SANGFOR

Endpoint Secure

Best Practices for Scenarios_Endpoint Secure Security Policy Implement Guide for Server

Version 3.2.22

Change Log

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

CONTENT

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 server security. The document includes two parts: identifying server security risks and implementing server security policies. Identifying server security risks guides users on how to identify client security risks in advance, makes users aware of the security risks and impacts of Server, and guides users to deal with security risks; implement server 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 server.

Chapter 3 Identify the Security Risks of Server

Identifying server 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 server, 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.

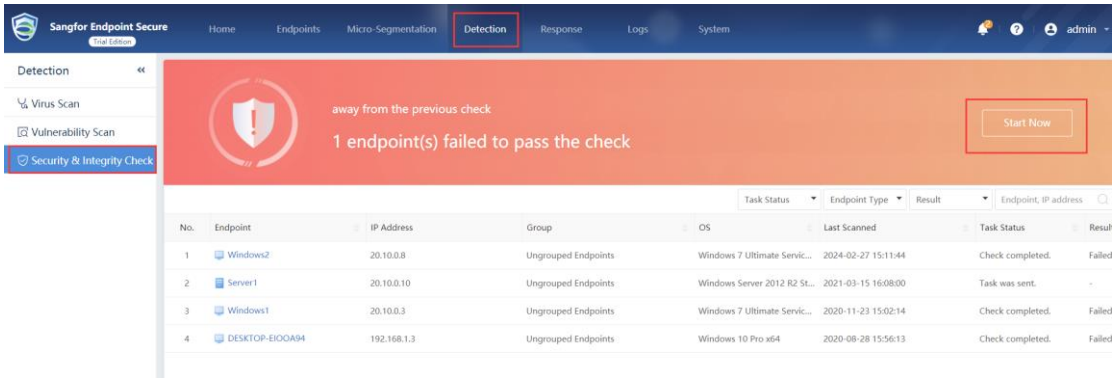
Note that if there are many servers, it is recommended to choose 1 or 2 servers to guide users on how to identify server security risks and how to deal with them.

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 terminals and non-compliant items in the intranet, and provide repair suggestions.

