find a computer in the same business environment to install the Endpoint Secure client test for a full-scale killing test.

Analyze and kill results: Analyze the threat files found by the test computer.

If it is confirmed that it is a misjudgment, add a whitelist.

Confirm that it is not a misjudgment, contact Sangfor Engineer to deal with

Verify business availability: Verify and test the computer business availability to ensure that the business can be used normally.

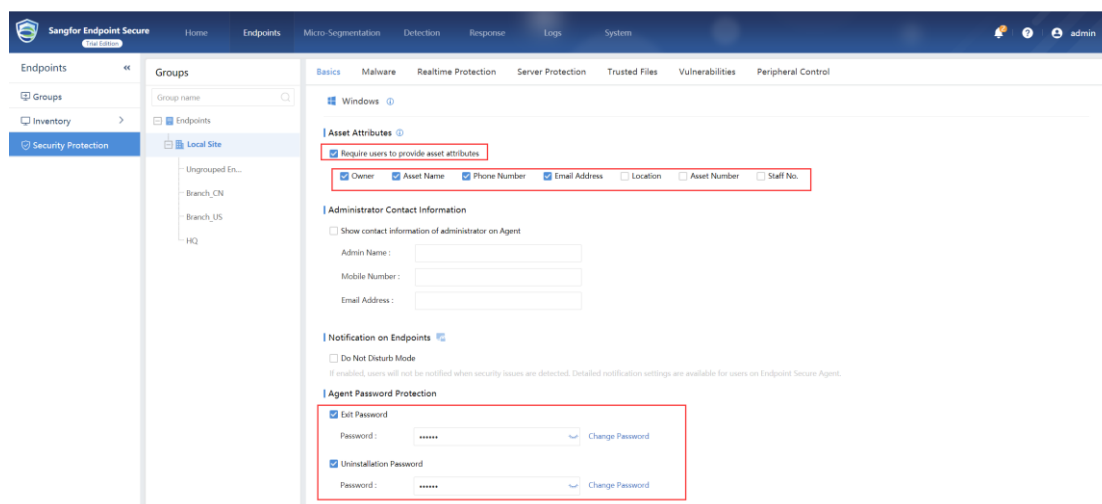
Promote the installation of other computers: the test computer is verified and the business is not affected, then it will be promoted to other computers in the same environment to install and kill.

Chapter 4 Host Security Policy Implementation Guidance

The implementation of host security policy refers to which security policy should be configured by Endpoint Secure and how to configure security policy in order to ensure the subsequent security of the client. The host security policy is configured from the basic policy, virus detection and killing policy, real-time protection policy, trust list, vulnerability detection and repair detection, and alarm policy to protect host security.