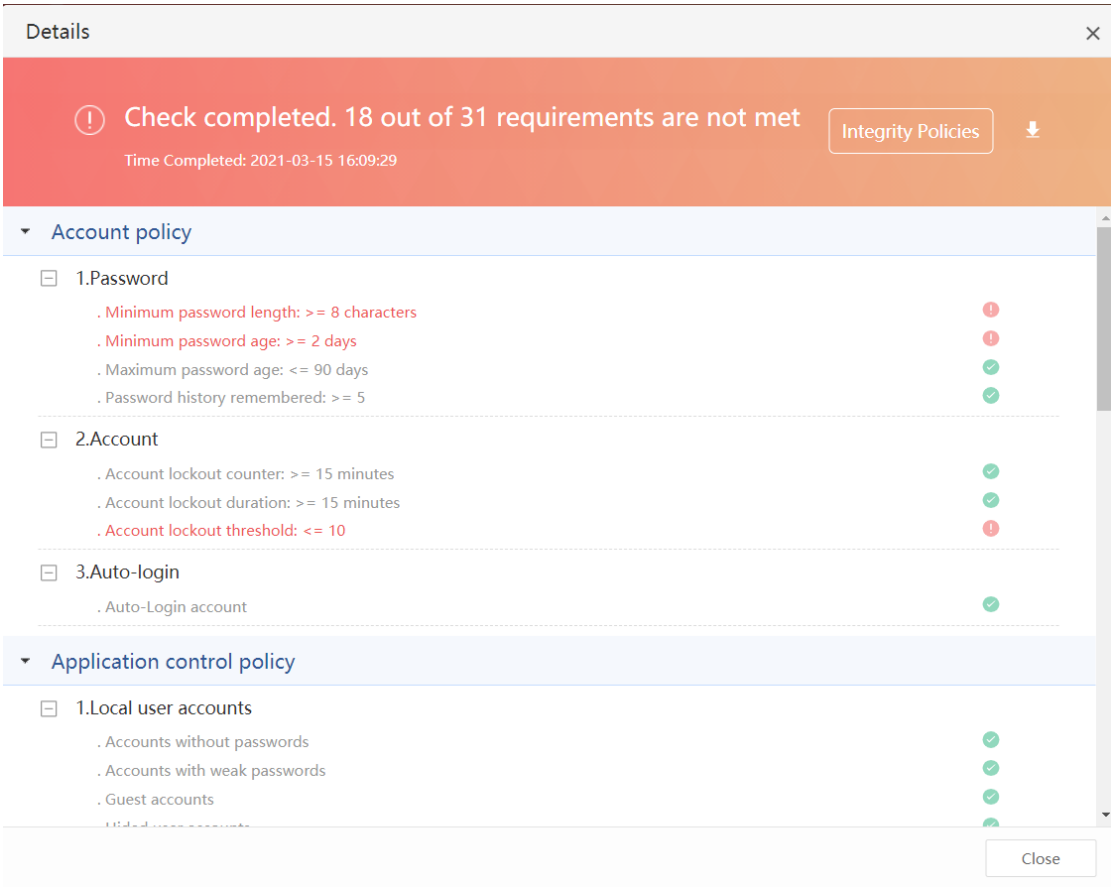
3.1.1 Security & Integrity Check

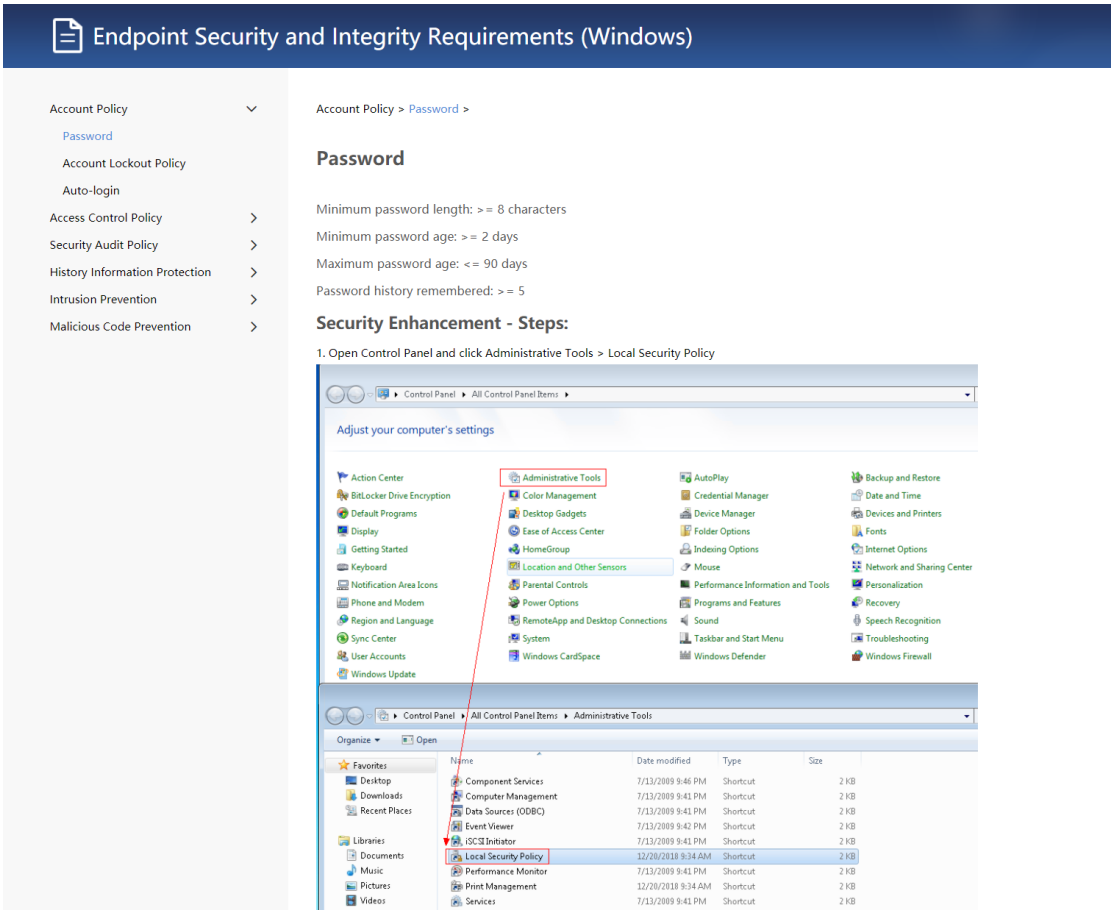
Go to Detection-> Security & Integrity Check, Perform basic security checks on the server.



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:


Details
Check completed. 18 out of 31 requirements are not met
Time Completed: 2021-03-15 16:09:29
Integrity Policies
Account policy
1.Password
. Minimum password length: >= 8 characters
. Minimum password age: >= 2 days
. Maximum password age: <= 90 days
. Password history remembered: >= 5
2.Account
. Account lockout counter: >= 15 minutes
. Account lockout duration: >= 15 minutes
. Account lockout threshold: <= 10
3.Auto-login
. Auto-Login account
Application control policy
1.Local user accounts
. Accounts without passwords
. Accounts with weak passwords
. Guest accounts
Close

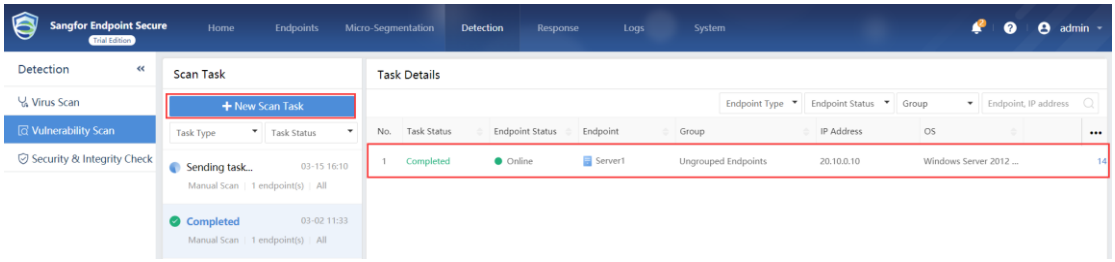

Endpoint Security and Integrity Requirements (Windows)
Account Policy
Password
Account Lockout Policy
Auto-login
Access Control Policy
Security Audit Policy
History Information Protection
Intrusion Prevention
Malicious Code Prevention
Account Policy > Password >
Password
Minimum password length: >= 8 characters
Minimum password age: >= 2 days
Maximum password age: <= 90 days
Password history remembered: >= 5
Security Enhancement - Steps:
1. Open Control Panel and click Administrative Tools > Local Security Policy
Adjust your computer's settings
Administrative Tools
Local Security Policy

3.2 System Vulnerability Check

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

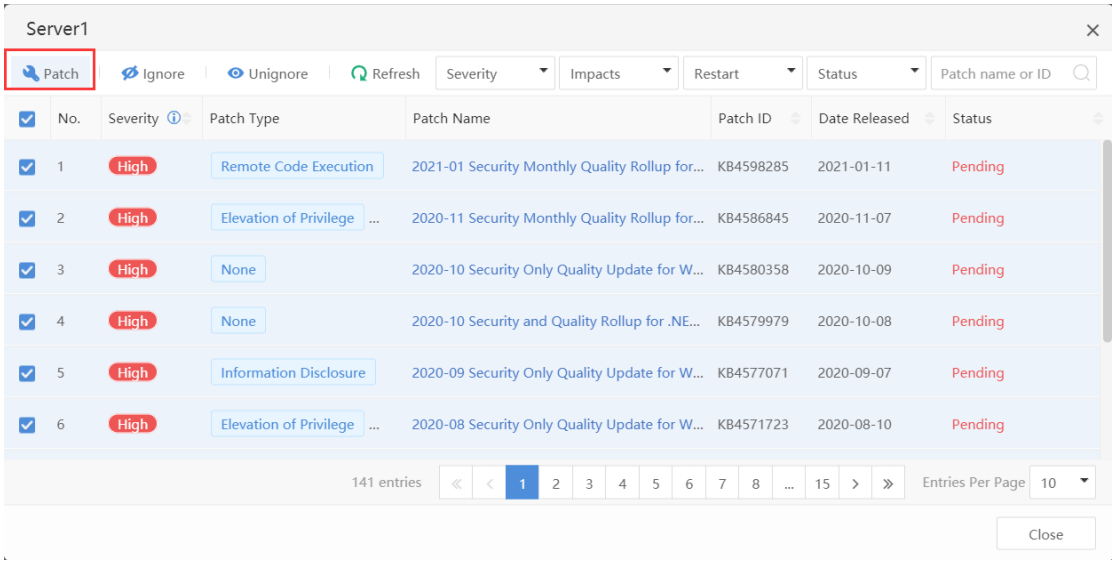
3.2.1 Vulnerability Check

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

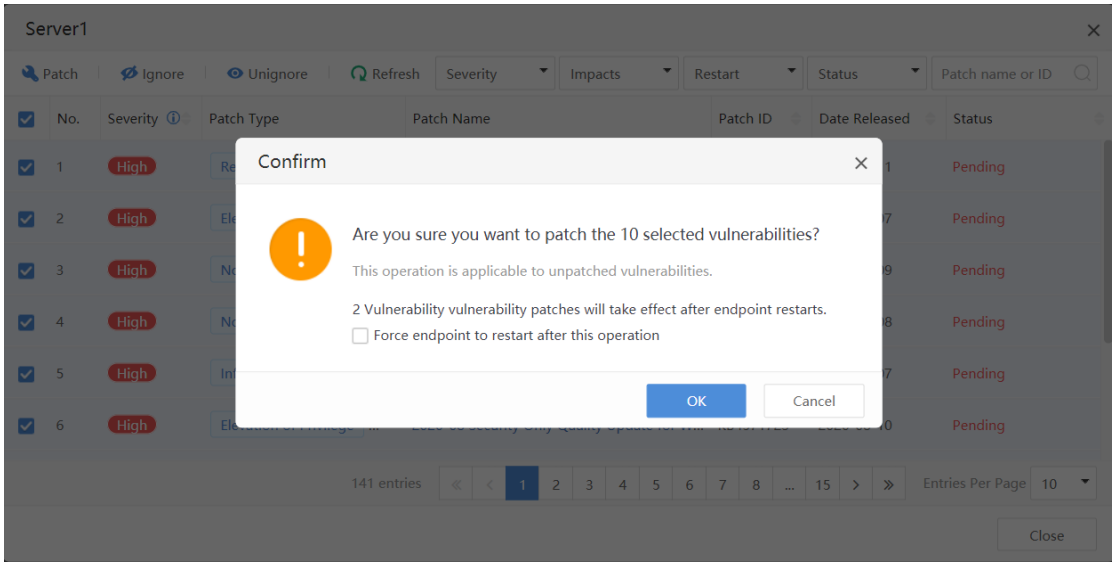


3.2.2 Dealing with Vulnerabilities

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 servers, 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.

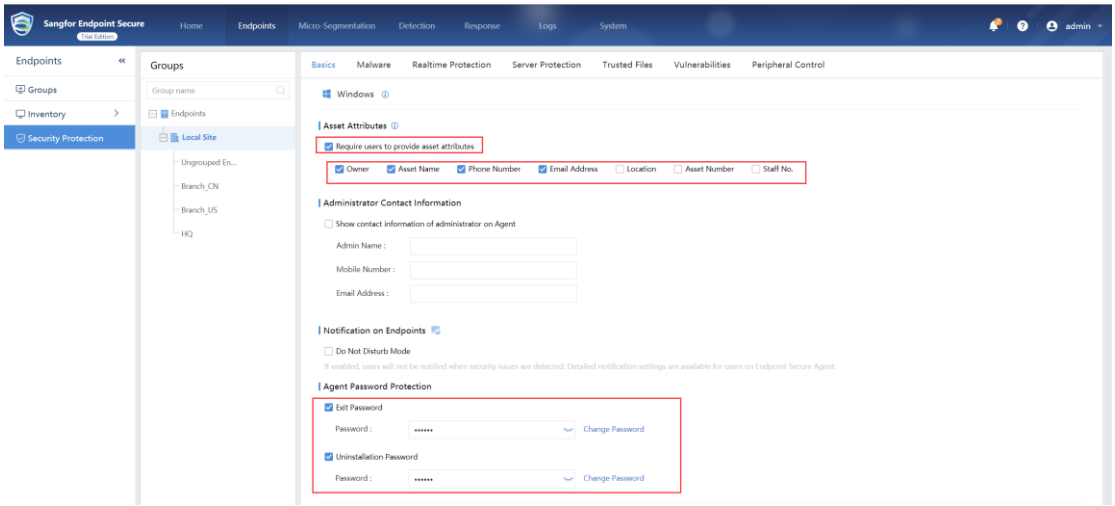
Promote the installation of other computers: the test computer is verified and the business is not affected, then it will be promoted to other computers in the same environment to install and kill.

Chapter 4 Server Security Policy Implementation Guidance

The implementation of server 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 server 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 server security.

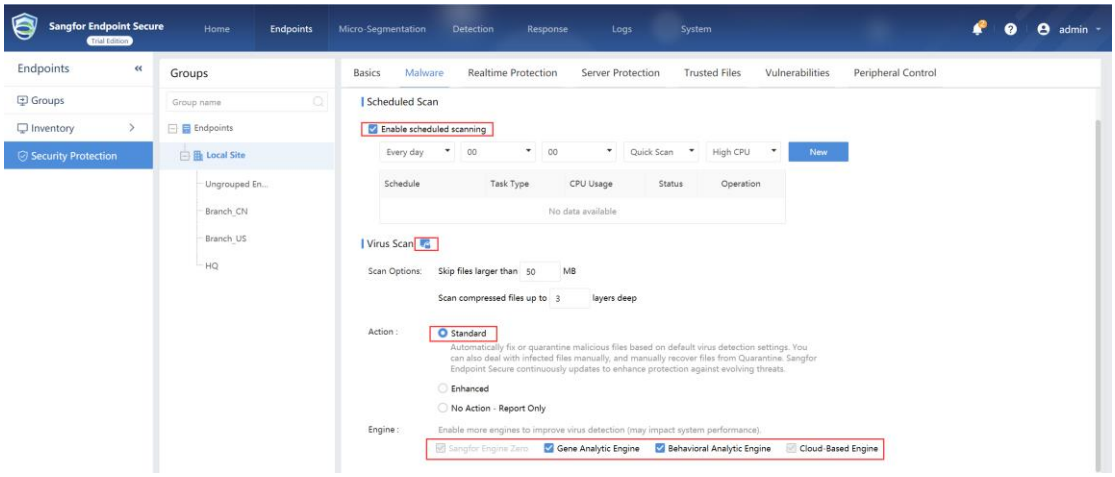
4.1 Basic Policy

Go to Endpoints->Security Protection path, configure the basic policy of the group where the servers are located, enable asset information registration, and set the terminal 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 servers are located, as shown in the following figure:

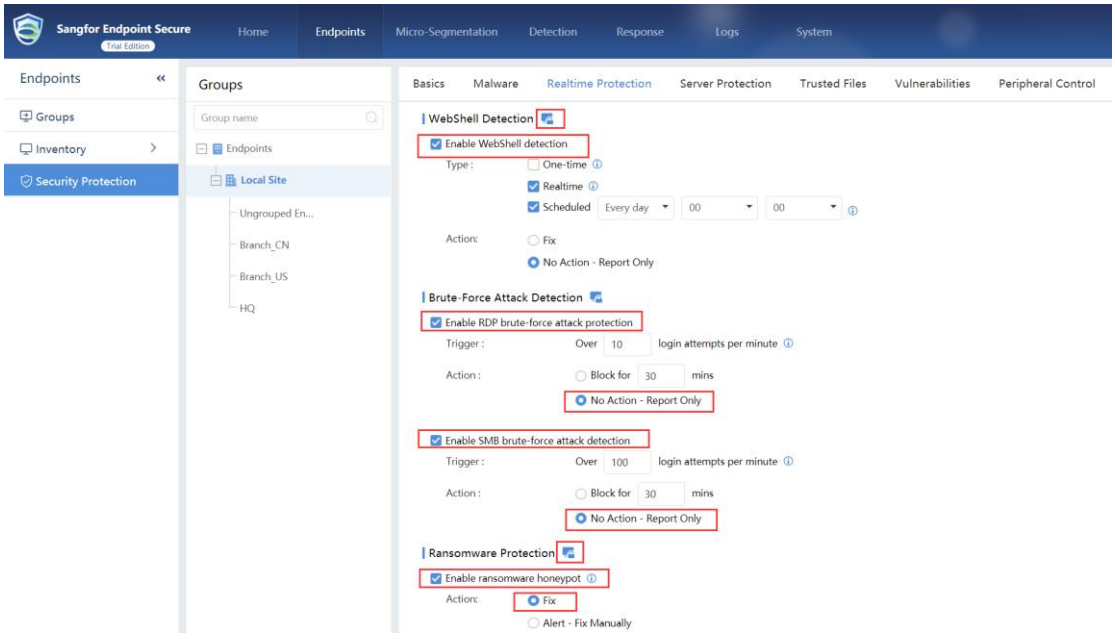


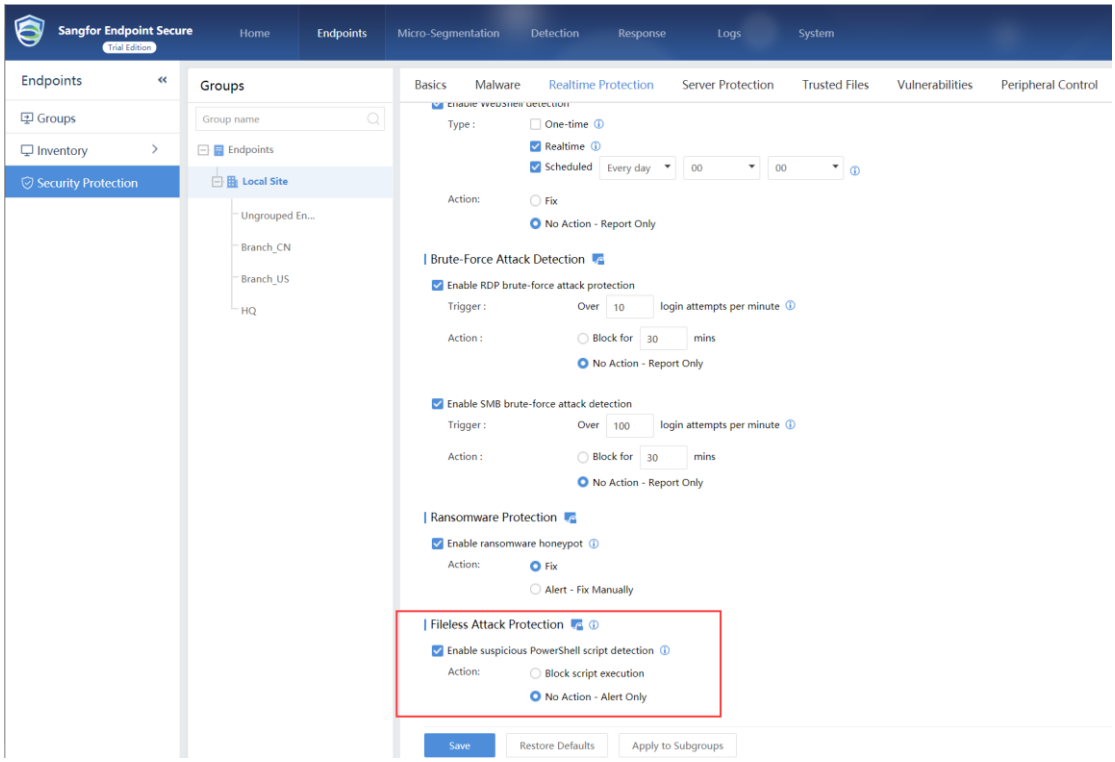
[Scheduled Scan] Turn on regular automatic scanning. It is recommended that the time to check killing intent is once a month, the scanning type is quick scanning, and the scanning mode is balanced.

[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 servers 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";

[File Type] 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 server'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"

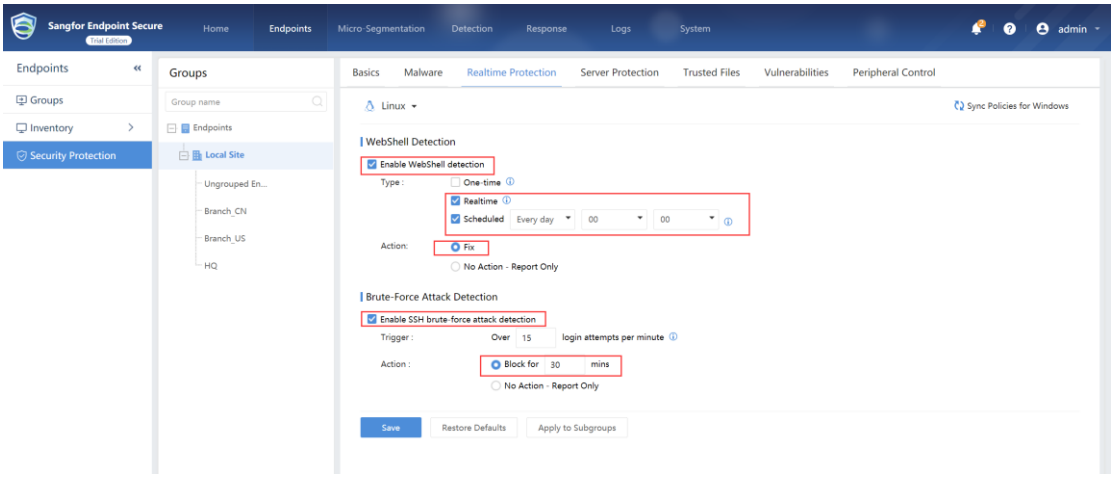
[Ransomware Protection] Enable the small lock icon on the right, and the ransomware protection policy will be sent from the management terminal to the ES agent.