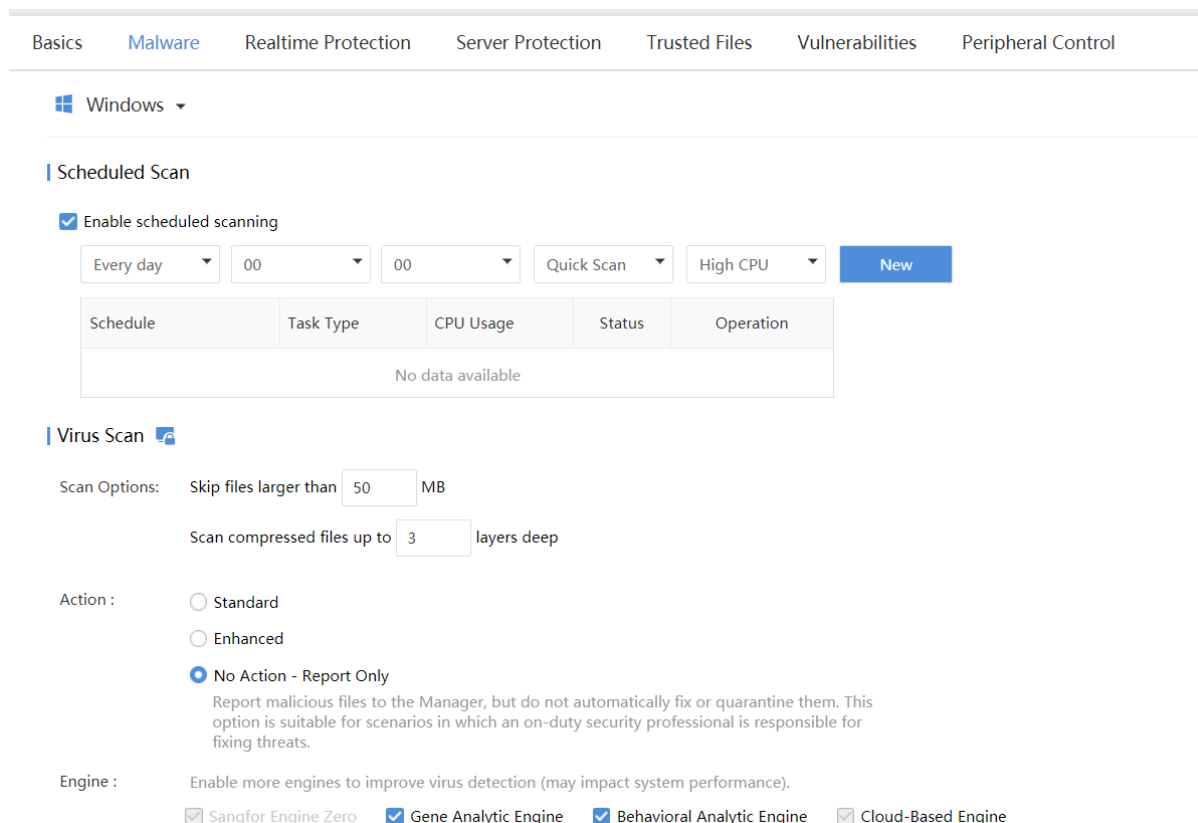
4.1 Basic Policy

Go to Endpoints->Security Protection path, configure the basic policy of the group where the hosts are located, enable asset information registration, and set the terminal's Exit Password/Uninstallation Password, as shown in the figure below:



4.2 Anti Virus

Go to Endpoints->Security Protection path, configure the virus detection and killing policy of the group where the hosts are located, as shown in the following figure:

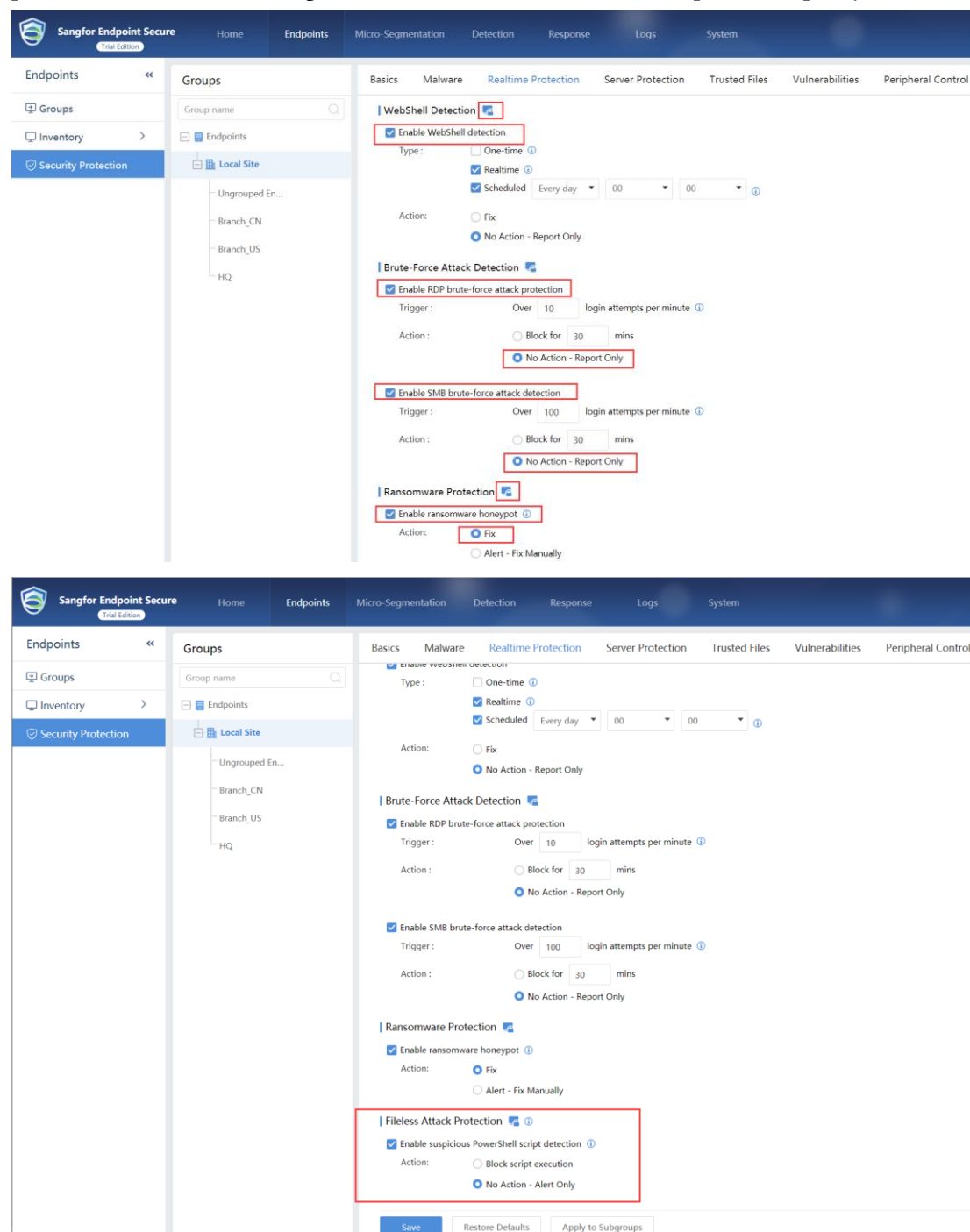


[Scheduled Scan] Turn on regular automatic scanning. It is recommended that the time to check killing intent is once a month, the scanning type is quick scanning, and the scanning mode is balanced.

[Action] Keep the default configuration; the disposal action after the threat file is found is recommended to be configured as "Standard"; if the scanning engine is fully turned on, it will occupy a relatively high resource. If the client CPU and memory are configured with 4 cores and 8G or more, it can be fully turned on. If you configure the following here, it is recommended to open the gene feature engine instead of the behavior analysis engine.

4.3 Realtime Protection

Go to Endpoints->Security Protection path, configure the real-time protection policy of the group where the hosts are located, including real-time file monitoring, ransomware protection and advanced threat protection, as shown in the figure below, set the windows real-time protection policy.



[Realtime File System Protection] Enable the small lock icon on the right, and the file real-time protection policy is issued from the MGR to the ES agent.

[Protection Level] It is recommended to configure the protection level as "Medium";

[FileType] It is recommended to select all file types;

[Scan Options] It is recommended to keep the default configuration for file scanning;

[Engine] If the scanning engine is fully turned on, it will occupy a relatively high resource. If the host's CPU and memory are configured with 4 cores and 8G or more, it can be fully turned on. If the

configuration is below, it is recommended to turn on the gene feature engine instead of the Sangfor Zero artificial intelligence engine. .

[Action] The default action after a malicious file is found is recommended to be set to "standard disposal"

[Ransomware Protection] Enable the small lock icon on the right, and the ransomware protection policy will be sent from the management terminal to the ES agent.

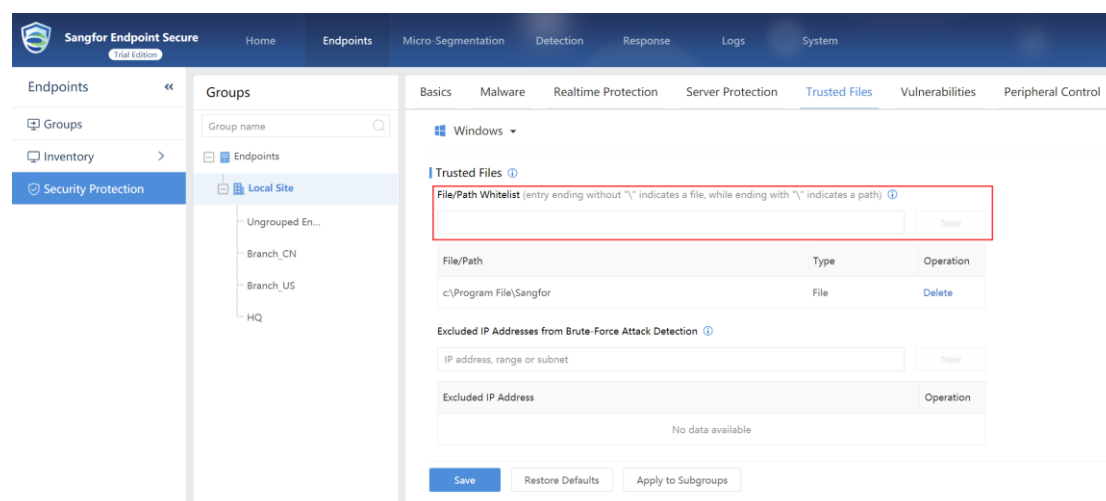
[Action] It is found that the recommended configuration for ransomware behavior is "Fix".