[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".

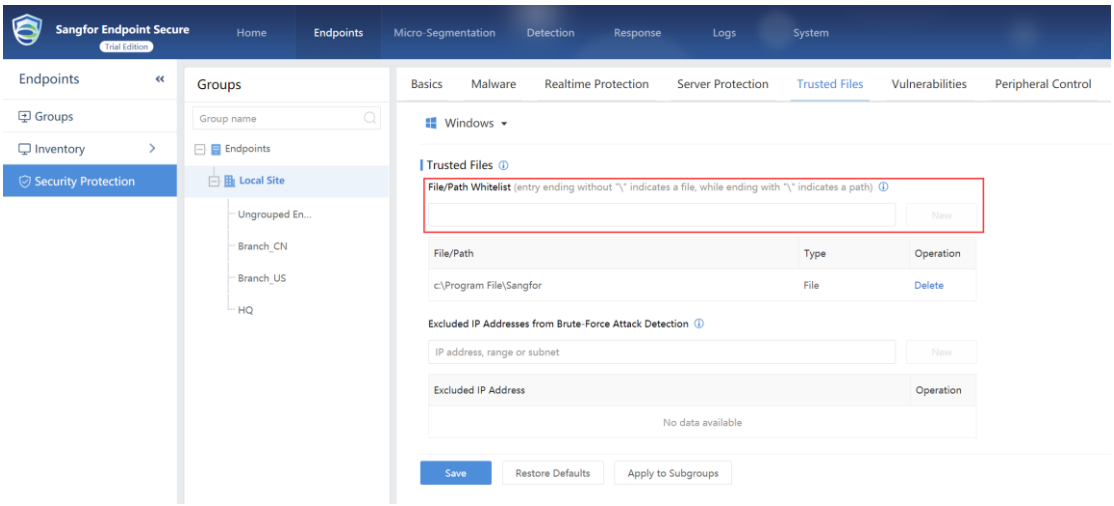
[Action] When a suspicious powershell script is found to be executed, it is recommended to set it to "Block script execution".

Set the Linux server real-time protection policy. The Linux server real-time protection policy only has webshell detection and brute force cracking detection, as shown in the figure below.



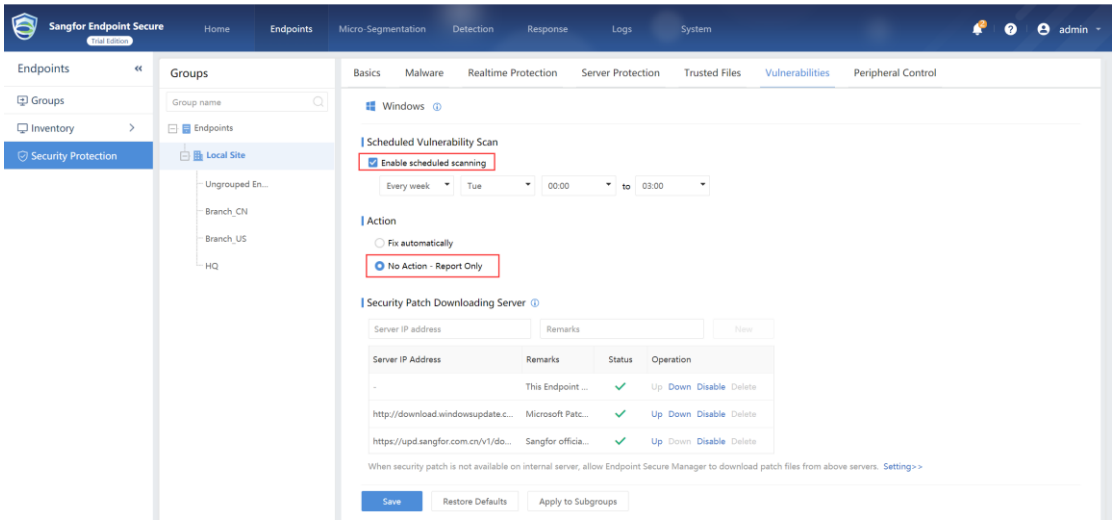
4.4 Trust Files

Go to Endpoints->Security Protection path, Configure the whitelist policy of the group where the server 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 servers 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 Micro-Segmentation Policy

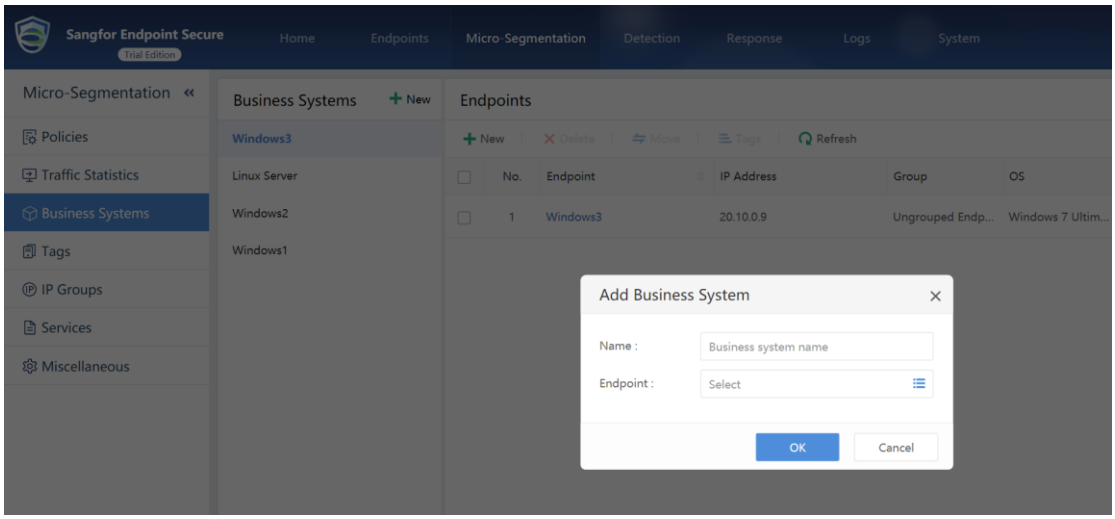
1. Micro-isolation is based on five-tuples to control the inbound and outbound traffic of the server to achieve the purpose of protecting the security of the server. It is recommended that necessary service ports can be released through the micro-isolation policy, and non-essential high-risk ports can be prohibited to improve service security. The configuration idea is as follows:

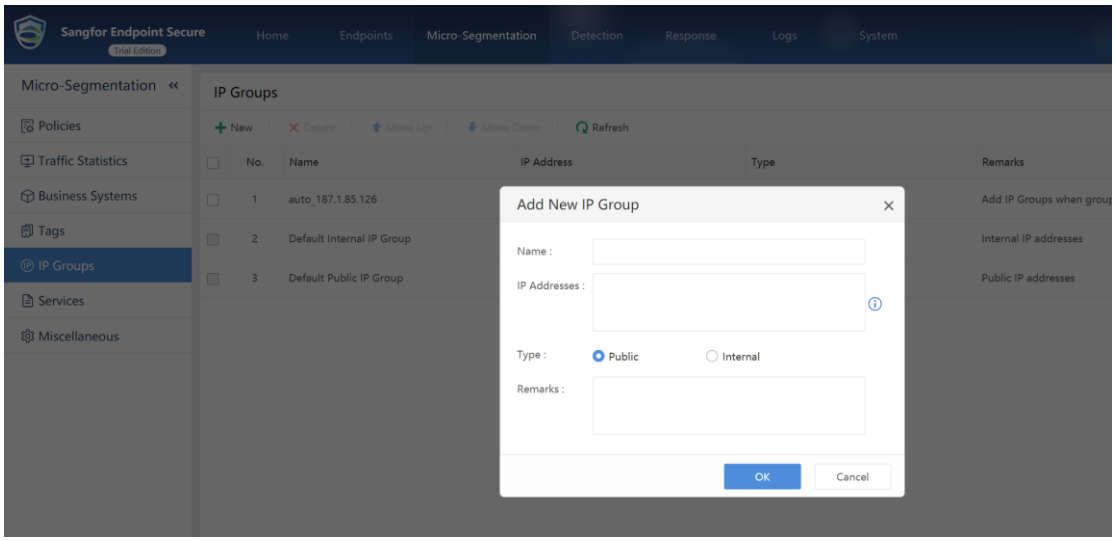
According to customer needs, sort out the access relationship between customer business system/IP/role/service and each object, and prepare for the following micro-isolation policy, as shown in the following table:

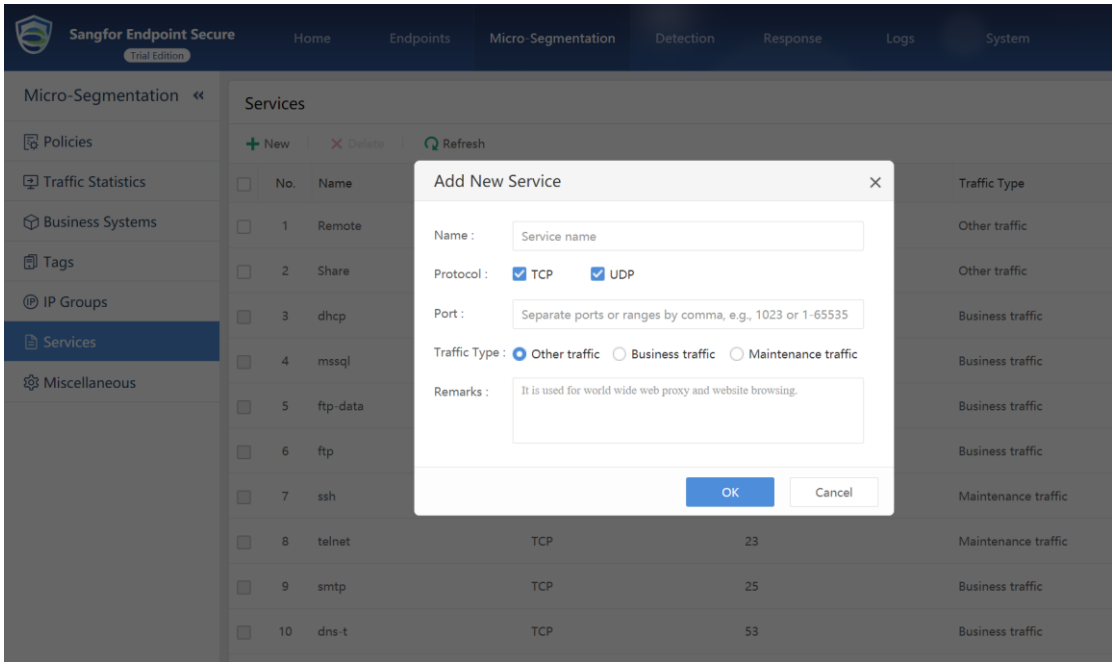
Objects	Business System	**Business System Name**	**Endpoint Group**	**Included Endpoints**	
		OA Server	Server Group	OA_WEB	
		Database Server	Server Group	Database Server	
	IP Group	**IP Group**	**IP Range**	**IP Group Type**	
		Office Endpoint	172.16.200.1-172.16.200.254	LAN	
	Services	**Services Name**	**Services Type**	**Port**	**Traffic Type**
		http	TCP	80	Business
		mysql	tcp	3306	Business
Access Relationship	Access Relationship	**Source**	**Destination**	**Services**	**Action**
		IP Group: Office Endpoint	Business System: OA Server	http	Allow

		Business System: OA Server	Business System: Database Server	mysql	Allow

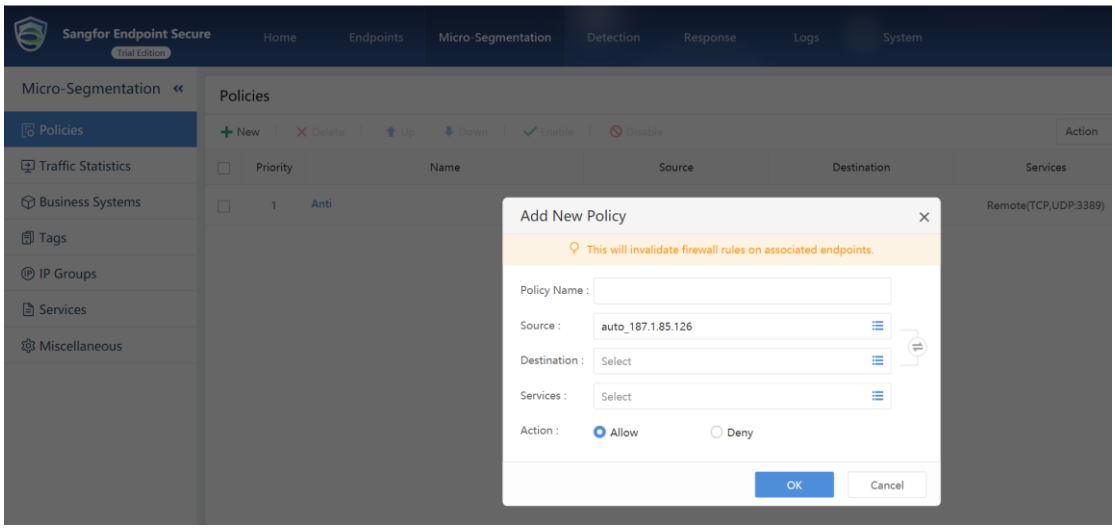
2. According to the content of the first step, define the business system/IP group/service, and call it in the micro-isolation policy, as shown in the figure below.



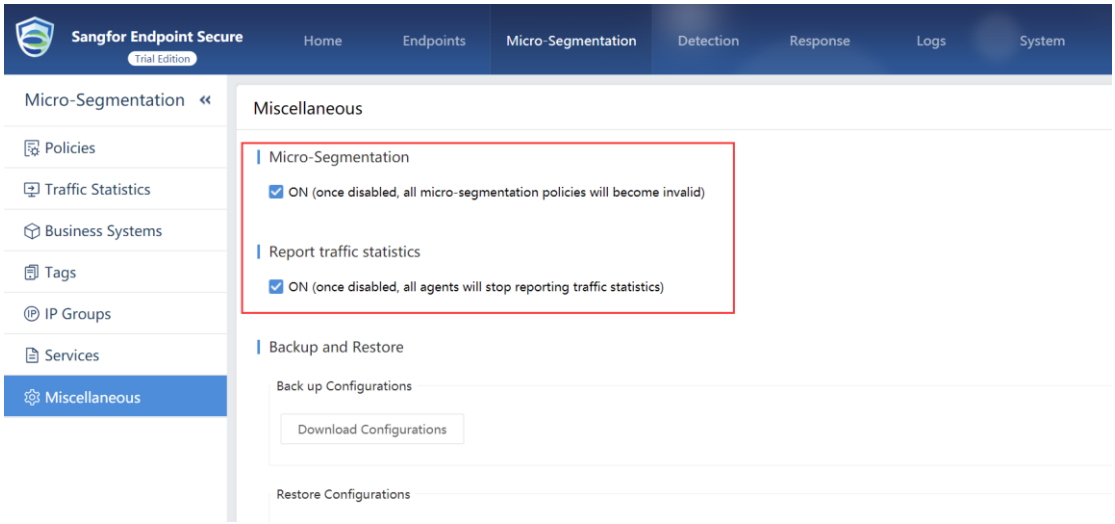




3. Define the micro-isolation policy. According to the access relationship sorted out in step 1 and the business system/IP group/service defined in step 2, define the micro-isolation policy, as shown in the figure below



4. Enable the micro-isolation policy switch and traffic report, as shown in the figure below.

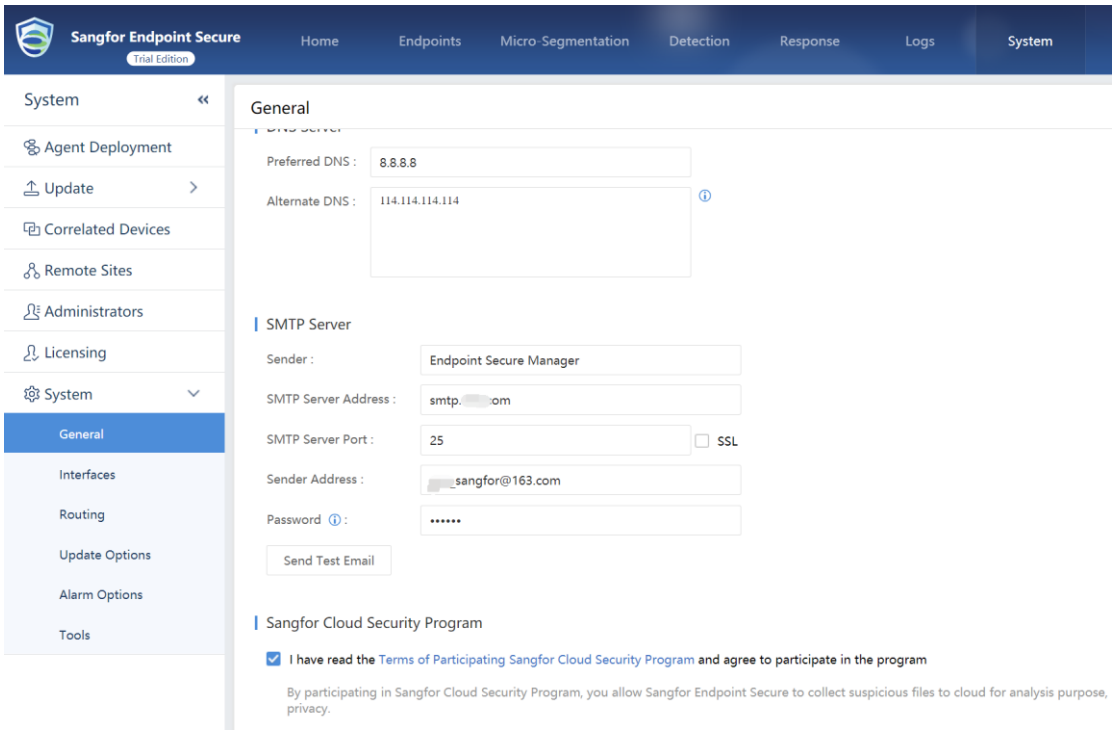


5. Verify the micro-isolation effect and test the server port connectivity.

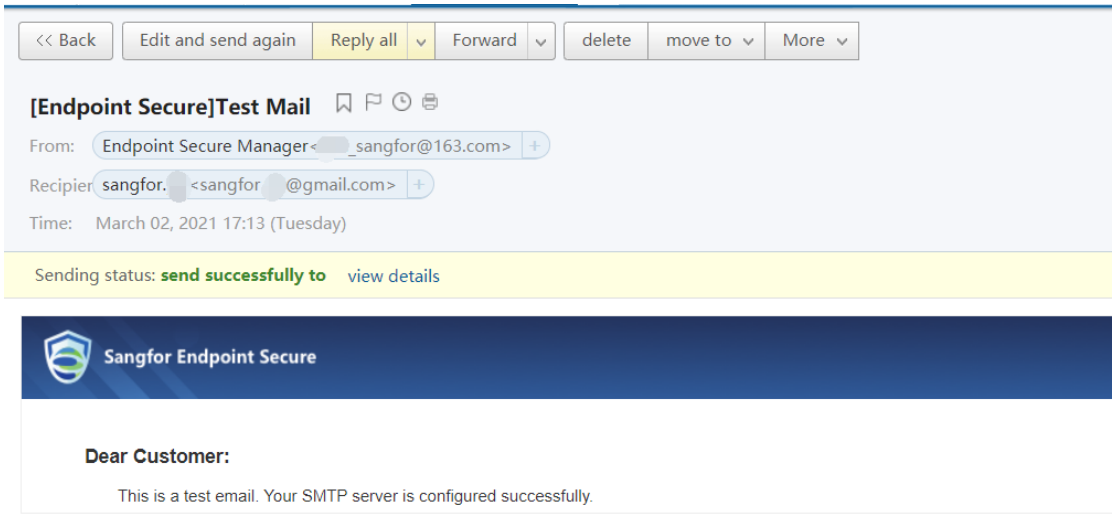
4.7 Alarm Policy

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

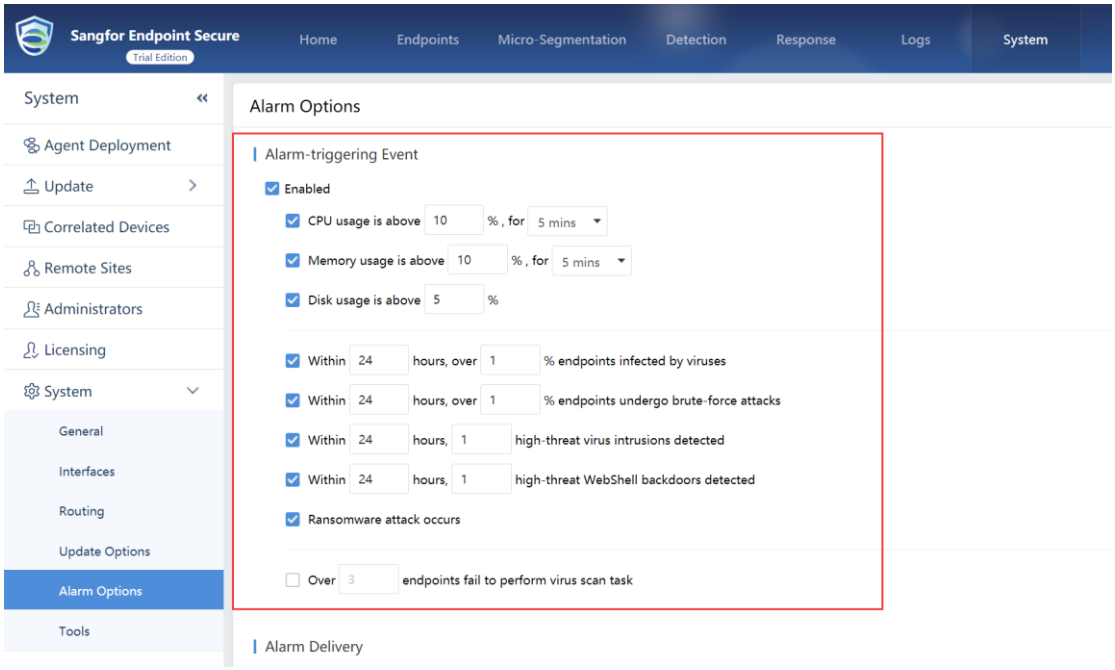
1. Configure SMTP Server.



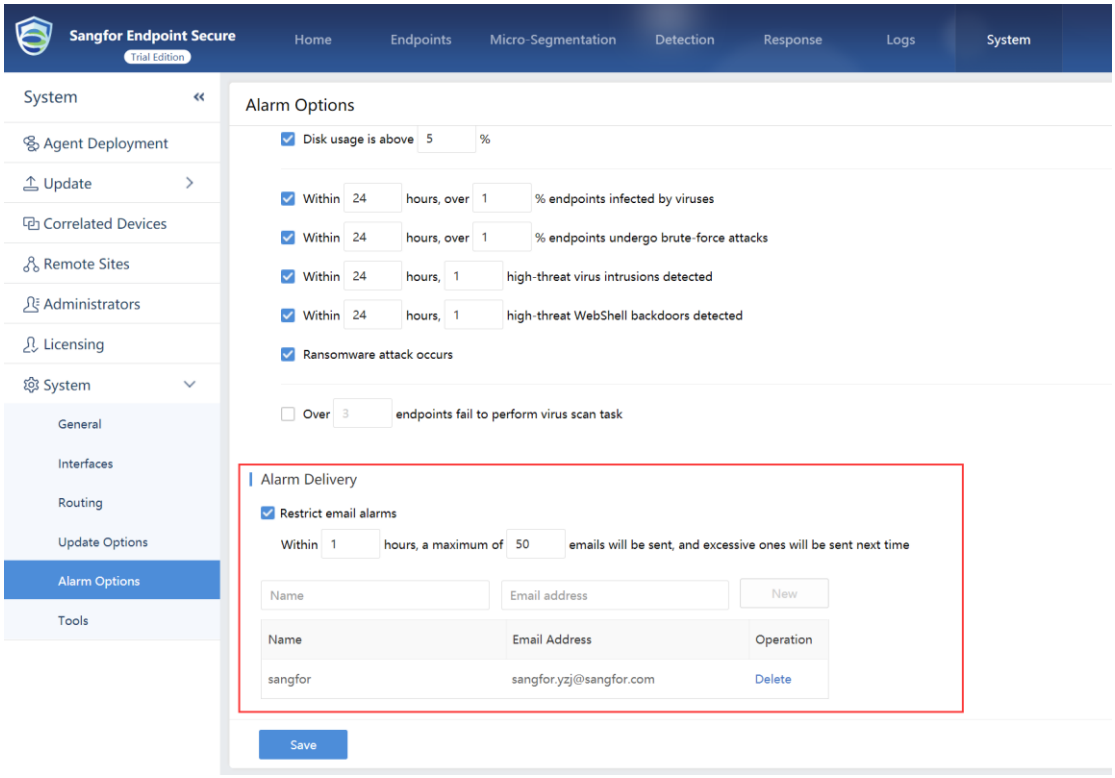
Click Send "Send Test Email", if you can receive the test email as shown in the figure below, it means that the mailbox server is configured successfully.



2. Configure alarm policy.



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



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