[Fileless Attack Protection] Enable the small lock icon on the right, and the advanced threat protection policy is issued from the management end to the ES agent, and check "Enable suspicious PowerShell script detection".

[Action] When a suspicious powershell script is found to be executed, it is recommended to set it to "Block script execution".

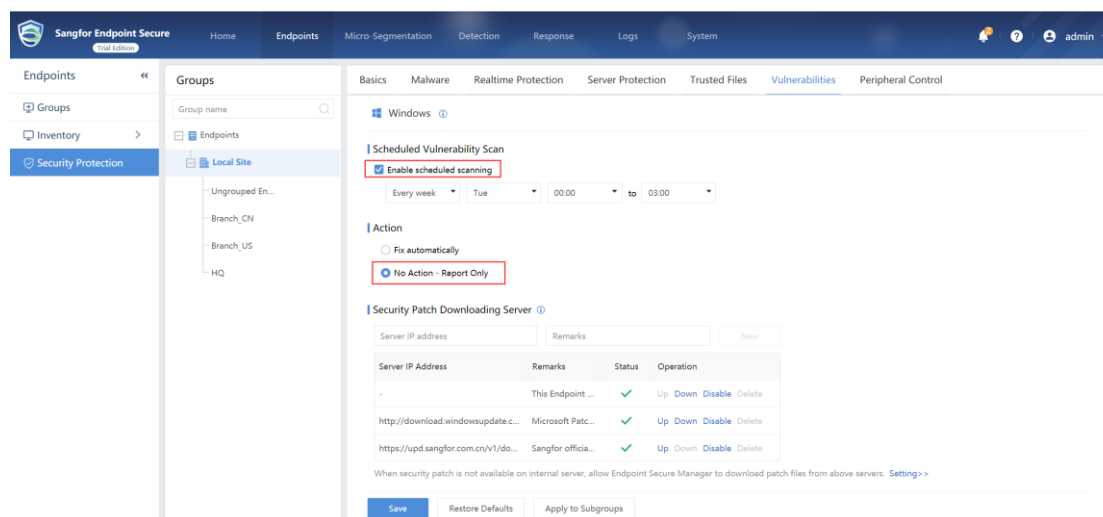
4.4 Trust Files

Go to Endpoints->Security Protection path, Configure the whitelist policy of the group where the host is located, and add files or directories that do not require antivirus and real-time protection to the trust list (such as business system files), as shown in the following figure:



4.5 Vulnerability Fix

Go to Endpoints->Security Protection path, Configure the vulnerability repair policy of the group where the hosts are located, as shown in the following figure:



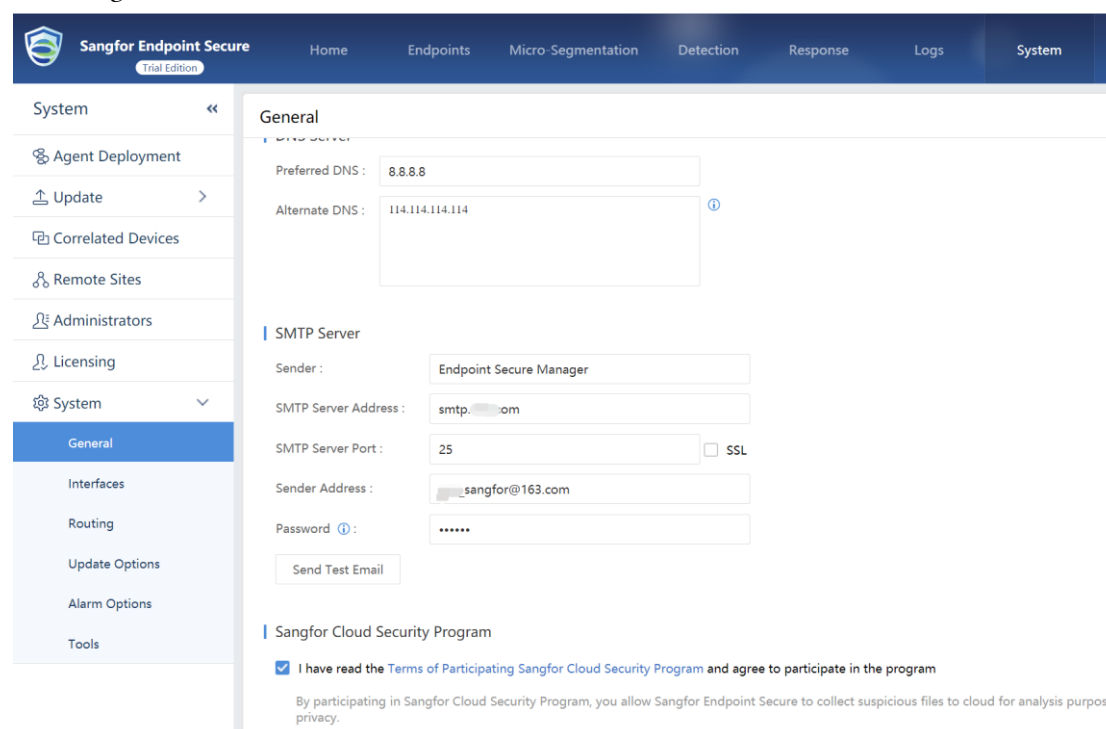
[Scheduled Vulnerability Scan] Enables regular automatic scanning.

[Action] It is recommended to set the vulnerability scan result to "No Action-Report Only", the network administrator will repair it according to the actual situation.

4.6 Alarm Policy

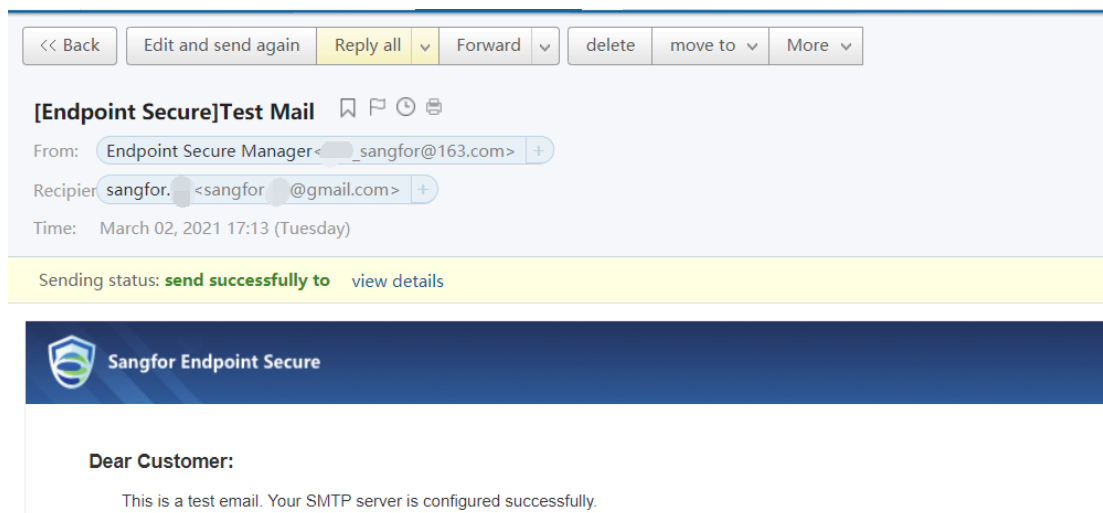
Configure alarm policies to notify the administrator in time when a threat event occurs on the intranet. The configuration steps are as follows:

1. Configure SMTP Server.

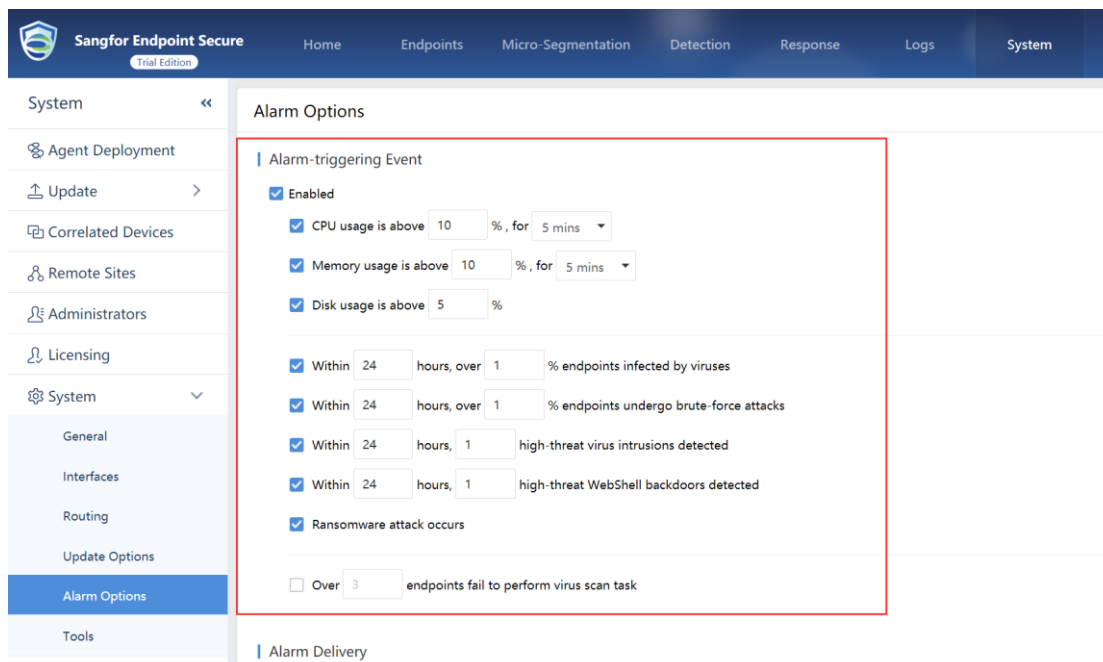


Click Send "Send Test Email", if you can receive the test email as shown in the figure below, it means that the mailbox server is configured successfully.

Endpoint Secure Security Policy Implement Guide for Host



2. Configure alarm policy.



3. Configure the recipient address, preferably as the mailbox of the network administrator.

Endpoint Secure Security Policy Implement Guide for Host

System <<

Agent Deployment

Update >

Correlated Devices

Remote Sites

Administrators

Licensing

System ▾

- General
- Interfaces
- Routing
- Update Options
- Alarm Options**
- Tools

Alarm Options

☒ Disk usage is above 5 %

☒ Within 24 hours, over 1 % endpoints infected by viruses

☒ Within 24 hours, over 1 % endpoints undergo brute-force attacks

☒ Within 24 hours, 1 high-threat virus intrusions detected

☒ Within 24 hours, 1 high-threat WebShell backdoors detected

☒ Ransomware attack occurs

☐ Over 3 endpoints fail to perform virus scan task

Alarm Delivery

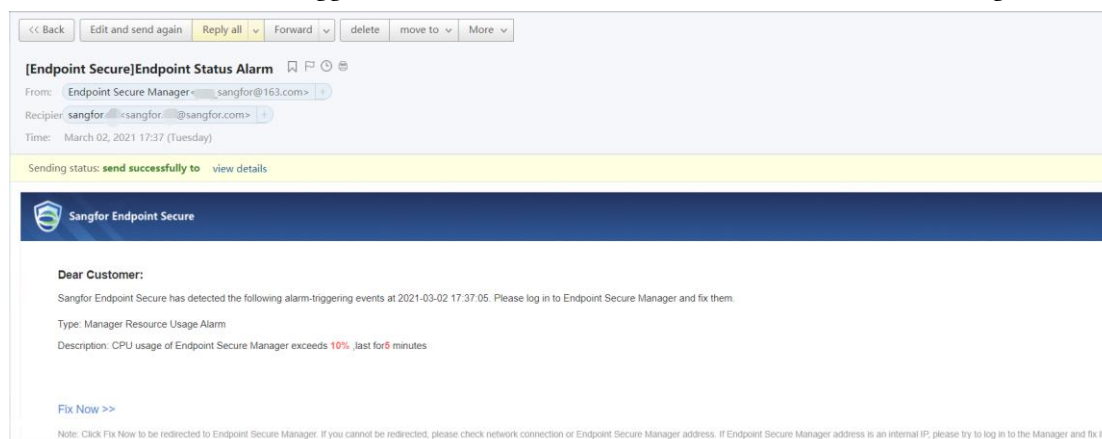
☒ Restrict email alarms

Within 1 hours, a maximum of 50 emails will be sent, and excessive ones will be sent next time

Name	Email address	Operation
sangfor	sangfor.yzj@sangfor.com	Delete

Save

When an alarm event is triggered, the network administrator will receive the following alarm email.





SANGFOR

Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc