SANGFOR

Endpoint Secure

User Manual

Version 3.2.22

Change Log

Date	Change Description
June 22, 2022	Version 3.2.22 document release.

Contents

Declaration

Unless otherwise agreed, the manual is only for user guidance. Any descriptions, information, or suggestions in the manual do not constitute any explicit or implicit guarantee.

The contents of this manual are subject to change without prior notice.

For the latest manual, please contact Customer Service Department, Sangfor Technologies Inc.

Sangfor Technologies Co., Ltd. (hereinafter referred to as Sangfor Technologies Inc. or SANGFOR).

Preface

About This Manual

Chapter 1 Introduction to the Sangfor Endpoint Secure

Chapter 2 Endpoint Secure Installation and Deployment

Chapter 3 Initial Login to Sangfor Endpoint Secure Manager

Chapter 4 Installing Agent on Windows client computers

Chapter 5 Appendix

1. **This manual uses the Sangfor Endpoint Secure official version 3.2.22. There are some differences in configurations for different versions.**

Document Conventions

Graphical Interface Conventions

Text Description	Symbol	Example
Button	Border + Shadow + Shading	The "OK" button can be simplified to OK.
Menu Item		The menu item "System Setup" can be simplified to **System Setup.**
Continuously select menu items and submenu items	→	Select **System Setup→ Interface Configuration.**
Drop-down list, radio box, and check box options	**[ ]**	The check box option "Enable User" can be simplified to **[Enable User]**.
Window name	**[ ]**	For example, click to pop up the **[New User]** window.
Prompt message	“”	The prompt box displays "Configuration saved successfully, the configuration has been modified. The DLAN service needs to be restarted to take effect. Restart now?"

Abbreviations:

MGR: The Manager of Endpoint Secure installed on Linux server.

Agent: Endpoint Secure Protect Agent installed on endpoint.

IAM/NGAF/Cyber Command: Sangfor security products.

Symbol Conventions

This manual also adopts the following symbols to indicate the parts which need special attention to be paid during the operation:

Convention	Meaning	Description
	Caution	Indicates actions that could cause setting error, loss of data or damage to the device
	Warning	Indicates actions that could cause injury to human body
	Note	Indicates helpful suggestion or supplementary information

Technical Support

For technical support, please contact us through the following:

Email: tech.support@sangfor.com

Hotline: +60 12711 7129 (7511)

Sangfor Community: community.sangfor.com

Sangfor's service provider and service validity period inquiry:

http://community.sangfor.com/plugin.php?id=index:index

Official site: www.sangfor.com

Acknowledgement

Thanks for choosing SANGFOR.

If you have any comments or suggestions on our products or user manual, please feel free to give us feedback by phone, forum or email, we will be very grateful

Chapter 1 Introduction to Sangfor Endpoint Secure

Sangfor Endpoint Secure is a set of endpoint security solutions provided by SANGFOR, which consists of lightweight endpoint security software (Agent) and a manager (MGR).

The Endpoint Secure Manager supports unified asset management, virus scan and removal, security and integrity check for endpoints, micro-segmentation, malicious file quarantine and tracking hot security events across network.

The Endpoint Secure Agent can perform the anti-virus, intrusion prevention, firewall isolation, data collection and reporting, and fixing. Sangfor Endpoint Secure is also able to correlate to IAM, NGAF and Platform-X, forming a new generation of security protection system.

1.1 Major Values

Overall management of endpoint assets: Provide a comprehensive inventory of endpoint assets on the entire network, including servers and PCs, including name, IP address, MAC address, operating system, CPU usage, memory usage, group, owner, asset number, asset location of each endpoint. The asset information on each endpoint is visible and clear and every security event is responsibility to a specific person, so that security management can be put in place.

Security and integrity check: Every organization has its own endpoint security and integrity requirements, especially the integrity requirements for classified protection and the security requirements for the host. The integrity policy review of endpoint security is designed according to the host security requirements of the classified protection and the review of the account, access control, security audit, intrusion prevention, malicious code prevention and other policies are carried out to meet the host security requirements of the enterprise to build a classified protection system.

Real-time defense against Ransomware: Ransomware extorts a certain amount of ransom from the victim by encrypting files. Ransomware attack is becoming more and more popular and every day, and customers have feedback that they have been attacked. Sangfor Endpoint Secure can identify different ransomware families accurately. By running

professional analysis, Endpoint Secure can identify the infection behaviors and encryption features of various ransomware and effectively scan and remove the latest ransomware to prevent users from infection.

Active detection of intrusion attacks: Hosts were intruded and infected by ransomware or mining viruses, most of these intrusions were generated in a form of a weak password attack by brute-force. Sangfor Endpoint Secure actively detects brute-force attacks and blocks the IP addresses where attacks are being detected and actively detect of the backdoor files for Web security targeting attacks.

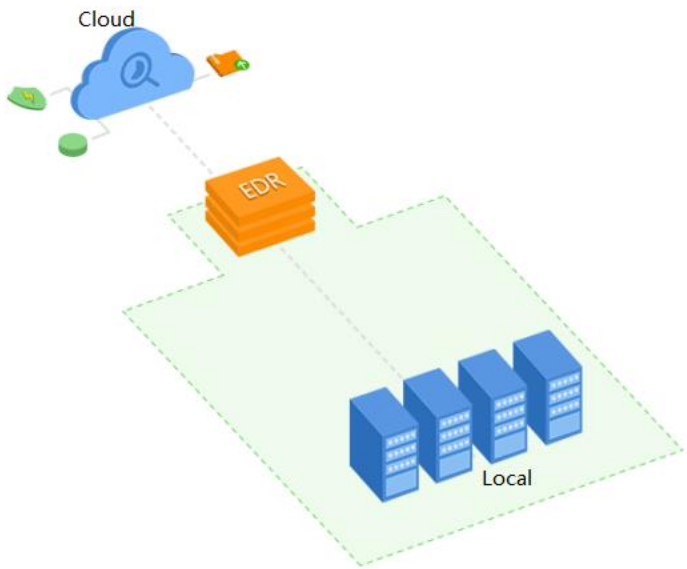
Proactive detection of intrusion attacks: Endpoints are attacked and infected with ransomware or mining viruses. Most of the attacks are implemented with the brute force against the weak passwords. Sangfor Endpoint Secure proactively detects brute-force attacks, and responds by blocking the attacker IP address. Endpoint Secure will actively detect the WebShell backdoor files to protect web security.

Rapid response to hot security events: Sangfor Neural-X can provide IOC intelligence for hot security events through the global security analysis for big data and push the intelligence data to Endpoint Secure. And it can quickly analyze the network-wide threats based on the IOC intelligence data, and timely detect and respond to the latest hot security events. It can analyze the root cause based on the historical behavior data so as to prevent organizations from breach notification.

Chapter 2 Endpoint Secure Installation and Deployment

2.1 Endpoint Secure Deployment

Sangfor Endpoint Secure is deployed in customer's network and the Agent is installed on each endpoint. The Endpoint Secure Manager consists of the software and the hardware. The software is deployed on Linux servers while the hardware is deployed in core network through bypass and centrally manages all Agents. Endpoint Secure Agent is installed on each endpoint. The MGR is linked with the Sangfor Security Cloud through the public network and each endpoint Agent in the intranet is connected to Endpoint Secure to provide accurate security information and solutions for the local endpoint users, and encrypt the communication process data. The deployment is as follows:



The implementation process of the local deployment of Endpoint Secure is as follows:

Step 1 - Download the installation package of agent and install it to the endpoints to be protected.

Step 2 - The Endpoint Secure Manager sends security policies to endpoints.

Step 3 - The endpoint performs virus scanning.

Step 4 - The endpoint reports the scanning results to the Endpoint Secure Manager.

Step 5 - The Endpoint Secure Manager reports the scanning results to the Sangfor security cloud for virus scanning and removal.

Step 6 - Cloud returns the scanning results to the Endpoint Secure Manager.

2.2 Endpoint Secure Manager Deployment

The MGR consists of software and the hardware. This section describes the Endpoint Secure Manager deployment. For the software, your service provider will deploy it for you when you purchase Sangfor Endpoint Secure.

2.2.1 Environmental Requirements

Endpoint Secure shall be used in the following environments:

- Input Voltage: 110V - 230V
- Temperature: 0 - 45℃
- Humidity: 5 - 90%

To ensure long-term and stable running, please make sure that the power supply is well grounded, dust-proof measures are taken, working environment is well ventilated and indoor temperature is stable. Endpoint Secure complies with the design requirements on environment protection. The placement, usage, and discard of the product should comply with relevant national laws and regulations where it is applied.

2.2.2 Power Supply

Endpoint Secure works with the power supply of AC 110V to 230V. Ensure that your power supply is well grounded before you power on.

2.2.3 Product Appearance

Figure 1: SANGFOR Endpoint Secure front panel (take Endpoint Secure-1000-B600 as an example)

1. The alarm light (identified as ALARM on the panel) is constantly red light during its startup. Generally, the red light goes out after one or two minutes, indicating the startup is normal. If the red light does not go out for a long time, please turn off the device and wait for 5 minutes before turning it on. If the red light remains on, please contact the Sangfor Support to determine whether the device is damaged. After the startup, sometimes the red light will flash, which is normal. A flashing red light indicates that the device is writing system logs.

2.2.4 Configuration and Management

You need a computer and make sure that the computer's web browser (such as Internet Explorer 10 or later versions) can run properly, then connect the computer to the eth0 port of the Endpoint Secure in the same LAN, and configure the device through the network.

The default IP address of the device's eth0 port is 10.251.251.251/24, and the computer logs in through the HTTPS standard port.

First, launch the browser, and enter in the address bar: https*://10.251.251.251.* Login page of Endpoint Secure Manager shows as follows:

Enter your username and password. Click Log In to log into Endpoint Secure Manager for configuration. The default username and password are: admin/admin.

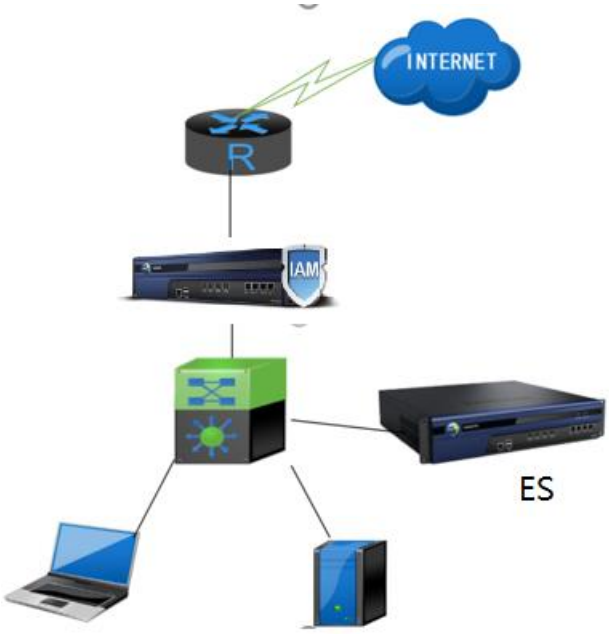
In order to protect manager security, administrator is prompted to change the default password after logging in to the Manager.

No controls are required for you to log in to the Manager. Internet Explorer 10 or later versions, Mozilla Firefox, and Google Chrome are supported for the login.

2.2.5 Network Connection

Connect the eth0 port of the device to the intranet switch (as shown below) with the standard RJ-45 Ethernet cable, and ensure that the Endpoint Secure device can communicate with the endpoints in the intranet properly.

Plug the power cable into the rear panel of the device, and then power on. At this time, the power indicator (green) and alarm indicator (red) in the front panel will be on. The alarm indicator will go out in one or two minutes, indicating the gateway is working properly.



2.3 Installing Agent on Client Computers

2.3.1 Open Ports

The following are ports used by the endpoints having Endpoint Secure Agent installed to access Sangfor Endpoint Secure Manager. These ports need to be allowed.

Port	Description
443	Used to visit Sangfor Endpoint Secure Manager
8083	Used for inter-process communication (IPC)
54120	Used to stop Endpoint Secure services in emergency and recover businesses services

2.3.2 Agent Installation

Once the Endpoint Secure Manager is set up, the Agent needs to be installed on the endpoints. This will enable endpoints to connect with the Endpoint Secure Manager, to realize real-time protection of endpoints.

Download the installation package of Agent from Sangfor Endpoint Secure Manager. Installation packages for Linux and Windows operating systems are available. Detailed list is as follows:

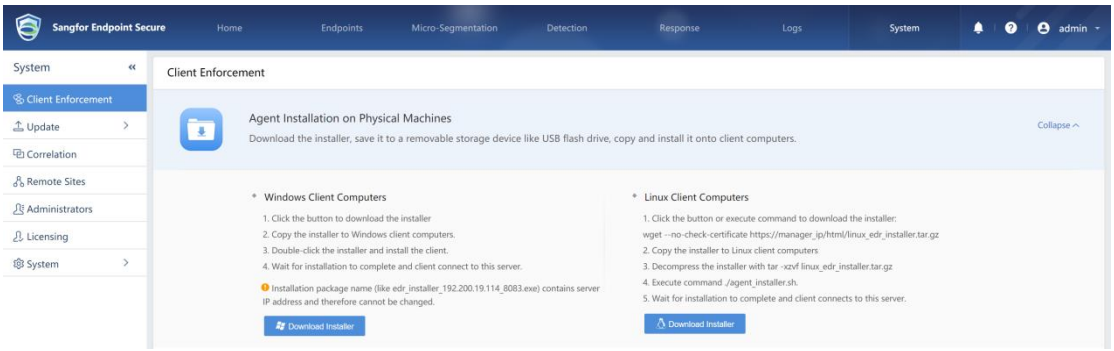
Operating System Type	Operating System	Endpoint Type
Windows	WinXPsp3	User Endpoint
	Win7	User Endpoint
	Win8	User Endpoint
	Win8.1	User Endpoint
	Win10	User Endpoint
	win2003	Server
	Win2008	Server

	Win2008R2	Server
	Win2012	Server
	Win2016	Server
	Win2019	Server
Linux	CentOS 5	Server
	CentOS 6	Server
	CentOS 7	Server
	Ubuntu 10.04	Server
	Ubuntu 11.04	Server
	Ubuntu 12.04	Server
	Ubuntu 13.04	Server
	Ubuntu 14.04	Server
	Ubuntu 16.04	Server
	Debian 6	Server
	Debian 7	Server
	RHEL 5	Server
	RHEL 6	Server
	RHEL 7	Server
	Suse 12	Server
	Oracle Linux	Server
32-bit Linux	CentOS 5	Server
	CentOS 6	Server
	CentOS 7	Server
	Ubuntu10.04	Server

	Ubuntu13.04	Server
	Ubuntu 16.04	Server
	Debian6	Server
	RHEL5	Server
	Oracle Linux	Server

The following describes how to install the endpoint Agent:

Go to **System** > **Client Enforcement** to download Agent installer from Sangfor Endpoint Secure Manager.

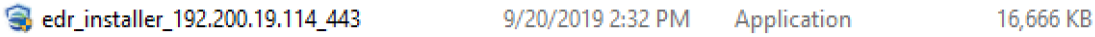


Or download it directly from Sangfor Endpoint Secure Manager login page.

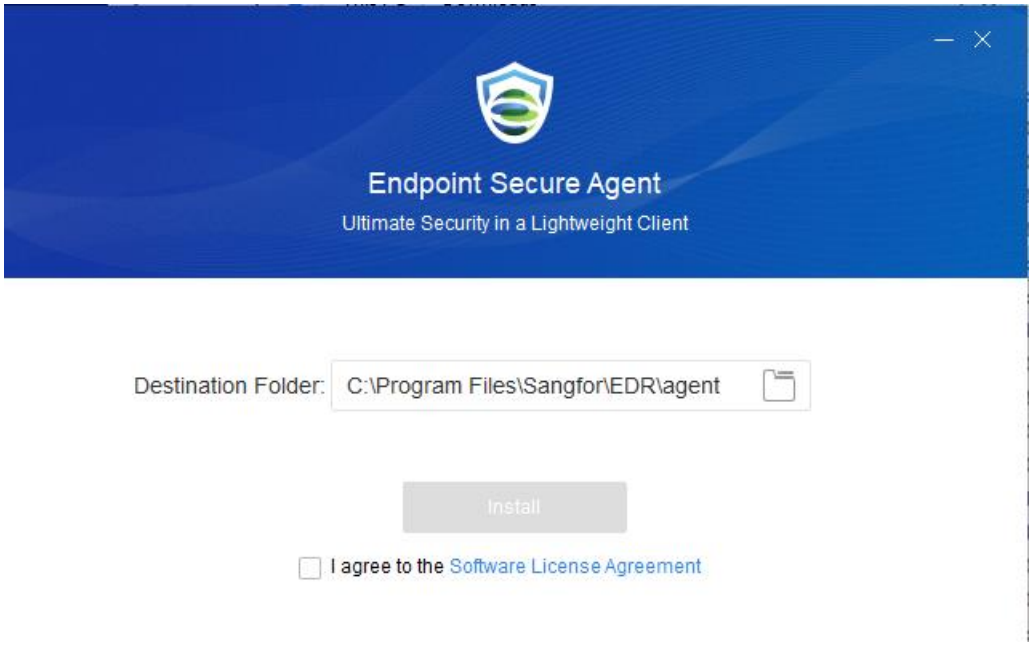
2.3.2.1 Installing Agent on Windows Client Computers

Network Check: Check whether the communication between client computer and Sangfor Endpoint Secure Manager is normal. The telnet command used to install the Agent checks whether they can communicate normally via the ports 443, 8083 and 54120.

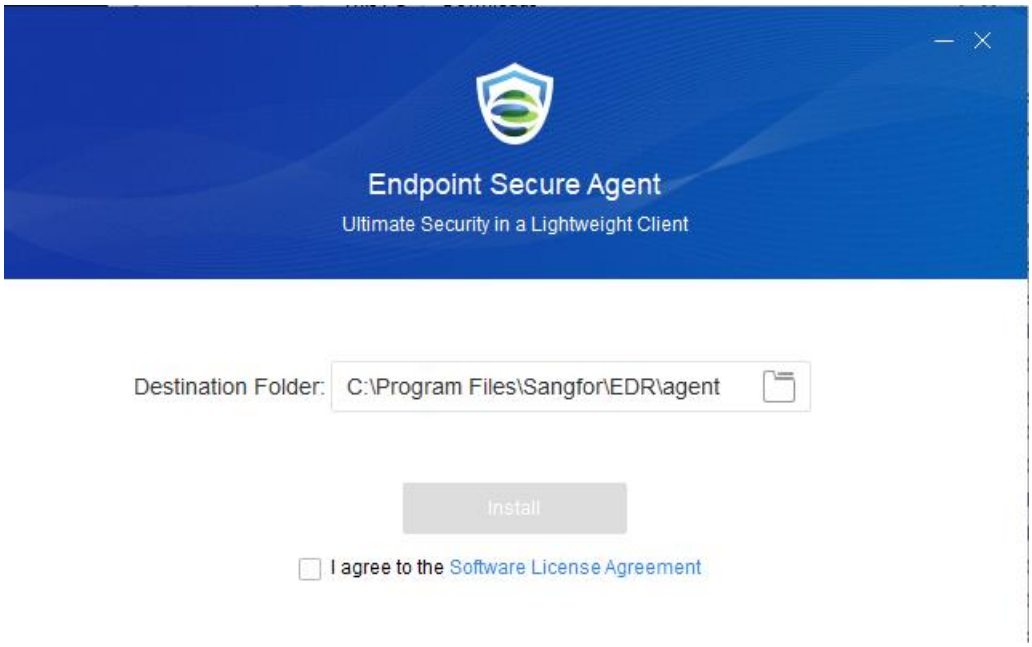
Click the **Windows** button under the **Windows Client Computers** to download the Agent installer.



Double click the installer to start installation.



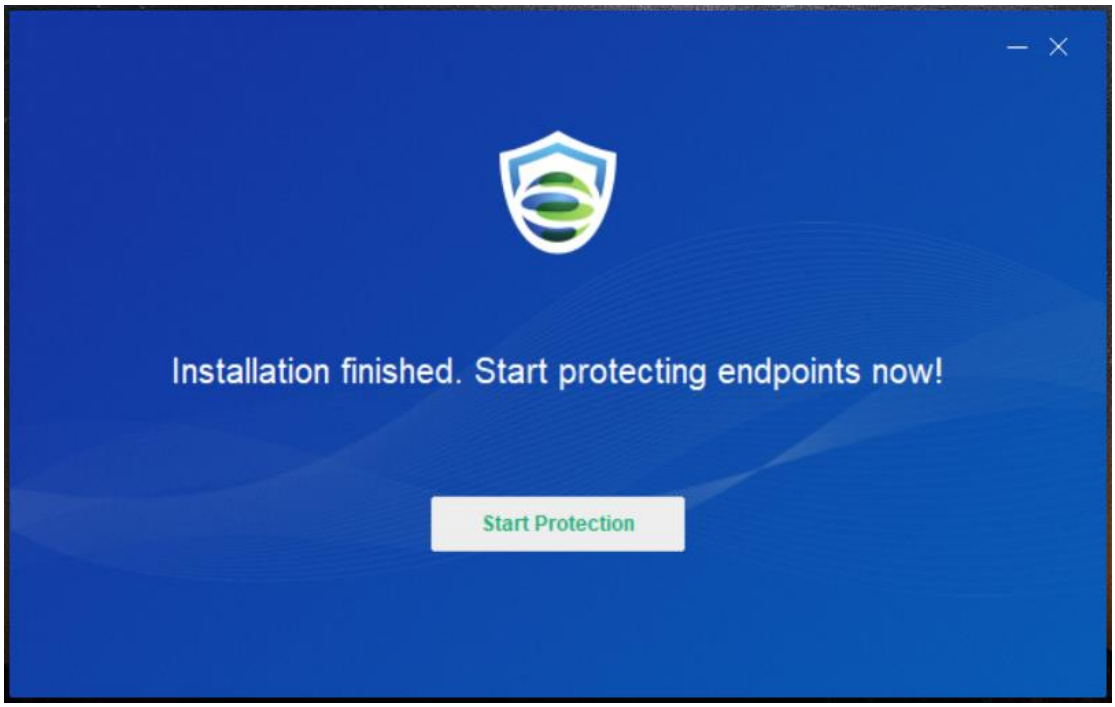
Select the destination folder, the default is C:\Program Files\Sangfor\EDR\agent by default. If there is any other anti-virus software on the endpoint, the following information will be prompted, as shown below:



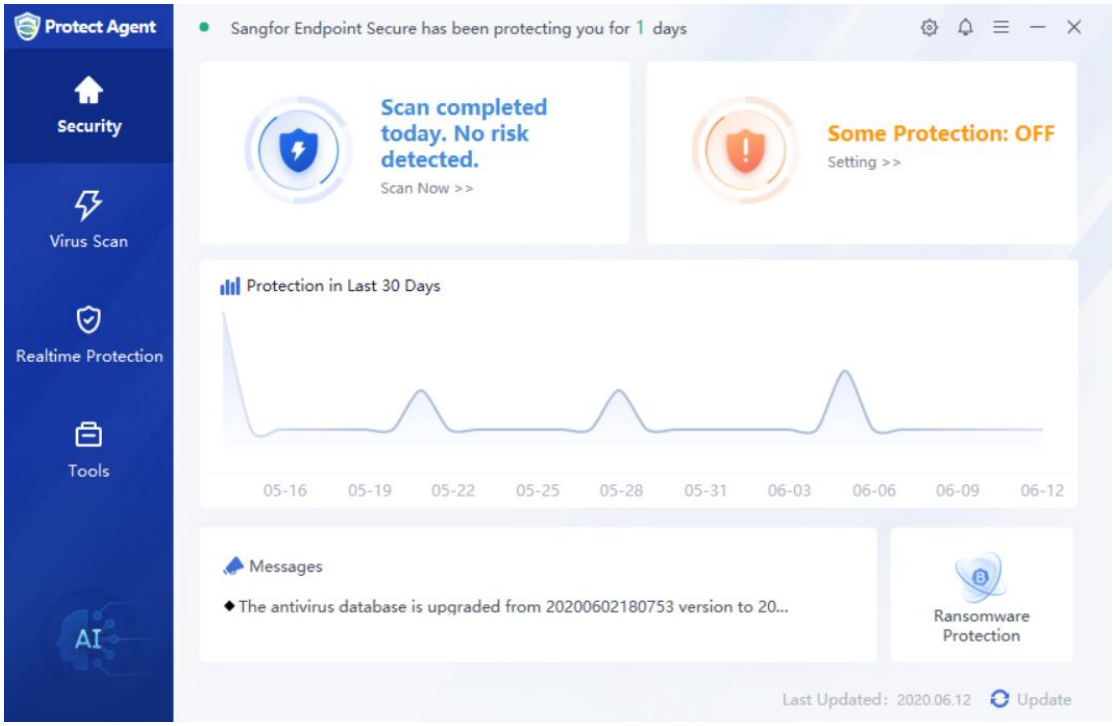
Check the option **Install in compatibility mode anyway and use Realtime protection later if necessary,** on the above dialog to continue the installation, but this will disable the real-time file monitor function. It is recommended to uninstall other anti-virus software before installation.

Then, click **Continue** to proceed and installation starts, as shown below:

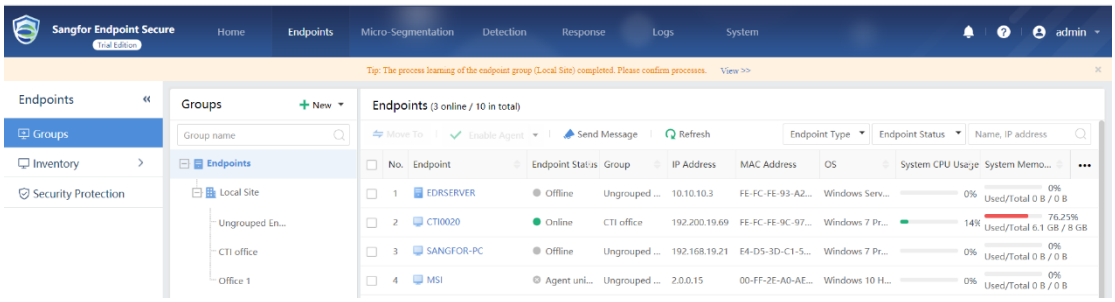
The figure below shows that installation is completed:



Click **Start Protection** button to enable protection for the endpoint.



After the installation, the Agent will automatically connect to Endpoint Secure. Wait for about 2 minutes, you can see the endpoint status shown as "Online" in **Endpoints > Groups** (as shown below) in the Manager.



1. The following describes different ways to uninstall Agent

1) On the Windows Menu, find and run the Endpoint Secure Agent uninstall program.

2) In the Control Panel > Programs and Features, choose the Endpoint Secure Agent and click Uninstall.

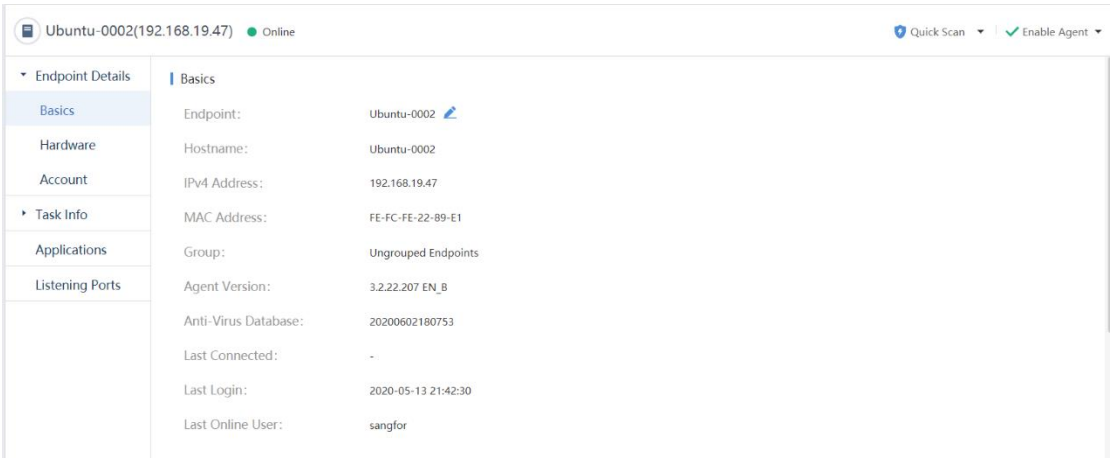
3) Find the uninst.exe file under the installation directory (C:\Program

Files\Sangfor\EDR\agent), double-click it to start uninstallation and then the endpoint is removed from the Endpoint Secure Manager after uninstallation.

2. Uninstall Agent directly through Sangfor Endpoint Secure Manager. In the Endpoints > Groups find and select the endpoint that you want to uninstall Agent from and then click Uninstall Agent. For details, see the Section 3.3 Endpoints.

3. Agent GUI is only available on the following Windows versions: Windows XP, Windows 7, Windows 8, Windows 8.1, Windows 10, exclusive of Windows Server.

2.3.2.2 Installing Agent on the Linux Client Computers



Method 1:

Run the following command to download the Agent installation pack to the current directory where wget is located.

1. wget --no-check-certificate https://%mgrdcip%/html/linux_edr_installer.tar.gz
2. Copy the installer to Linux computers.
3. Decompress the installer with tar -xzvf linux_edr_installer.tar.gz.
4. Execute command ./agent_installer.sh.
5. Wait for installation to complete and the Agent connects to this manager.

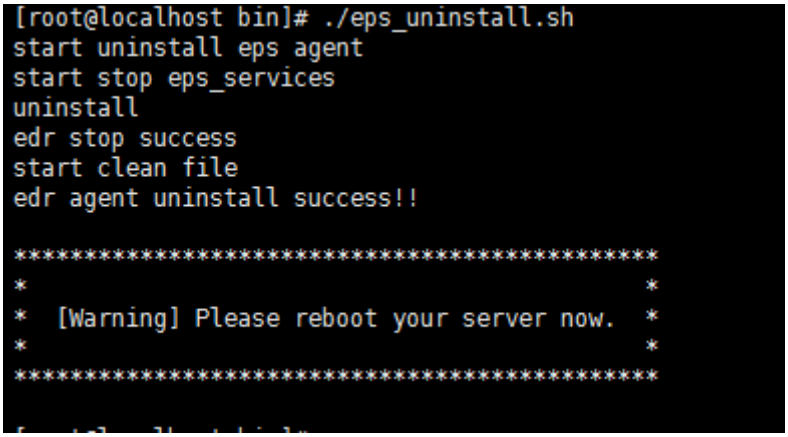
1. The manager_info.txt file is used to ensure that the endpoints connect to the Sangfor Endpoint Secure Manager to keep Agent up-to-date.

2. Uninstallation methods of Agent on Linux: Once the installation is completed, the

eps_uninstall.sh script is generated in the bin directory of the installation folder; run this script to uninstall the Agent.

3. If the file directory cannot be found, use find / -name eps_uninstall.sh to find it.

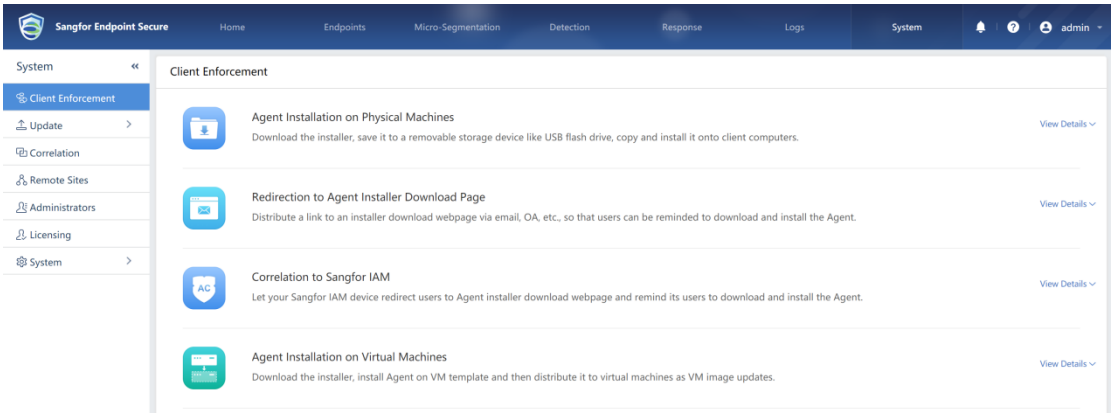
4. The successful installation of Agent on the Linux client computers requires that the endpoint can ping the Endpoint Secure Manager successfully.



To improve the performance of the endpoint, it is recommended to install ipset on the Linux client computer with micro-segmentation enabled.

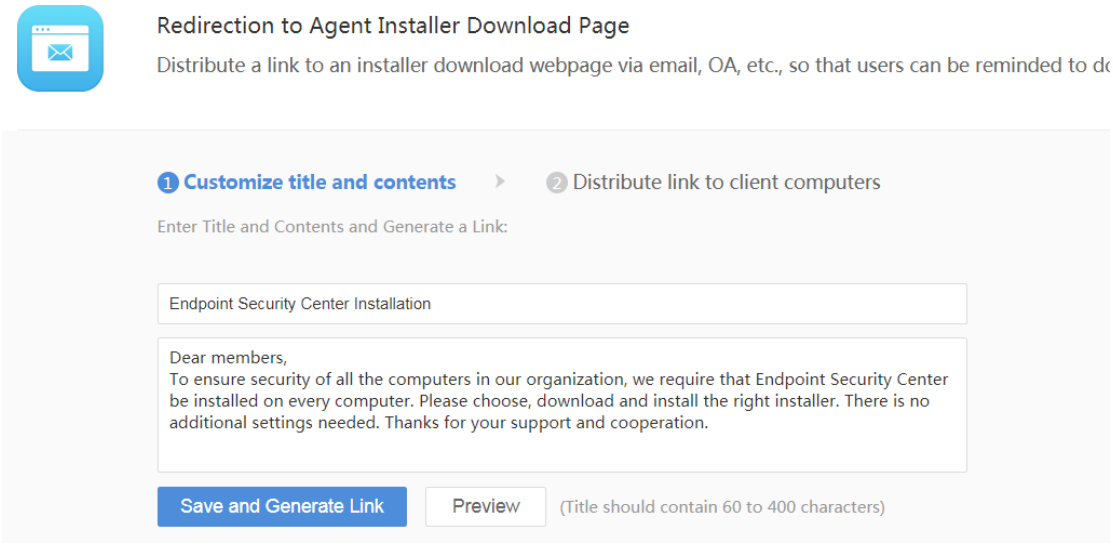
2.3.2.3 Other Installation Methods

In **System**> **Agent Client Enforcement**, you can also install Agent through **Redirection to Agent Installer Download Page**, **Correlation to Sangfor IAM** and **Agent Installation on Virtual Machines**

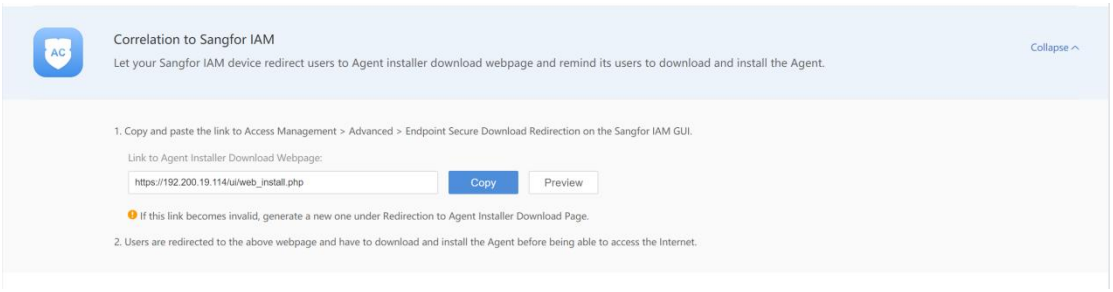


Redirection to Agent Installer Download Page: Distribute a link to an installer download

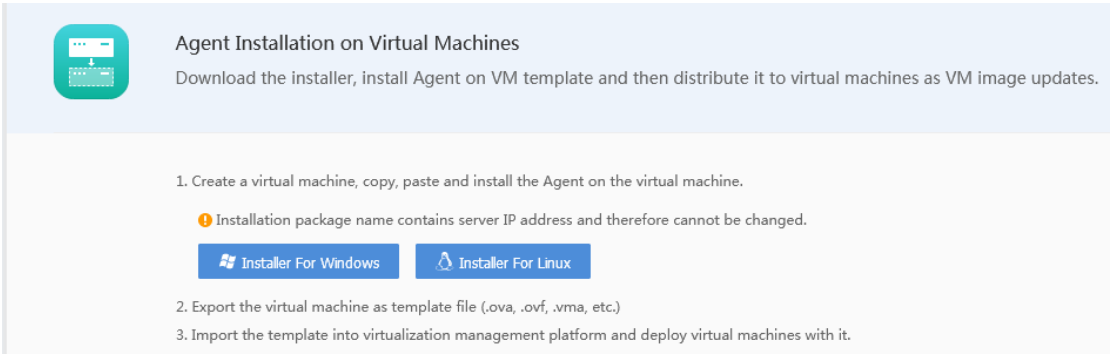
webpage via email, OA, etc., so that users can be reminded to download and install the Agent.



Correlation to Sangfor IAM: Let correlated Sangfor IAM to redirect users to Agent installer webpage. And then Agent is downloaded and installed on endpoints. For detailed configuration, see Section 3.6.3 Correlation.



Agent Installation on Virtual Machines: Download the installer, install Agent on VM template and then distribute it to virtual machines as VM image updates.



Endpoint Secure requires signature database update by connecting to Internet. In

order to obtain timely and effective protection, please make sure that MGR and Agent can connect to the Internet and the following servers:

auth.sangfor.com.cn

upd.sangfor.com.cn

download.sangfor.com.cn

analysis.sangfor.com.cn

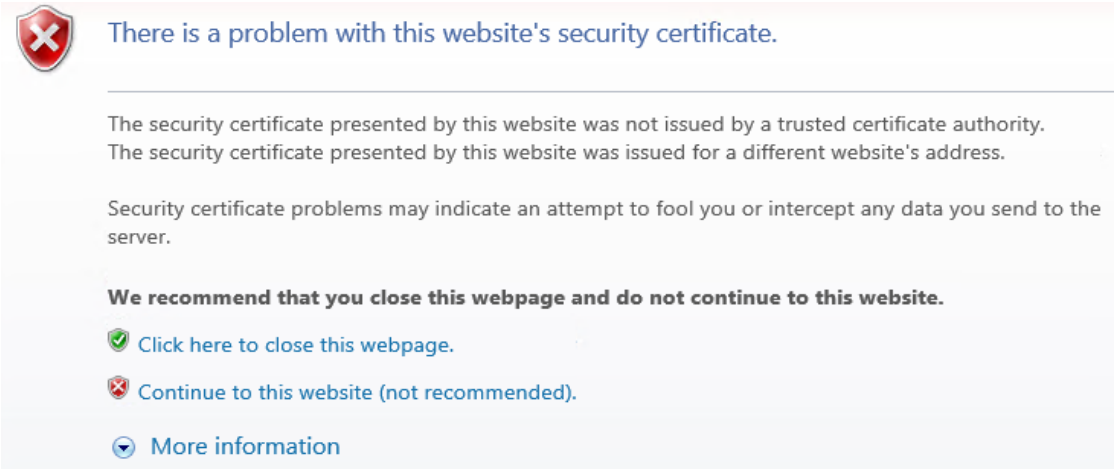
clt.sangfor.com.cn

Chapter 3 Initial Login to Sangfor Endpoint Secure Manager

3.1 Logging into Endpoint Secure Manager

Sangfor Endpoint Secure Manager provides web-based administration through standard HTTPS port. The default login URL is https://*EDR_IP*. (EDR_IP is the IP address of the Linux server where the Endpoint Secure Manager is installed)

Open a browser, enter default Endpoint Secure Manager address and port into the address bar and then press the Enter key. A security prompt appears, as shown below:



.

Click **Continue to this website** as shown below:

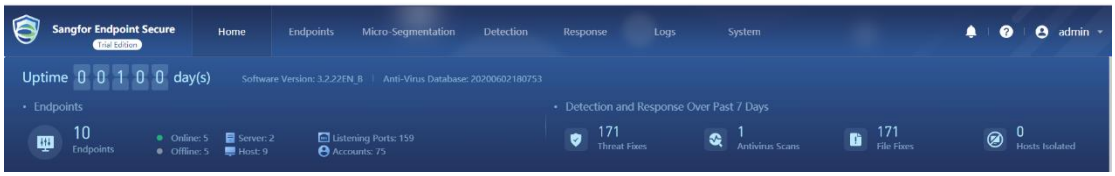
Enter the username and password, click the **Log In** button to log in to the Endpoint Secure Manager. The default username and password are **admin**.

The initial login does not need to install any ActiveX controls. Administrators can use IE9 or later, Firefox or Chrome to visit Sangfor Endpoint Secure Manager.

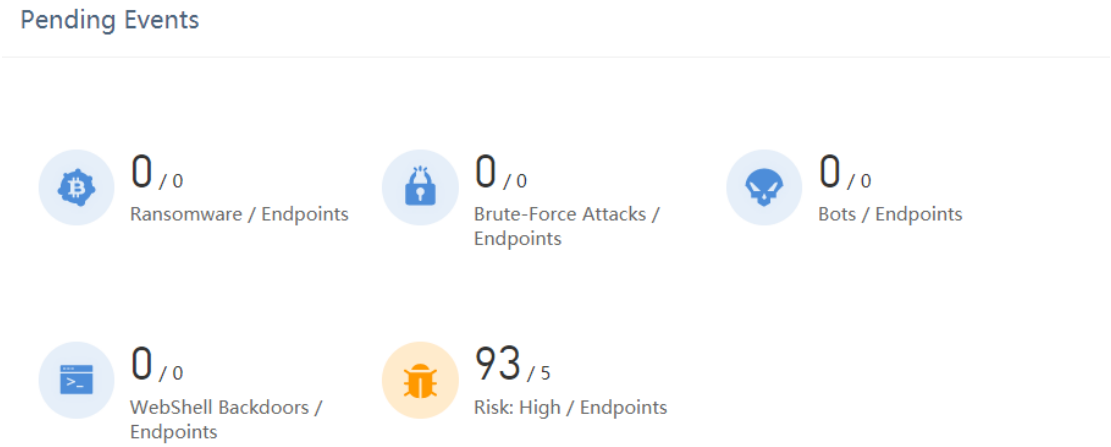
3.2 Home

You can check summary and status in **Home** page after logging in to the Endpoint Secure Manager. This page provides the administrator the following information, **Endpoints, Pending Events, Victim Endpoints, Security Events, Global Hot Events and Correlated Response**.

It also shows other information like the duration that the Endpoint Secure Manager has been running, the Software Version, Anti-virus Database version and so on.



Endpoints: This section provides the overview of the total number of connected endpoints, number of endpoints in different states (online, offline) and different endpoint types (server, PC) and detection and response in the last 7 days.

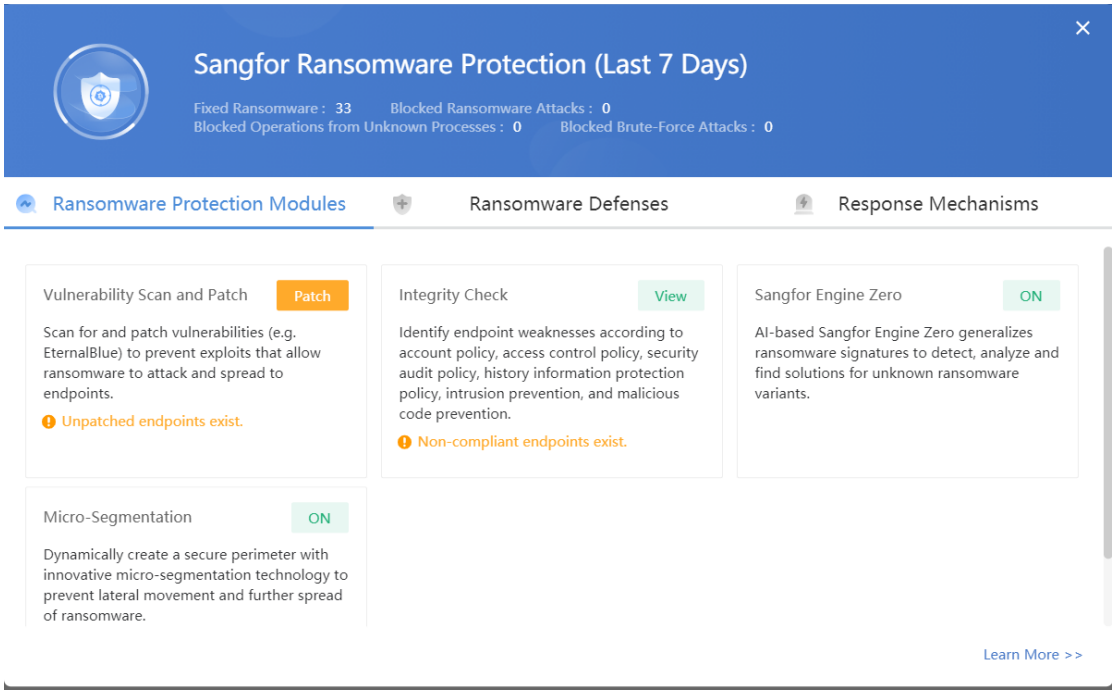


Pending Events: This section shows the number of unsolved security events such as Ransomware, Brute-force attack, WebShell backdoor and the number of victim endpoints. Click on the number to redirect to the Response and for details.

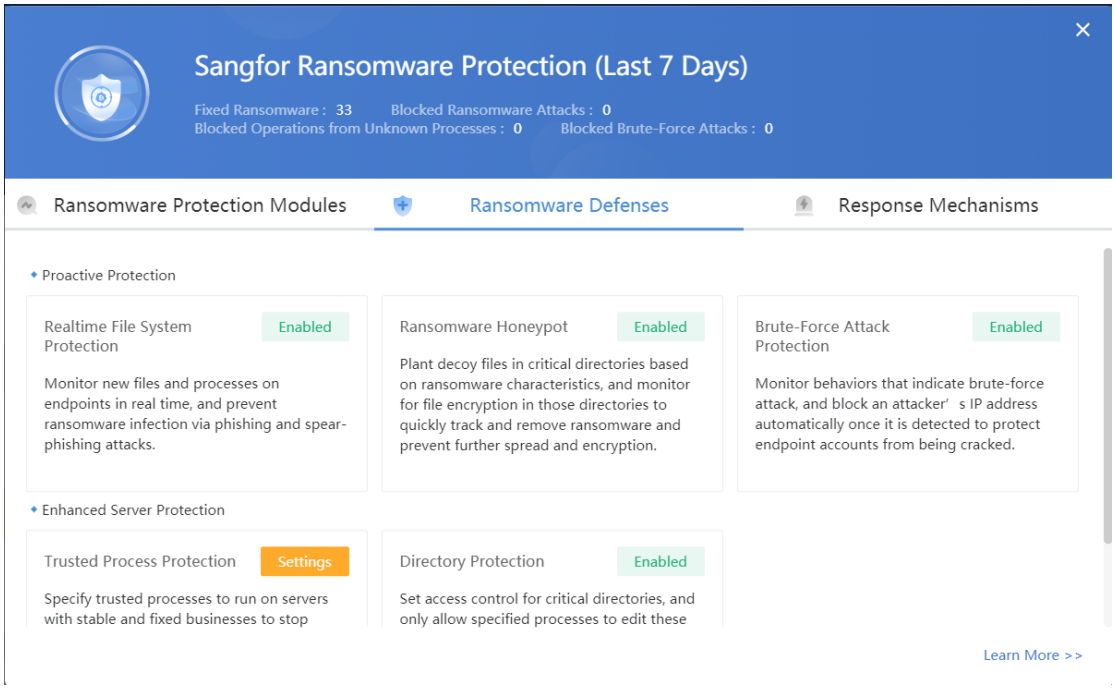
Ransomware Protection: Presentation of the introduction of the ransomware protection system and EDR, how many ransomware viruses were detected by ES agent in the last 7 days, how many suspicious ransomware activities were organized through ransomware bait, and how many untrusted processes were intercepted through server hardening (unknown Process) operation, and at the same time through the brute force prevention function to help customers block the number of brute force attacks.

The ransomware defense system introduces the protection methods and functions of ES in

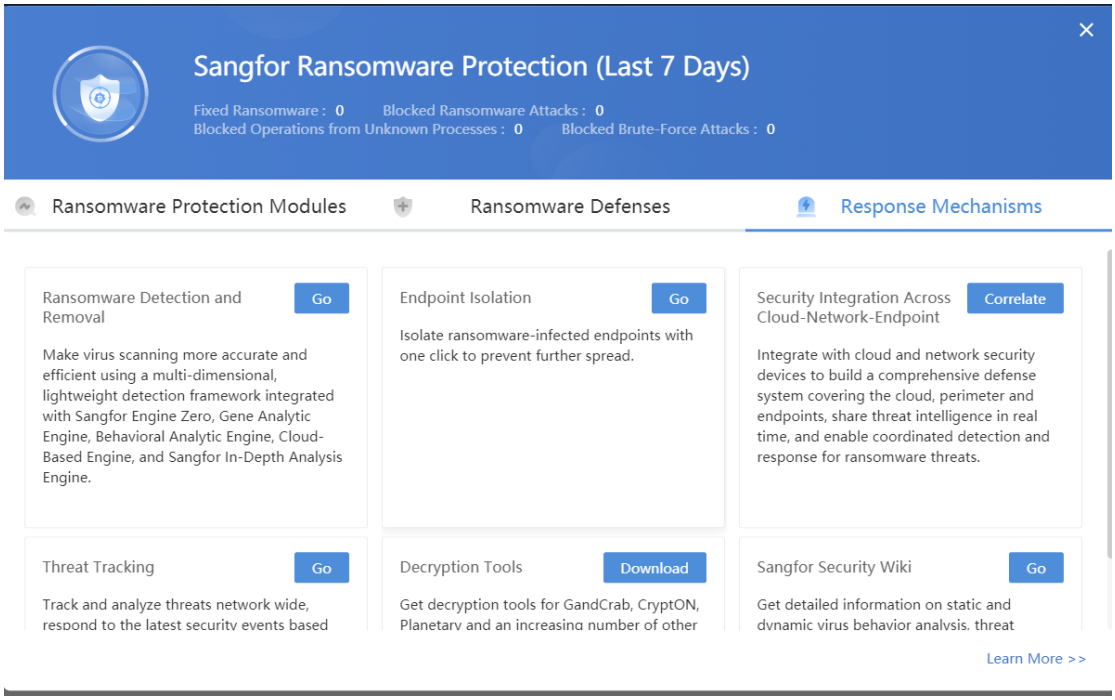
each stage of prevention, protection, detection and response, and at the same time informs the customer of the current configuration and guides the customer to enable and configure the function.



Ransomware Protection Modules: includes vulnerability detection and patch repair, security baseline inspection, Sangfor Engine Zero artificial intelligence engine protection against unknown ransomware virus, and micro segmentation. Green indicates that the function is turned on, and a yellow button indicates that the function is not turned on. Click the yellow button to jump to the policy configuration page to configure.


Sangfor Ransomware Protection (Last 7 Days)
Fixed Ransomware : 33
Blocked Ransomware Attacks : 0
Blocked Operations from Unknown Processes : 0
Blocked Brute-Force Attacks : 0
Ransomware Protection Modules
Ransomware Defenses
Response Mechanisms
Proactive Protection
Realtime File System Protection
Enabled
Monitor new files and processes on endpoints in real time, and prevent ransomware infection via phishing and spear-phishing attacks.
Ransomware Honeypot
Enabled
Plant decoy files in critical directories based on ransomware characteristics, and monitor for file encryption in those directories to quickly track and remove ransomware and prevent further spread and encryption.
Brute-Force Attack Protection
Enabled
Monitor behaviors that indicate brute-force attack, and block an attacker's IP address automatically once it is detected to protect endpoint accounts from being cracked.
Enhanced Server Protection
Trusted Process Protection
Settings
Specify trusted processes to run on servers with stable and fixed businesses to stop
Directory Protection
Enabled
Set access control for critical directories, and only allow specified processes to edit these
Learn More >>

Ransomware Defenses: includes real-time file system protection to prevent ransomware from landing and running, ransomware honeypot to prevent further encryption of ransomware, Bruce force attack protection, trusted process protection, and directory protection. Green indicates that the function is turned on, and a yellow button indicates that the function is not turned on. Click the yellow button to jump to the policy configuration page to configure.

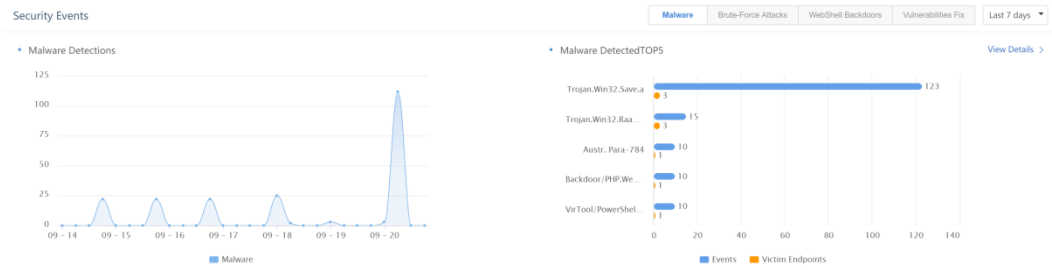


Response Mechanism: including ransomware detection and removal, endpoint isolation, security integration across cloud-network-endpoint, threat tracking, and known decryption tools for ransomware. Encyclopedia of ransomware threat analysis.

Victim Endpoint Distribution: This section shows the total number of local endpoints and the number of compromised, critical, suspicious and secure endpoints separately. Click to

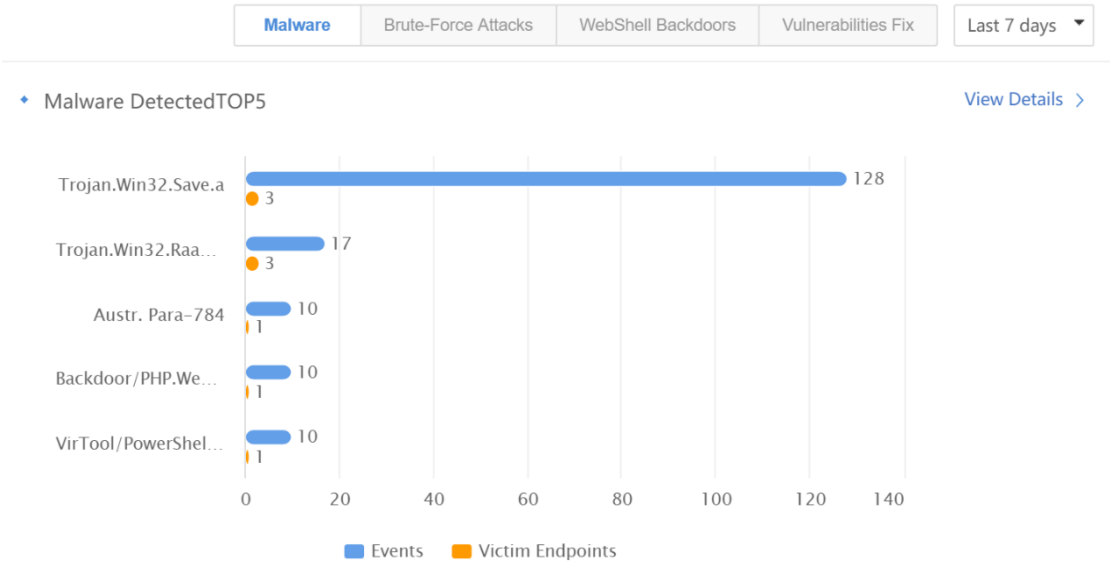
redirect to **Threat Response** in **Response** for details.

Top 5 Victim Endpoints: This section lists the top 5 endpoints ranked by discovered and pending threats. Click View **Details** to redirect to **Threat Response in Response**.

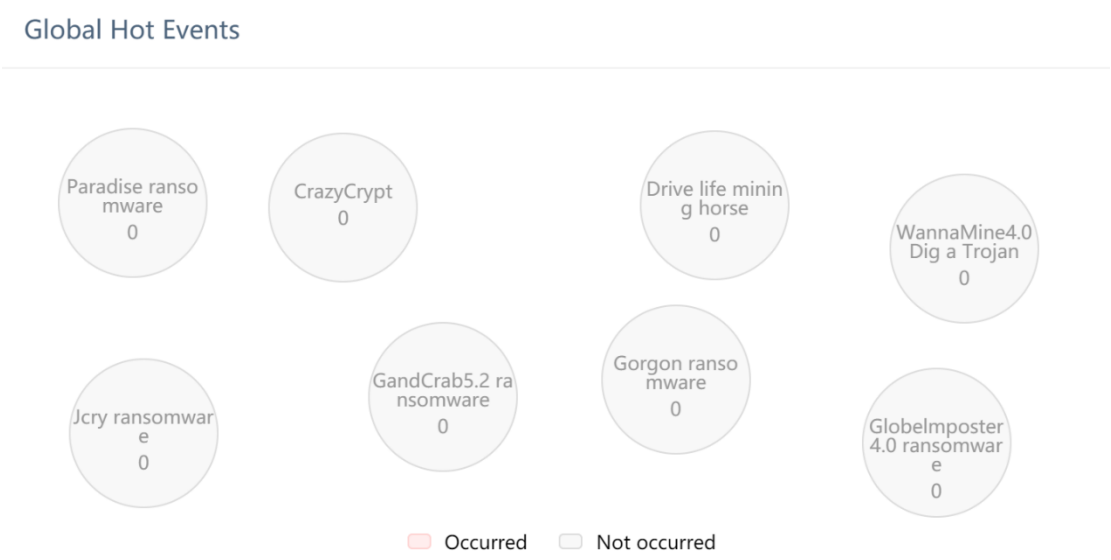


Malware Detections: This section displays statistics on the number of malware detected in the last 7 days, 30 days and 90 days, including ransomware, Trojan and malware.

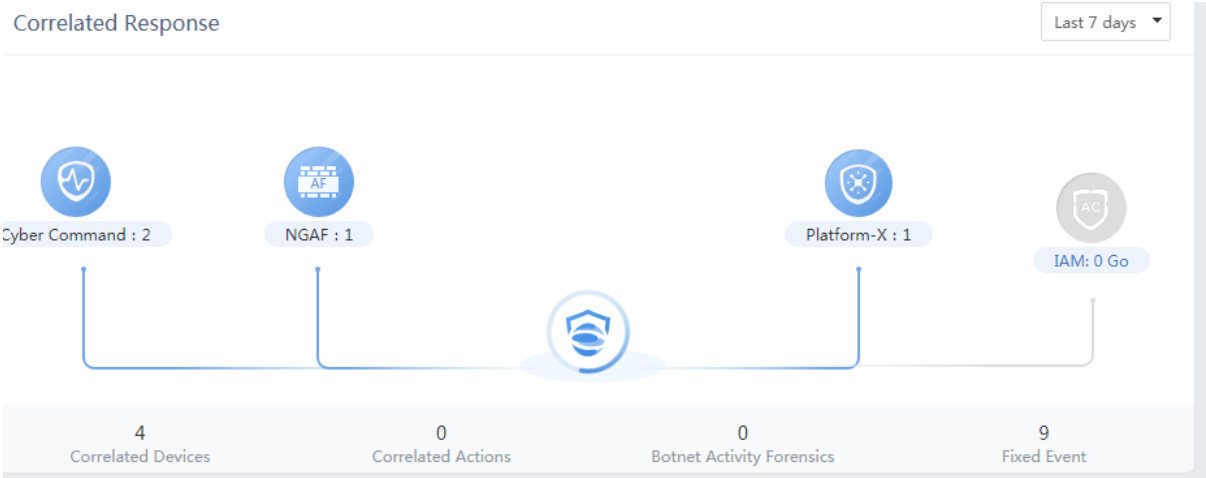
Top 5 Malware Detected This section lists the five most common viruses detected on the endpoints. Click on **View Details** to view details.



You can choose to view "Brute-force attack" and "WebShell backdoor" in the last 7, 30 or 90 days.



Global Hot Events: This section shows the hottest and most threatening security events globally and occurrence on endpoints across the network.

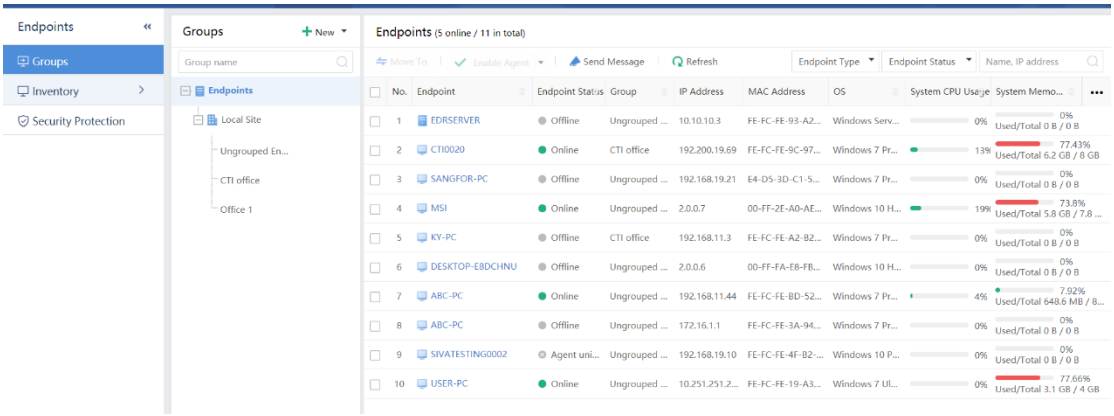


Correlated Response: Endpoint Secure can be correlated to Security Intelligence Platform (Cyber Command), Next Generation Application Firewall (NGAF), Internet Access Management (IAM), and Platform-X. This section shows the correlation status between the Endpoint Secure and these products and distributed policies.

3.3 Endpoints

3.3.1 Managing Endpoint Groups

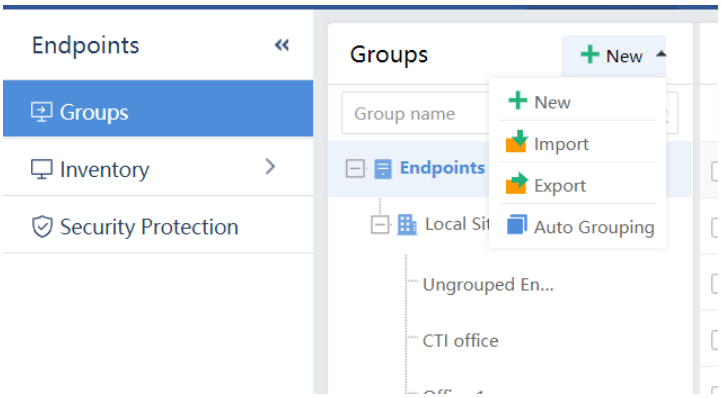
Endpoint group is used to group and manage endpoints and facilitates configuring security policies for endpoints.



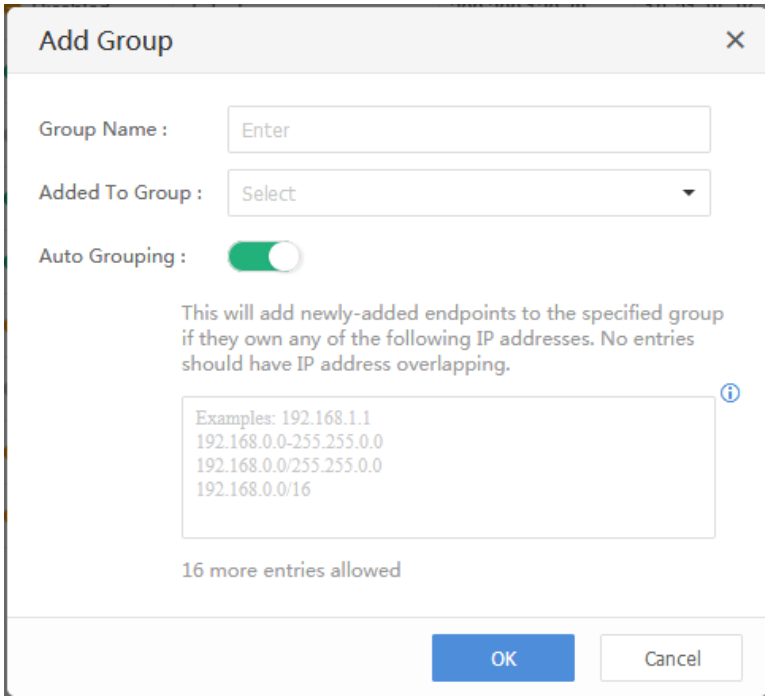
Groups is used to manage the connected endpoints by grouping. It displays some basic information of the endpoints, including endpoint status, group, IP address, MAC address, operating system, CPU usage, disk usage, owner, asset number and asset location. You can click the ellipsis (...) in the upper right of the above image to check the item you want to display.

When the Agent is installed on endpoint and can communicate with the Endpoint Secure Manager, the endpoint will automatically go online and appear in the All Endpoints list in **Endpoints** > **Groups.**

Click **New** button, a drop-down menu pops up as shown blown:



Click **New** to add a new endpoint group.

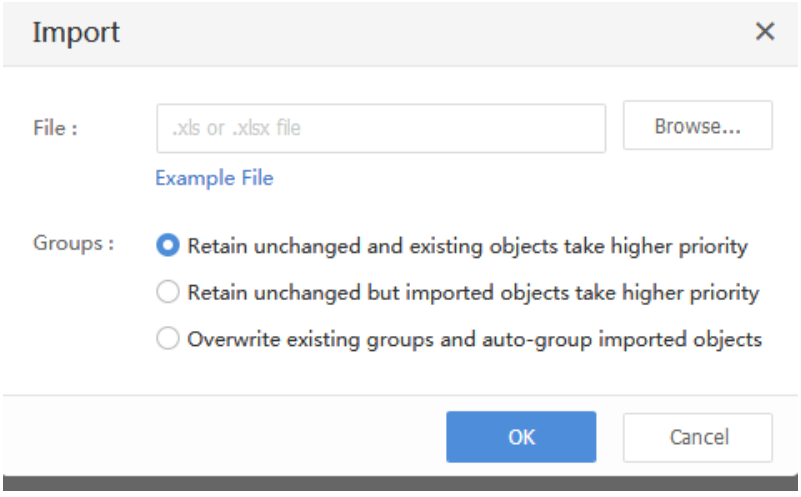


Group Name: Specifies the name of the group.

Auto Grouping: Click the icon to enable this function and then configure the IP range. When the IP address of an online endpoint belongs to the specified IP range, the endpoint will be automatically assigned to the specified group.

After the configuration is done, click **OK** to submit.

Click **Import** to import Excel file with the information of endpoints onto Endpoint Secure Manager.



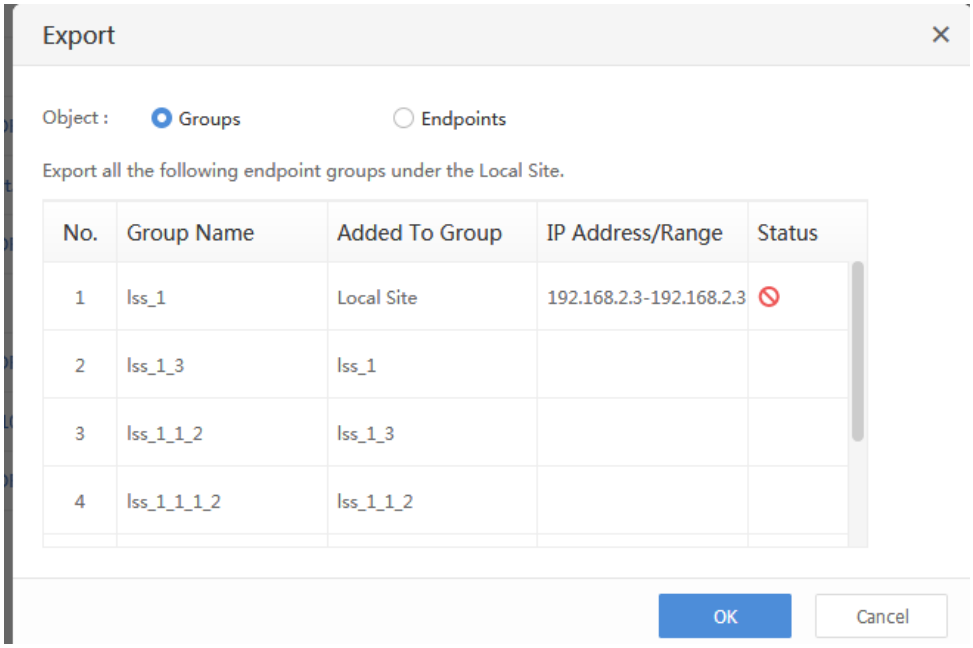
It is recommended to download sample file, as shown below:

A	B	C	D
Group Name	Upper-level Group	Auto-grouping IP Range	Status
Example 1	Local Site	192.168.0.1-192.168.0.255;192.168.1.1-192.168.1.255	Disabled
Example 2	Example 1	192.168.2.1;192.168.3.1/16;192.168.4.1/255.255.255.0	Enabled
Example 3	Example 2		

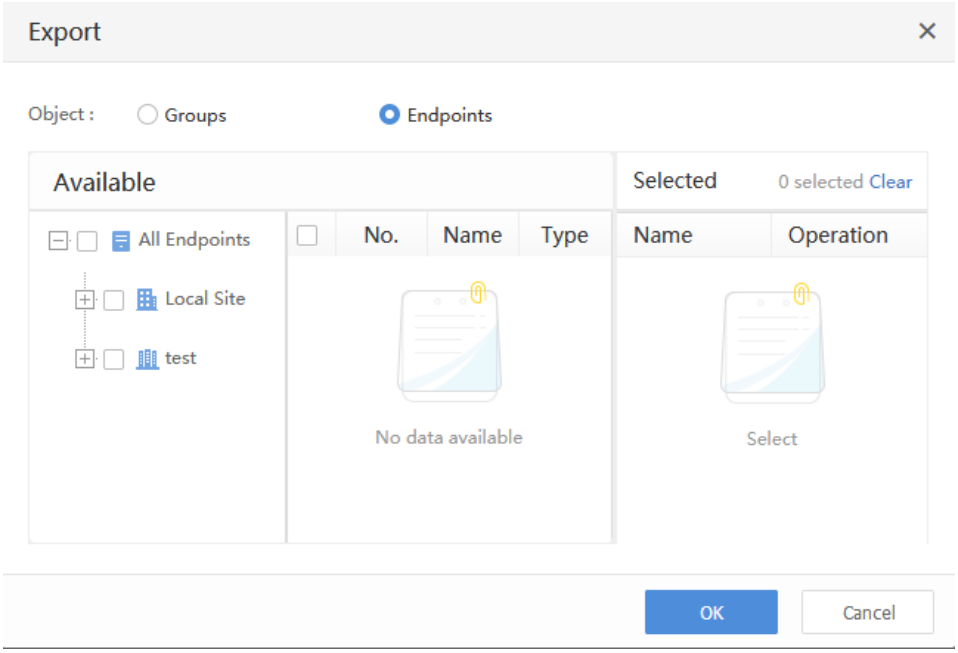
Fill in the information of endpoints according to the downloaded example file and save it, then click Import and upload it to Endpoint Secure server, then click **OK** to submit.

Click **Export** to export all the current endpoints listed on the Endpoint Secure server to an Excel file.

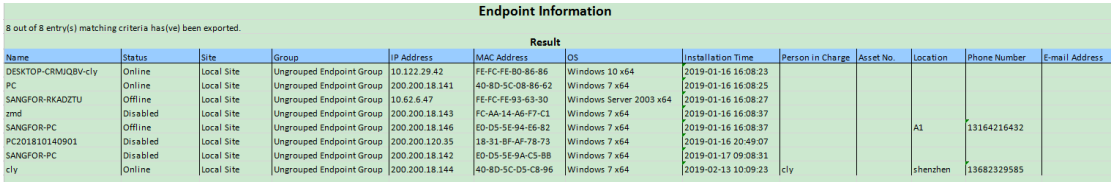
You can choose to export groups or endpoints. To export groups, choose **Groups** as **Object**, as shown below.



To export endpoints, choose Endpoints as **Object**, as shown in the figure below. Then choose the group to export the endpoints in it.



The exported Excel information is shown as below:



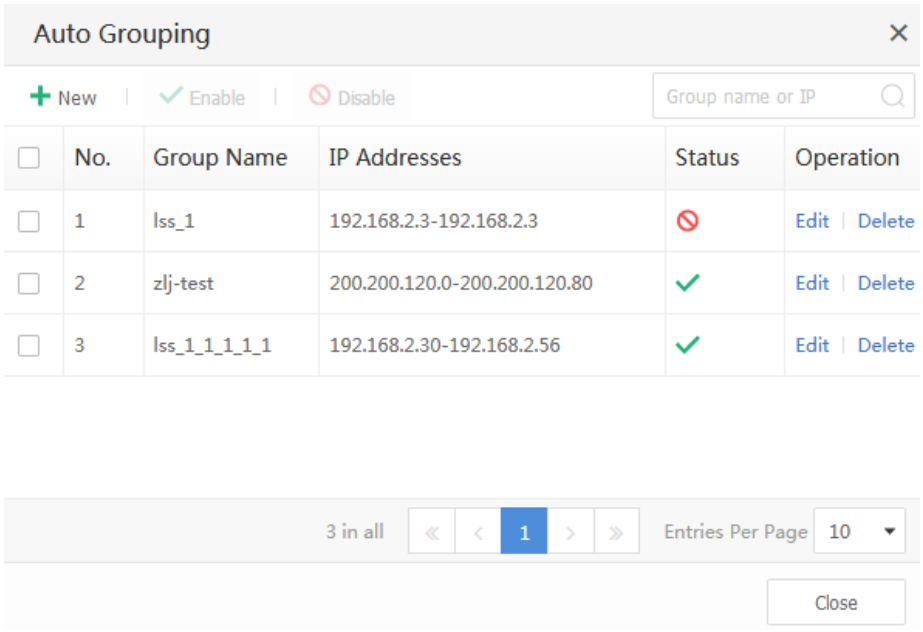
Endpoint Information

8 out of 8 entry(s) matching criteria has(ve) been exported.

Result

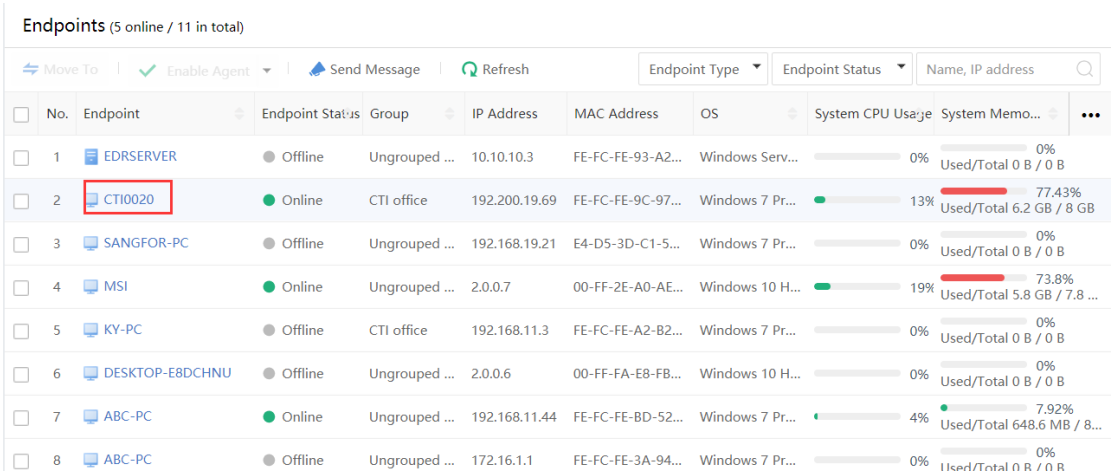
Name	Status	Site	Group	IP Address	MAC Address	OS	Installation Time	Person in Charge	Asset No.	Location	Phone Number	E-mail Address
DESKTOP-CRMJQBV-cly	Online	Local Site	Ungrouped Endpoint Group	10.122.29.42	FE-FC-FE-B0-86-86	Windows 10 x64	2019-01-16 16:08:23					
PC	Online	Local Site	Ungrouped Endpoint Group	200.200.18.141	40-8D-5C-08-86-62	Windows 7 x64	2019-01-16 16:08:25					
SANGFOR-RKADZTU	Offline	Local Site	Ungrouped Endpoint Group	10.62.6.47	FE-FC-FE-93-63-30	Windows Server 2003 x64	2019-01-16 16:08:27					
zmd	Disabled	Local Site	Ungrouped Endpoint Group	200.200.18.143	FC-AA-14-A6-F7-C1	Windows 7 x64	2019-01-16 16:08:37					
SANGFOR-PC	Offline	Local Site	Ungrouped Endpoint Group	200.200.18.146	E0-D5-5E-94-E6-82	Windows 7 x64	2019-01-16 16:08:37			A1	13164216432	
PC201810140901	Disabled	Local Site	Ungrouped Endpoint Group	200.200.120.35	18-31-BF-AF-78-73	Windows 7 x64	2019-01-16 20:49:07					
SANGFOR-PC	Disabled	Local Site	Ungrouped Endpoint Group	200.200.18.142	E0-D5-5E-9A-C5-B8	Windows 7 x64	2019-01-17 09:08:31					
cly	Online	Local Site	Ungrouped Endpoint Group	200.200.18.144	40-8D-5C-D5-C8-96	Windows 7 x64	2019-02-13 10:09:23	cly		shenzhen	13682329585	

To use auto grouping, click **New** > **Auto Grouping**, the following page pops up:

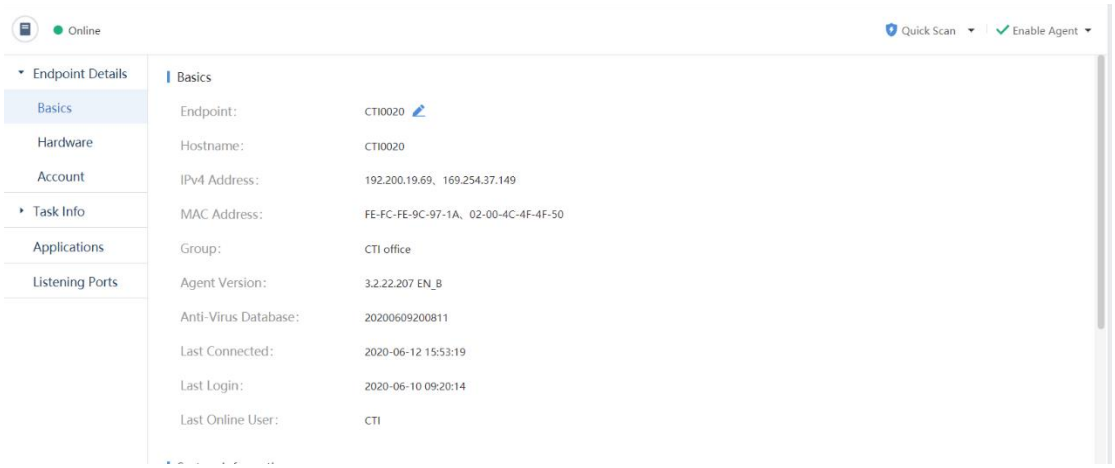


Auto grouping enables newly added endpoints that own any of the specified IP addresses to the specified group. Specified IP ranges should not overlap with each other. You can add a new group, or enable, disable, edit or delete an existing group.

The endpoints with corresponding IP addresses are automatically identified and added to the corresponding group.



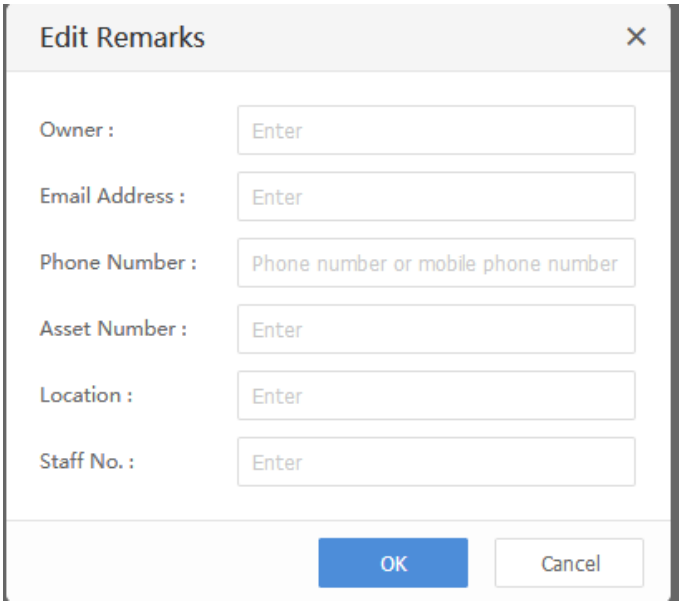
Click on endpoint name to view the details of the endpoint, as shown in the figure above.



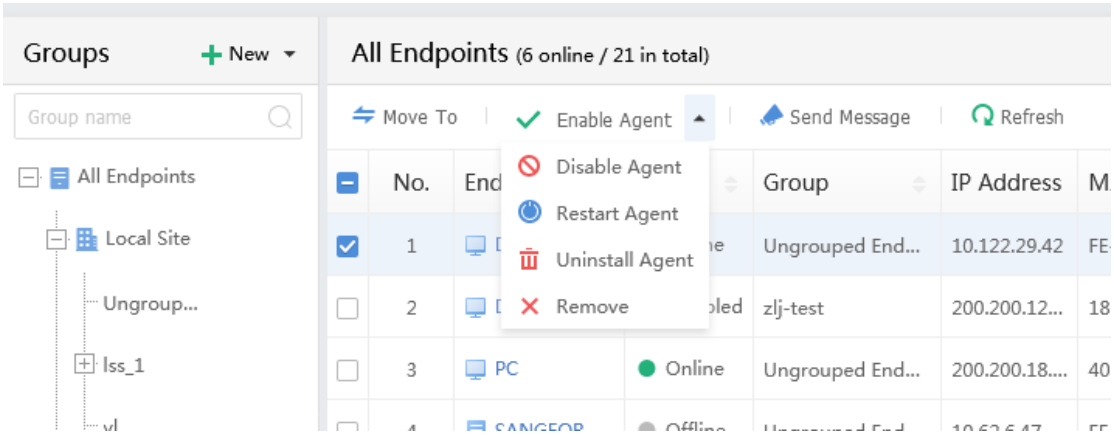
Basic: It displays basic information of endpoint, such as endpoint name, hostname, status, IP address, MAC address and operating system, which are reported by the Agent installed on the endpoint.

Others: It displays version of Agent and anti-virus database (used to check whether they are the same as the current version of Endpoint Secure Manager and anti-virus database) and last login time and last online user.

Remarks: To edit asset owner information, click on the icon to enter the following page:



You can enable, disable, uninstall and remove the Agent on endpoints through the Sangfor Endpoint Secure Manager, as shown below:



Enable Agent: By clicking this, you can enable Agent again to re-protect endpoints if it is disabled.

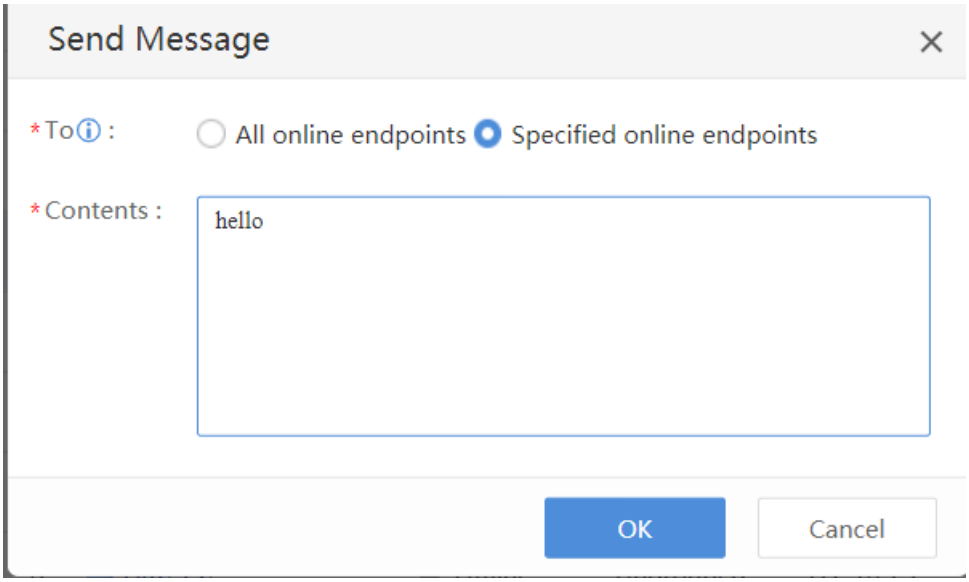
Disable Agent: By clicking this, you can disable Agent for troubleshooting when endpoint encounters error.

Uninstall Agent: When the endpoint does not need Endpoint Secure to provide security protection, you can uninstall the Agent from it. The used licenses will not be released after the uninstallation operation.

Remove: Click **Remove** to remove the endpoint that has Agent uninstalled from the All Endpoints list on Sangfor Endpoint Secure Manager and the used licenses will be released.

By clicking **Send Message**, you can send message to Windows client computers (Windows

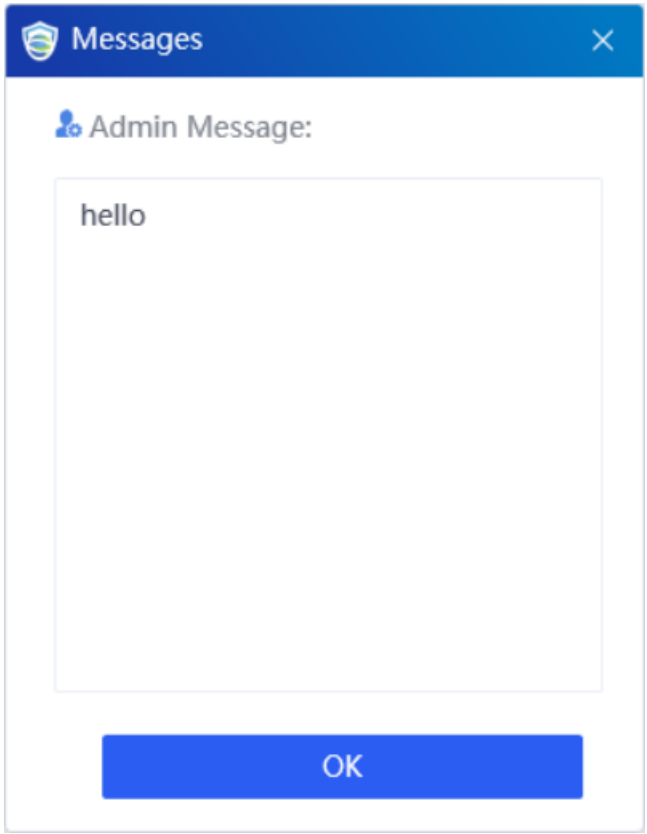
XP, 7, 8.1, 10) through Sangfor Endpoint Secure Manager.



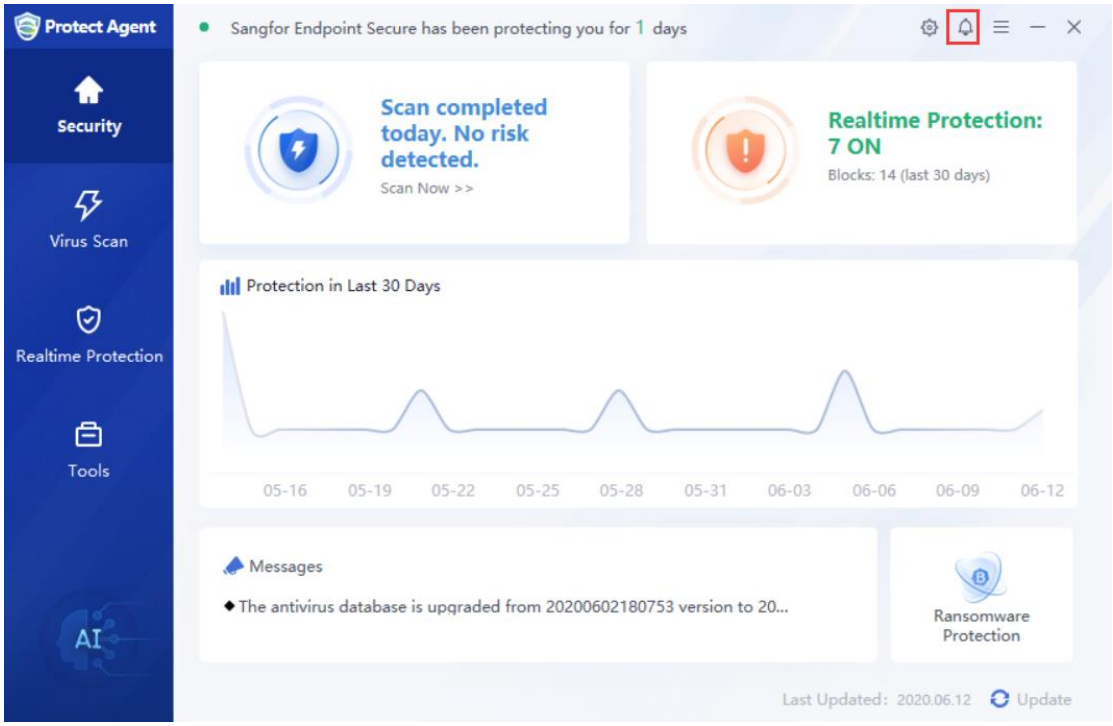
To: Select the endpoints that you want to send message to. You can select all online hosts or specified online hosts.

Contents: Specify message contents.

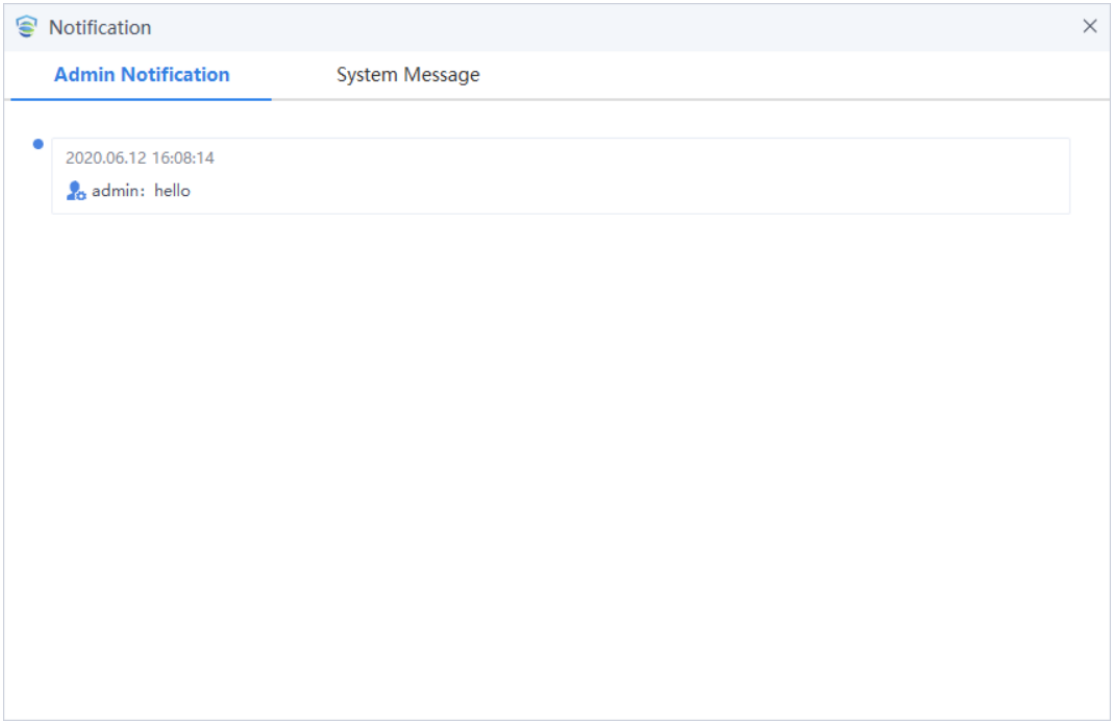
Click **OK** to save and send the message. The message received by the endpoint is as shown below:



On the endpoint, click OK or click on the icon in the upper right corner of the window to close the message. After you close the message, a small red dot will appear, as shown below:

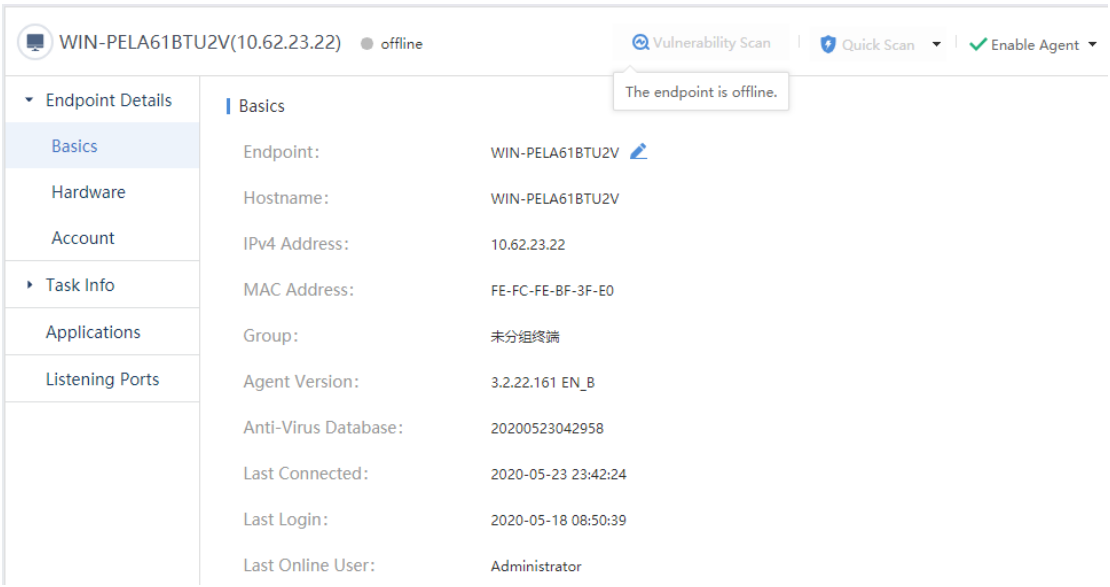


Click **Admin Notification** to view all the messages.



1. All the online endpoints need to be added to the custom group, and shall not be added to Ungrouped Endpoint, otherwise the micro-segmentation policy cannot be applied.

Click the endpoint name to view detailed information of the endpoint. Endpoint details include "Endpoint Details", "Task Info", "Applications" and "Listening Ports".



The right side of the Endpoint name on the details page is the common operations on the current terminal. The details of the common operations are as follows:

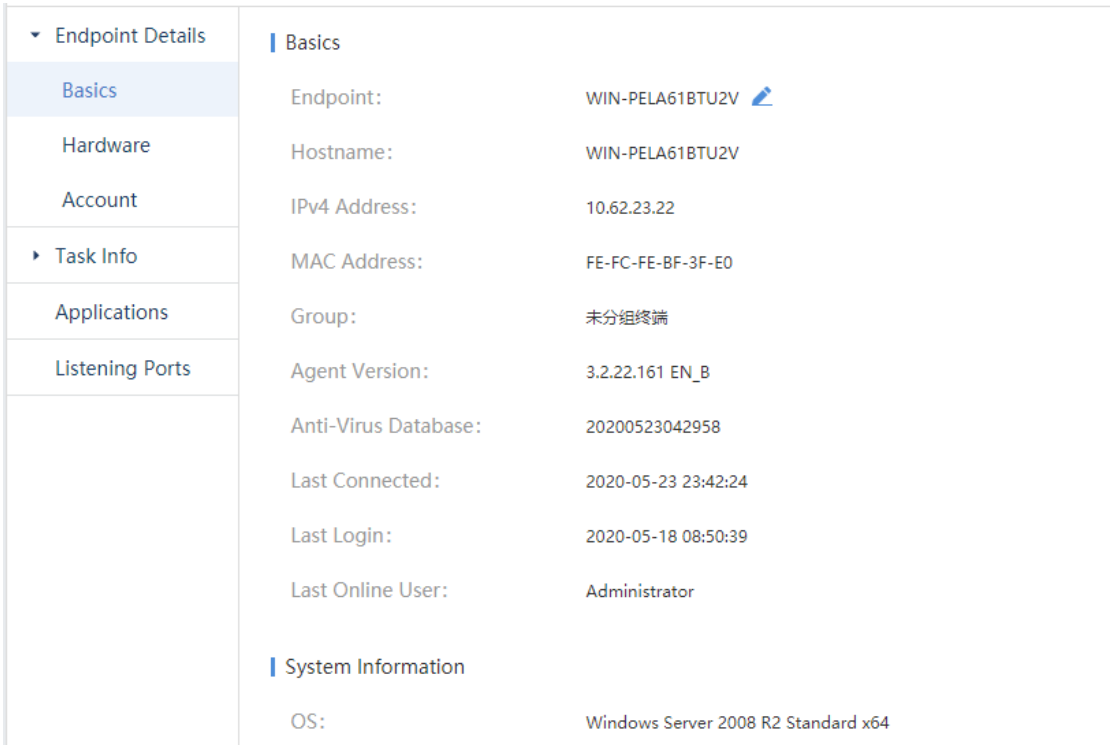
[Vulnerability Scan]: A quick entry for vulnerability scanning. You can click this to perform system vulnerability detection on the current endpoint.

[Quick Scan], [Full Scan]: A quick entry of virus scan. You can choose to perform quick virus scan or full virus scan on the current Endpoint.

[Enable Agent], [Disable Agent], [Restart Agent], Uninstall Agent], [Delete] When the installed Agent is found abnormal, you can disable, or uninstall it from the manager. When you need to reduce the number of the licensed Agent number, uninstall Agent first, and remove the endpoint with Agent uninstalled from the manager.

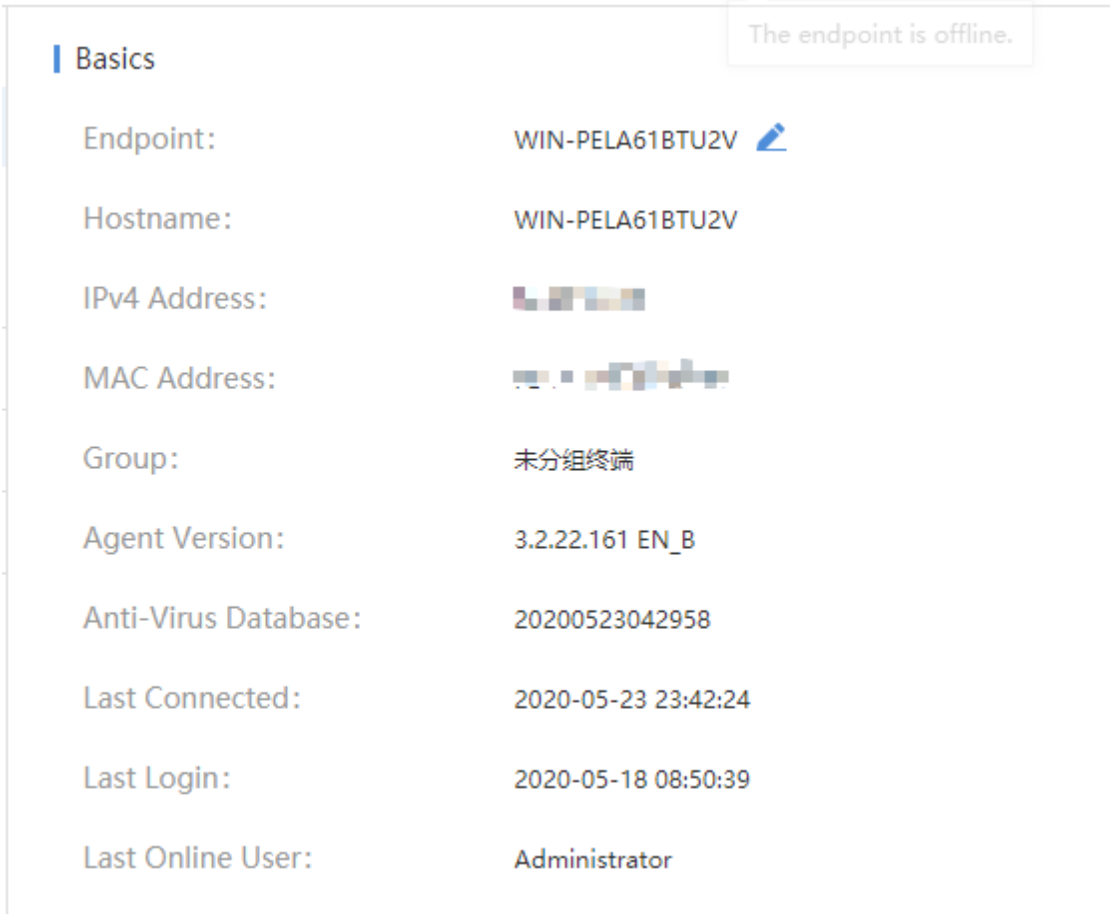
[Send Message] You can send message to the endpoint from the Endpoint Secure Manager platform and then that endpoint receives the notification.

[Endpoint Details] include **[Basics], [Hardware]** and **[Account]**， as shown in the figure below:

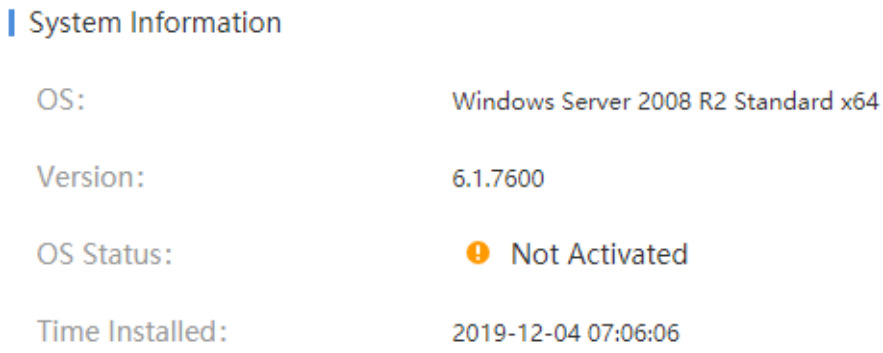


[Basics] includes **[Basics], [System Information], and [Others]** of the endpoint.

Among them, **[Basics]** includes the endpoint name, hostname, IP address and other information, as shown below:

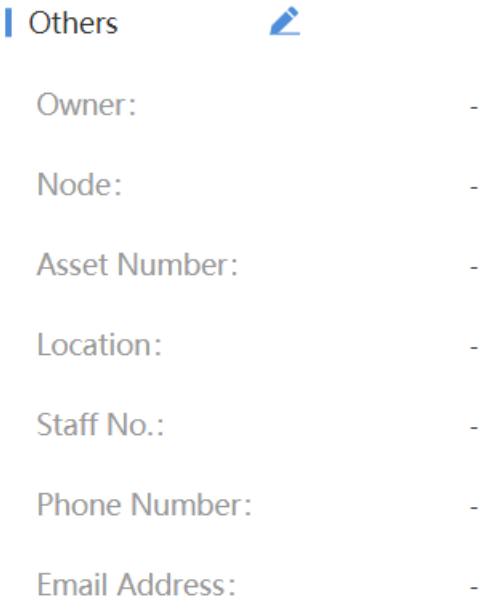


[System Information] includes the endpoint's operating system, operating system version number, operating system activation status and operating system installation time, as shown below.

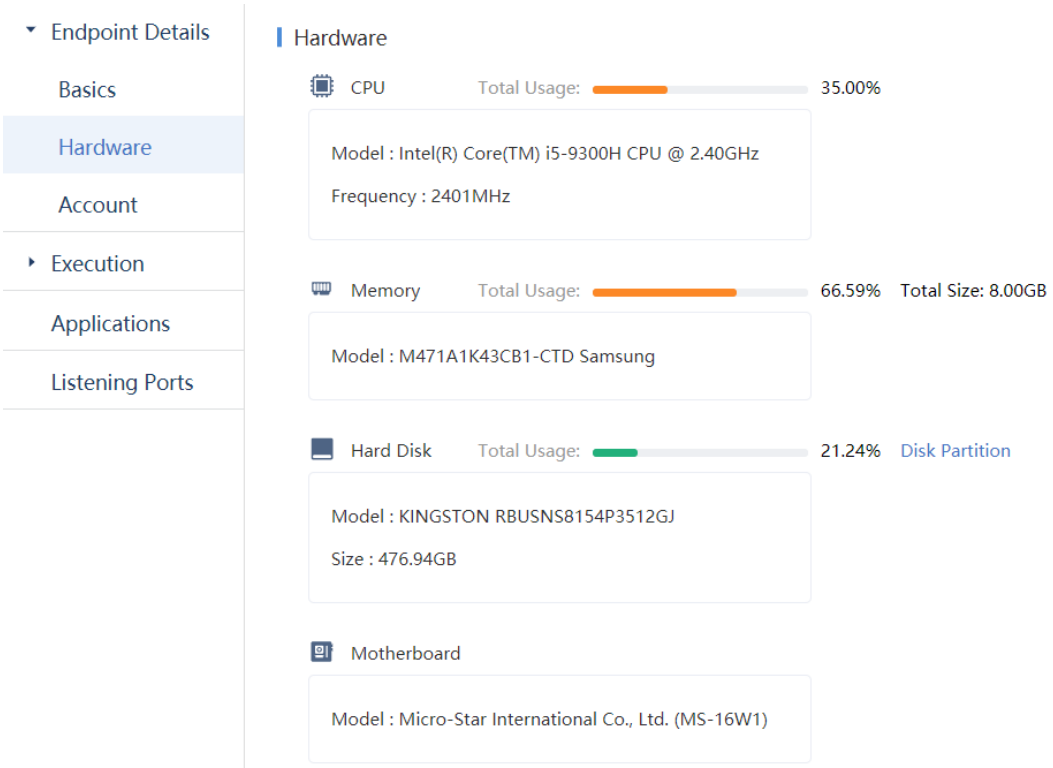


[Others] includes the asset owner, asset number, asset location and other information, as

shown below.

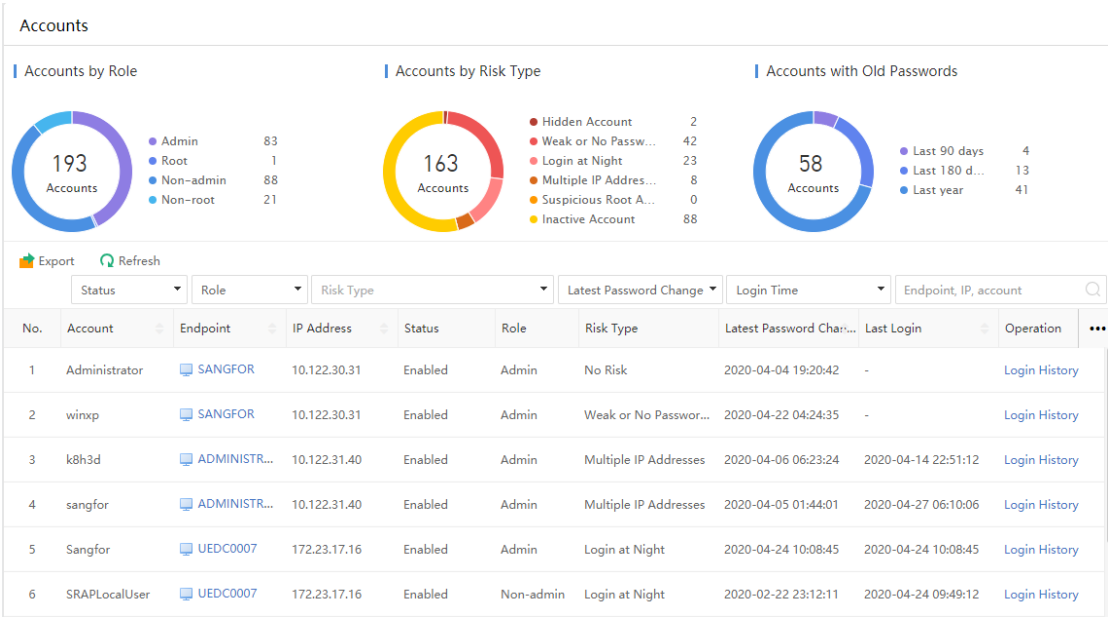


[Hardware] includes detailed hardware information of the endpoint's CPU, memory, hard disk, motherboard, adapter, monitor, etc., as shown below.

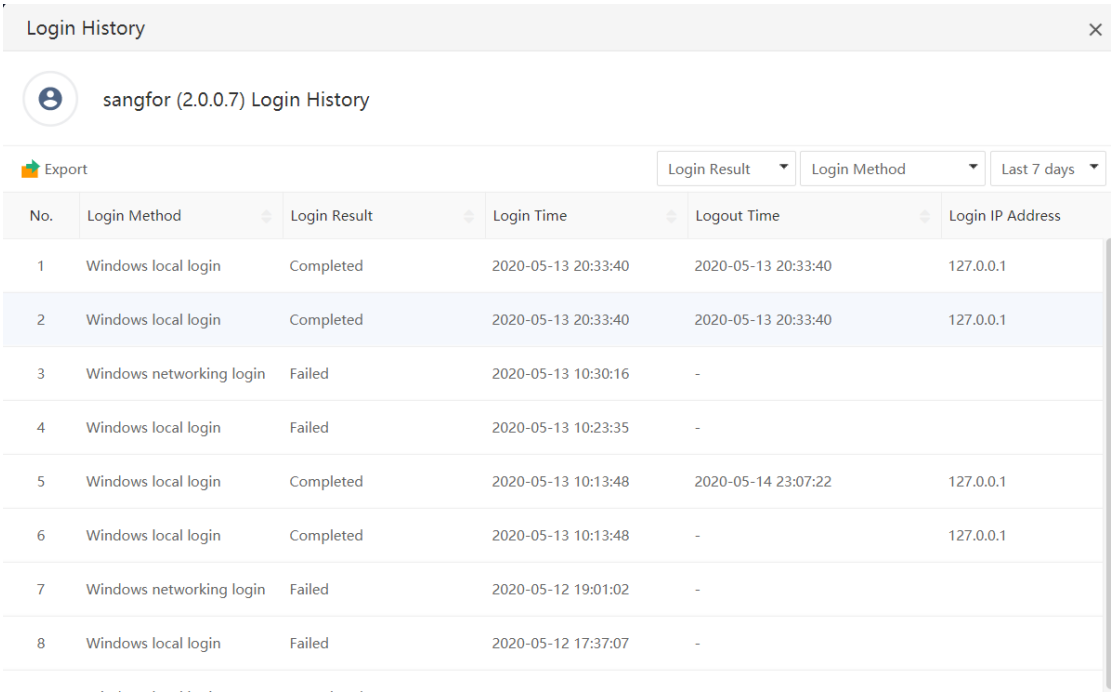


[Account] lists detailed information such as the account name, account status, and role and risk type of all system accounts of the endpoint. The administrator can determine whether

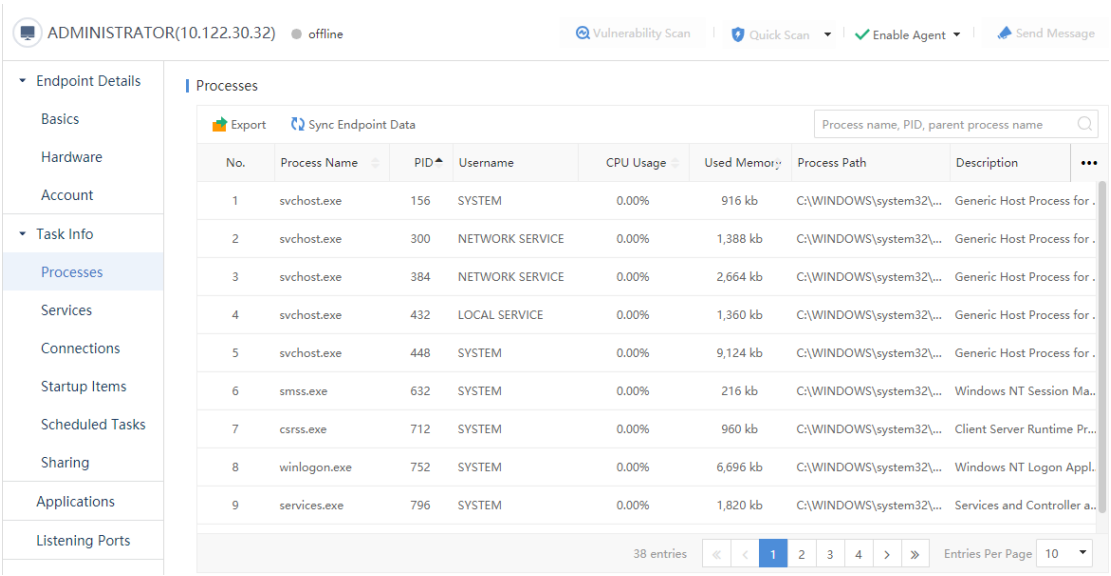
there is a risky account through the collected account information, as shown below.



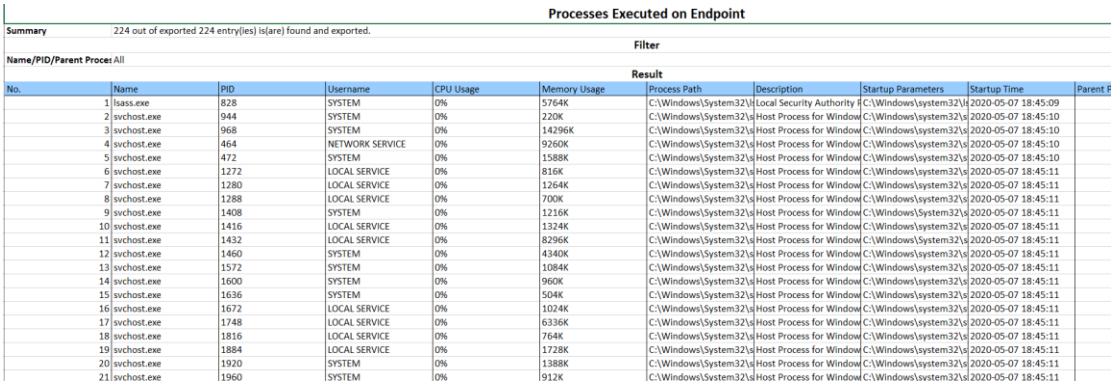
Click Login History to view the detailed login information of the system account, as shown below.



[Task Info] includes **[Processes]**, **[Services]**, **[Connections]**, **[Startup Items]**, **[Scheduled Task]** and **[Sharing]** information, as shown in the figure below:



[Processes] lists information about all running processes on the endpoint, including process name, username, CPU usage, used memory and other information. Click **Sync Endpoint Data** to trigger the manager to issue a command to collect process information. Click **Export** to export the process information of the endpoint currently as excel file for the administrator to further analyze, as shown in the following figure.



Processes Executed on Endpoint

Summary	224 out of exported 224 entry(ies) is(are) found and exported.

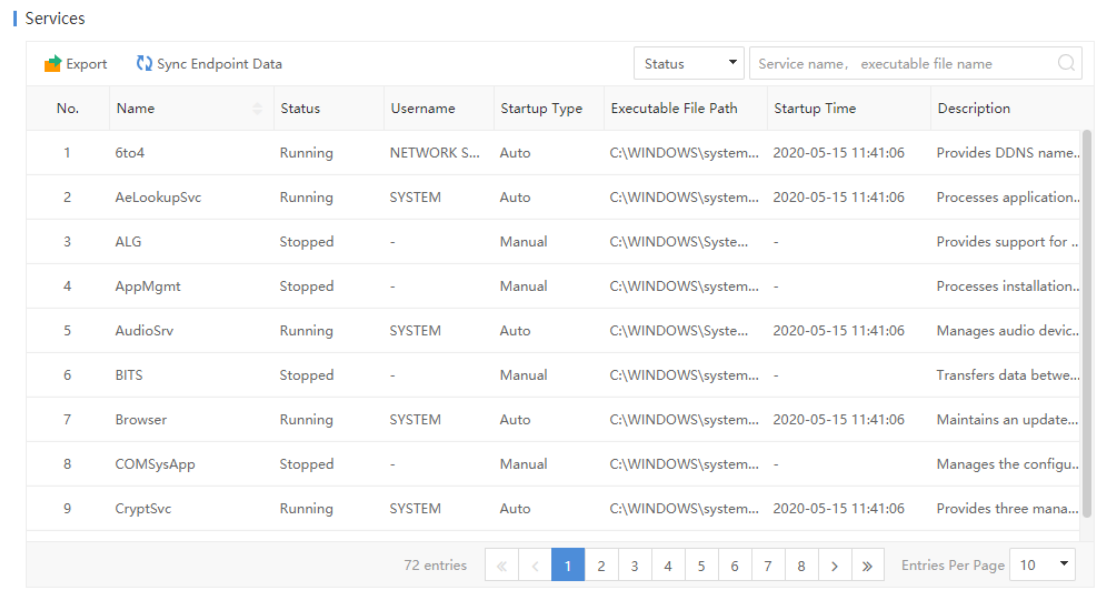
Filter

Name/PID/Parent Proce:	All

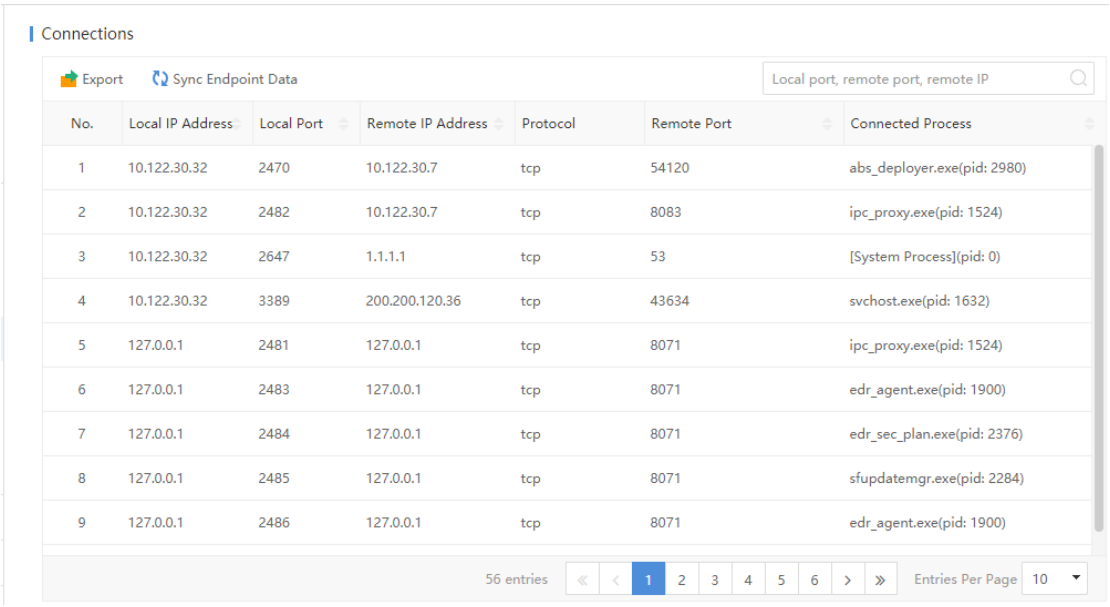
Result

No.	Name	PID	Username	CPU Usage	Memory Usage	Process Path	Description	Startup Parameters	Startup Time	Parent F
1	lsass.exe	828	SYSTEM	0%	5764K	C:\Windows\System32\l	Local Security Authority P	C:\Windows\system32\l	2020-05-07 18:45:09	
2	svchost.exe	944	SYSTEM	0%	220K	C:\Windows\System32\s	Host Process for Window	C:\Windows\system32\s	2020-05-07 18:45:10	
3	svchost.exe	968	SYSTEM	0%	14296K	C:\Windows\System32\s	Host Process for Window	C:\Windows\system32\s	2020-05-07 18:45:10	
4	svchost.exe	464	NETWORK SERVICE	0%	9260K	C:\Windows\System32\s	Host Process for Window	C:\Windows\system32\s	2020-05-07 18:45:10	
5	svchost.exe	472	SYSTEM	0%	1588K	C:\Windows\System32\s	Host Process for Window	C:\Windows\system32\s	2020-05-07 18:45:10	
6	svchost.exe	1272	LOCAL SERVICE	0%	816K	C:\Windows\System32\s	Host Process for Window	C:\Windows\system32\s	2020-05-07 18:45:11	
7	svchost.exe	1280	LOCAL SERVICE	0%	1264K	C:\Windows\System32\s	Host Process for Window	C:\Windows\system32\s	2020-05-07 18:45:11	
8	svchost.exe	1288	LOCAL SERVICE	0%	700K	C:\Windows\System32\s	Host Process for Window	C:\Windows\system32\s	2020-05-07 18:45:11	
9	svchost.exe	1408	SYSTEM	0%	1216K	C:\Windows\System32\s	Host Process for Window	C:\Windows\system32\s	2020-05-07 18:45:11	
10	svchost.exe	1416	LOCAL SERVICE	0%	1324K	C:\Windows\System32\s	Host Process for Window	C:\Windows\system32\s	2020-05-07 18:45:11	
11	svchost.exe	1432	LOCAL SERVICE	0%	8296K	C:\Windows\System32\s	Host Process for Window	C:\Windows\system32\s	2020-05-07 18:45:11	
12	svchost.exe	1460	SYSTEM	0%	4340K	C:\Windows\System32\s	Host Process for Window	C:\Windows\system32\s	2020-05-07 18:45:11	
13	svchost.exe	1572	SYSTEM	0%	1084K	C:\Windows\System32\s	Host Process for Window	C:\Windows\system32\s	2020-05-07 18:45:11	
14	svchost.exe	1600	SYSTEM	0%	960K	C:\Windows\System32\s	Host Process for Window	C:\Windows\system32\s	2020-05-07 18:45:11	
15	svchost.exe	1636	SYSTEM	0%	504K	C:\Windows\System32\s	Host Process for Window	C:\Windows\system32\s	2020-05-07 18:45:11	
16	svchost.exe	1672	LOCAL SERVICE	0%	1024K	C:\Windows\System32\s	Host Process for Window	C:\Windows\system32\s	2020-05-07 18:45:11	
17	svchost.exe	1748	LOCAL SERVICE	0%	6336K	C:\Windows\System32\s	Host Process for Window	C:\Windows\system32\s	2020-05-07 18:45:11	
18	svchost.exe	1816	LOCAL SERVICE	0%	764K	C:\Windows\System32\s	Host Process for Window	C:\Windows\system32\s	2020-05-07 18:45:11	
19	svchost.exe	1884	LOCAL SERVICE	0%	1728K	C:\Windows\System32\s	Host Process for Window	C:\Windows\system32\s	2020-05-07 18:45:11	
20	svchost.exe	1920	SYSTEM	0%	1388K	C:\Windows\System32\s	Host Process for Window	C:\Windows\system32\s	2020-05-07 18:45:11	
21	svchost.exe	1960	SYSTEM	0%	912K	C:\Windows\System32\s	Host Process for Window	C:\Windows\system32\s	2020-05-07 18:45:11	

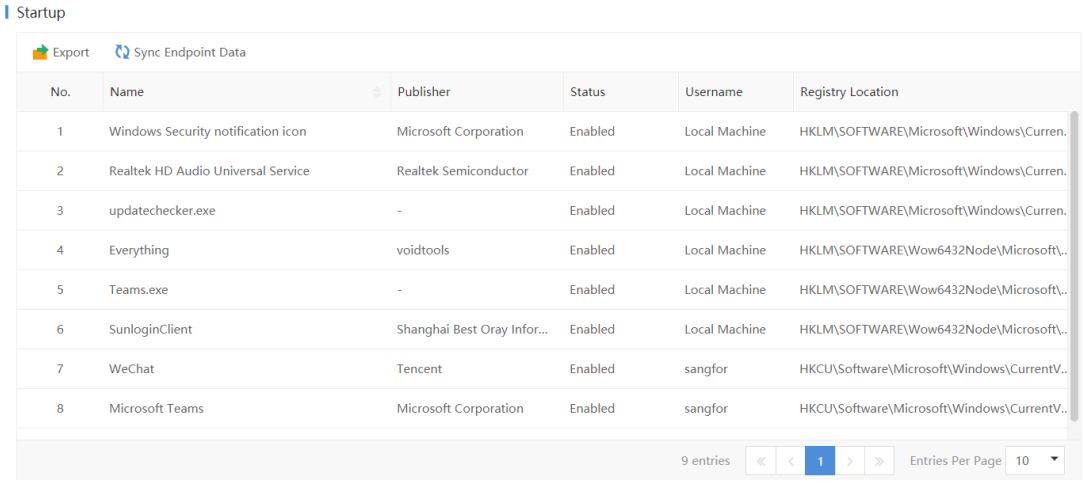
[Services] collects all the service information of the endpoint, including service name, service status, startup type and other information. Click **Sync Endpoint Data** to trigger the manager to issue a command to collect service information. Click **Export** to export the currently running service information of the endpoint as excel file to facilitate further analysis for the administrator.



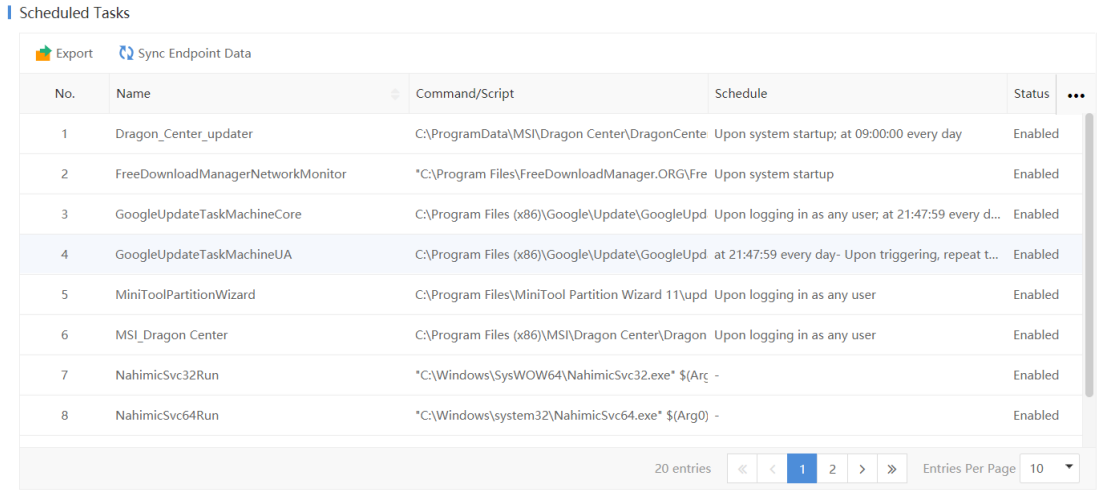
[Connections] lists the current network connection information of the endpoint, including local IP address, local port, remote IP address, remote port, protocol, and other information. Click **Sync Endpoint Data** to trigger the manager to issue a command to collect network connection information. Click **Export** to export the current network connections as excel file to facilitate further analysis for the administrator.



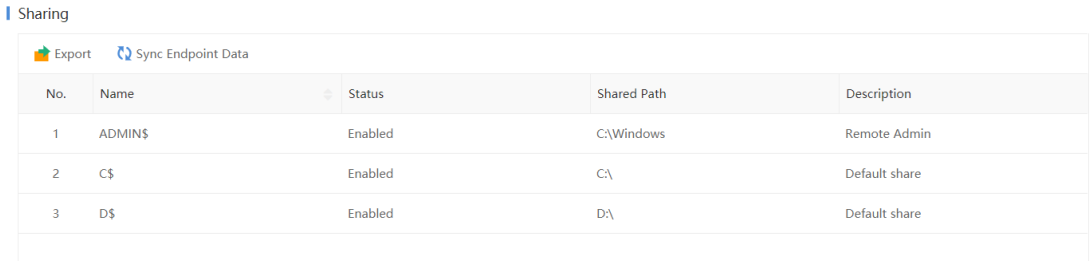
[Startup Items] displays the startup item information of the endpoint, including the startup item name, publisher, and status. Click **Sync Endpoint Data** to trigger the manager terminal to issue a command to collect start item information and click **Export** to export the current start items as excel file to facilitate further analysis for the administrator.



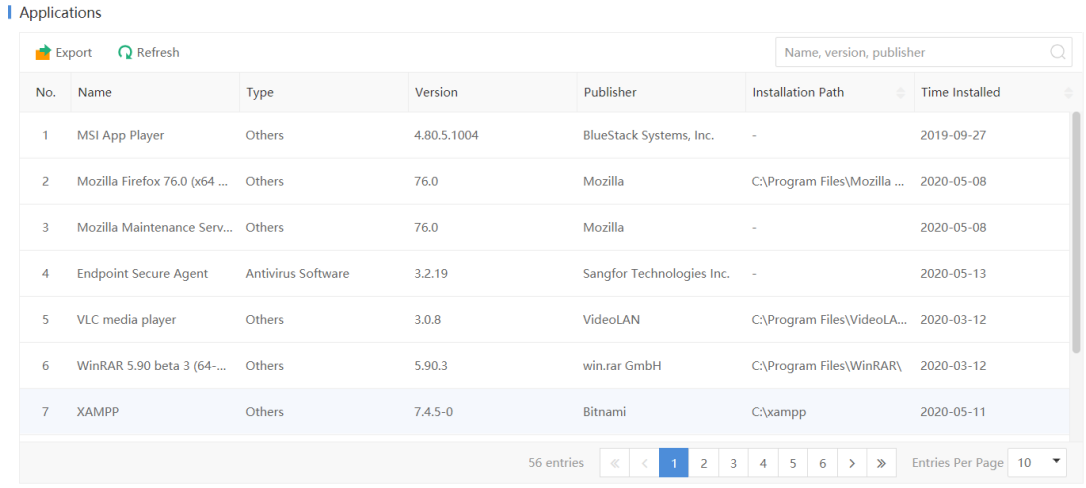
[Scheduled Tasks] shows the scheduled task information of the endpoint, including the scheduled task name, command/script, scheduled execution time and other information. Click **Sync Endpoint Data** to trigger the manager to issue a command to collect scheduled task information and click **Export** to export the current scheduled tasks as excel file to facilitate the administrator's further analysis.



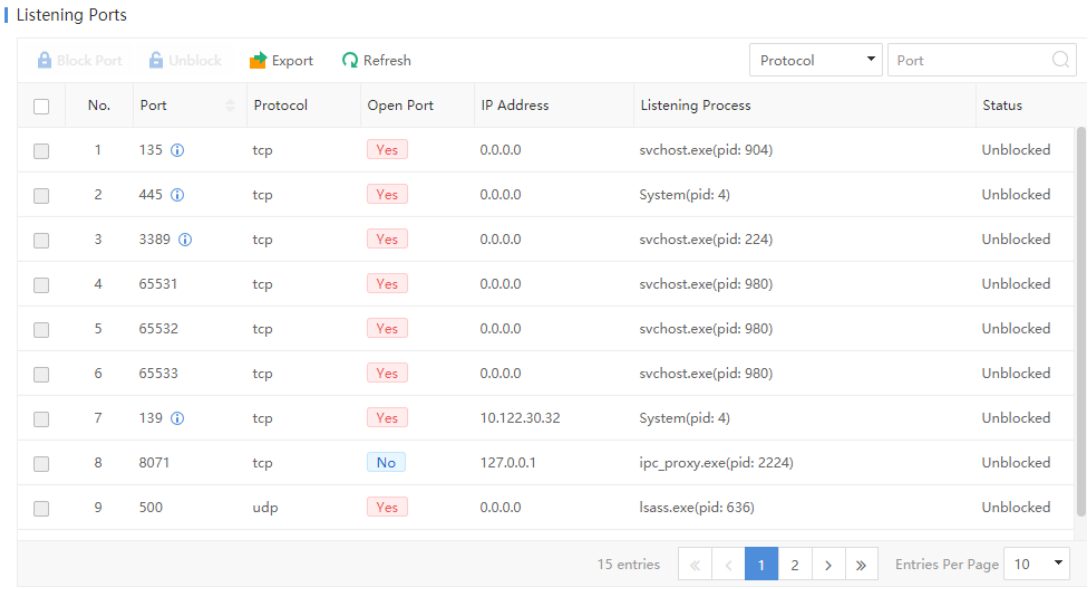
[Sharing] lists information about the shared directory or file of the endpoint, including information such as name, status, and shared path. Click **Sync Endpoint Data** to trigger the manager to issue a command to collect shared information. Click **Export** to export the terminal's current shared information as excel fie to facilitate further analysis for the administrator.



[Applications] shows information of applications installed on the endpoint, including application name, type, version, and other information. Click **Export** to export the current application information of the endpoint as excel file to facilitate the administrator's further analysis.



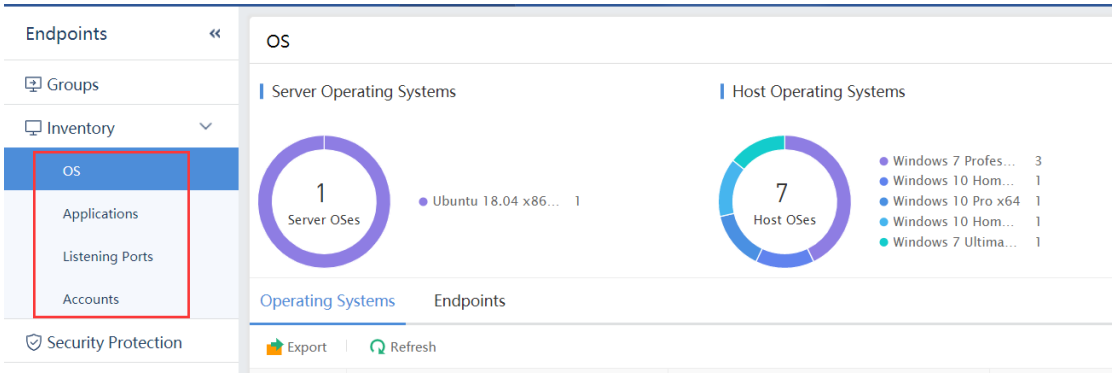
[Listening Ports] displays the information of the endpoint's listening ports, including port number, protocol, listening process and other information. Click **Export** to export the current listening port information of the endpoint as excel file to facilitate the administrator's further analysis.



When a risky port is found, select the port, and click **Block** to block it; click **Unblock** to unblock the port in blocked state.

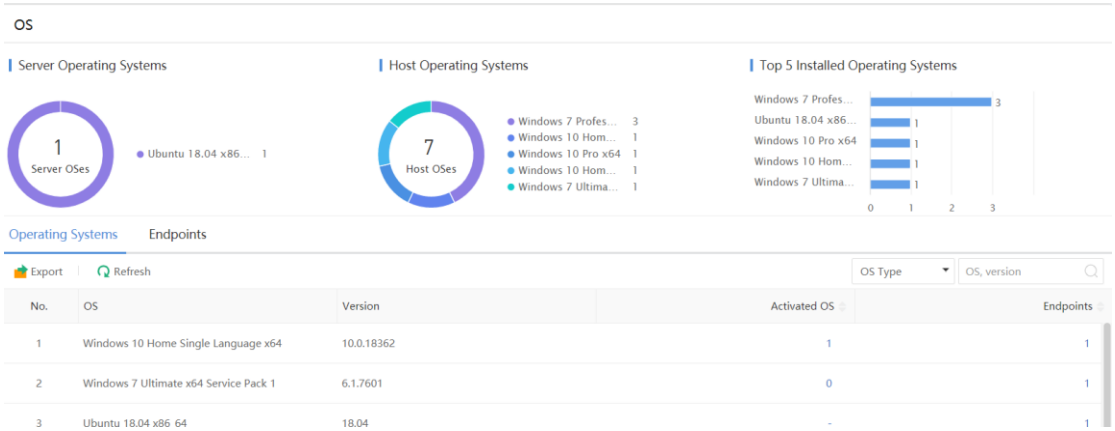
3.3.2 Inventory

Inventory refers to the inventory of the operating system, applications, listening ports, and accounts of all the managed endpoints, as shown in the figure below.



3.3.2.1 Operating System (OS)

Check the version and distribution of the operating system of all endpoints, as shown below.



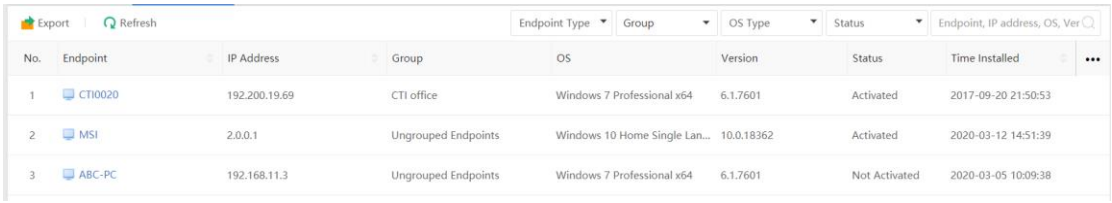
[Server Operating Systems] shows total number of server operating systems in customer network and number of each type of OS installed on servers.

[Host Operating Systems] shows total number of host operating systems in customer network and number of each type of OS installed on hosts.

[Top 5 Installed Operating Systems] shows the top 5 operating systems installed on the managed endpoints on the whole network.

[Operating Systems] From the operating system perspective, list the number of endpoints that install the operating system on the entire network and the number of endpoints that activate the system. Click on the numbers in the two columns, Activated OS, Endpoints, to display the details of the endpoints with specific OS, as shown below.

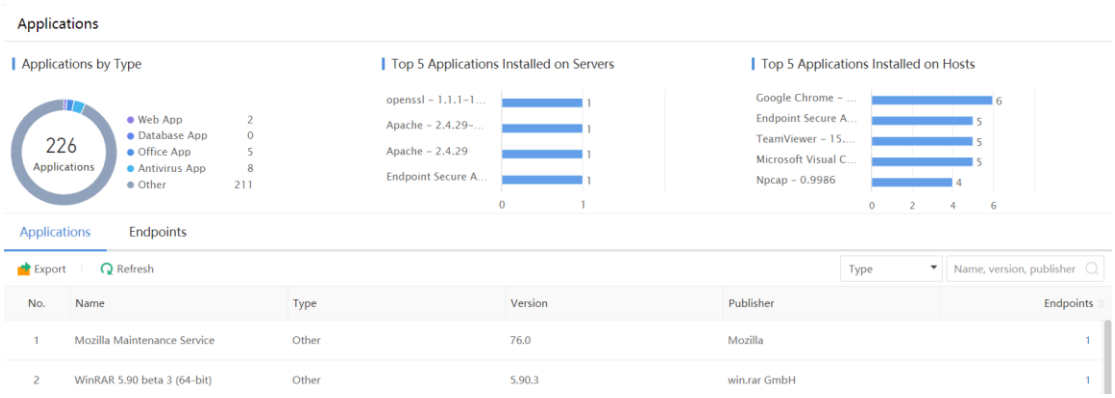
[Endpoints] From the endpoint perspective, list the operating operating system type, version number, and installation time, as shown below.



Click Export button to export as excel, which is convenient for the administrator to do further statistical analysis. In addition, you can further filter endpoints by specifying Endpoint type, Group, OS Type, and OS Status.

3.3.2.2 Applications

The Applications section displays applications installed on managed endpoints across the network, and provides Applications tab and Endpoints tab to display information from different perspectives, so as to help administrators to find risky applications quickly, and then take measures to enhance security such as updating version or application reinforcement.



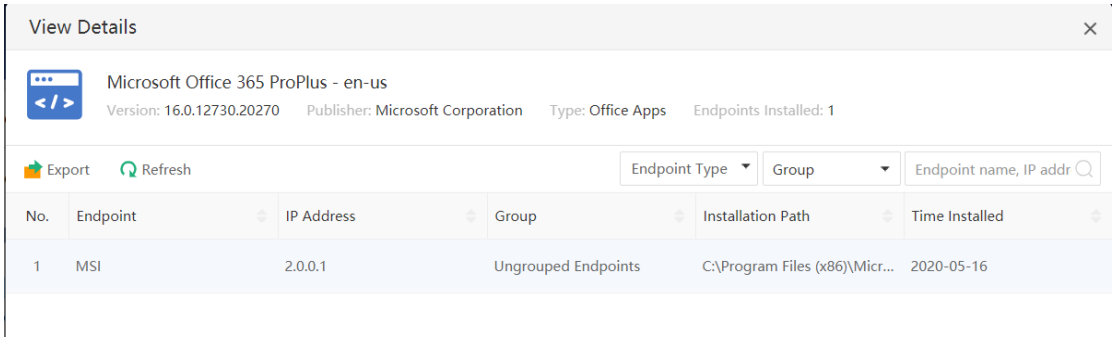
[Applications by Type] shows the total number of applications installed on endpoints across the network and number of applications of different types.

[Top 5 Applications Installed on Servers] shows the top 5 applications installed on servers across the entire network

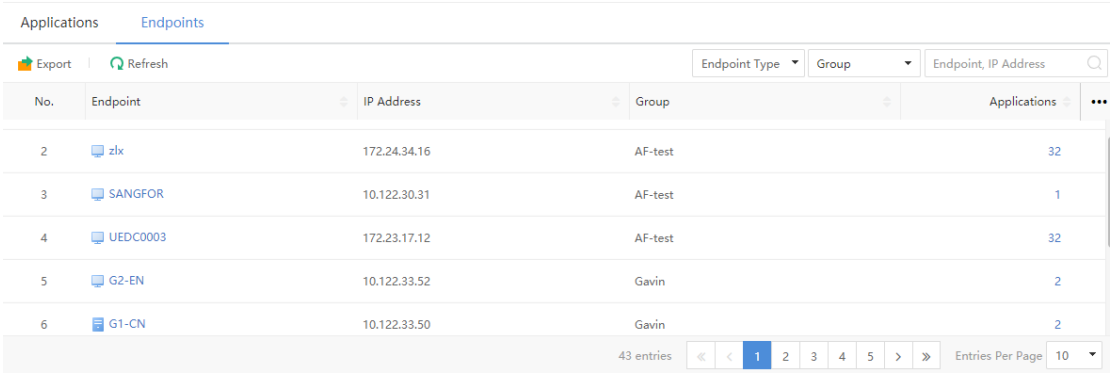
[Top 5 Applications Installed on Hosts] shows the the top 5 applications installed on hosts across the entire network.

[Applications] lists the number of endpoints that install a specific application on the

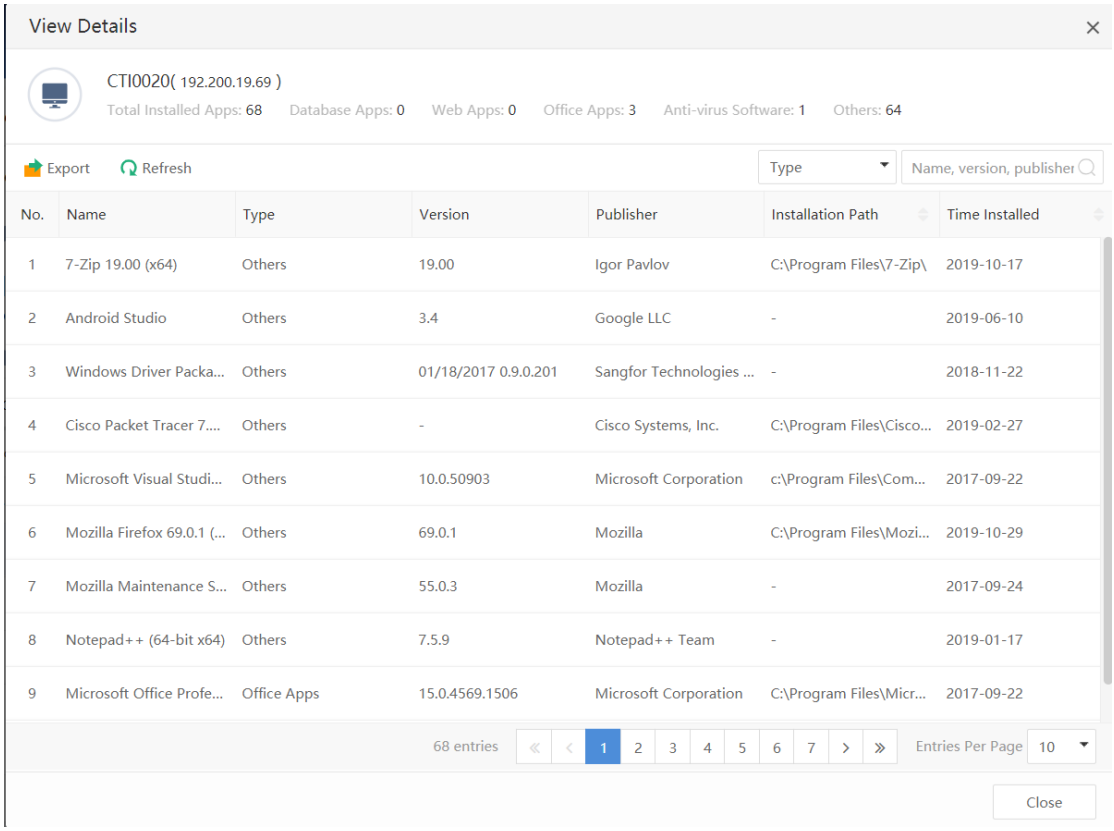
entire network, application name, application version, and application publisher. Click the number in the Endpoints column to view details of the endpoints, as shown below.



[Endpoints] lists the number of applications that each endpoint has installed, endpoint IP address, and group, as shown below.



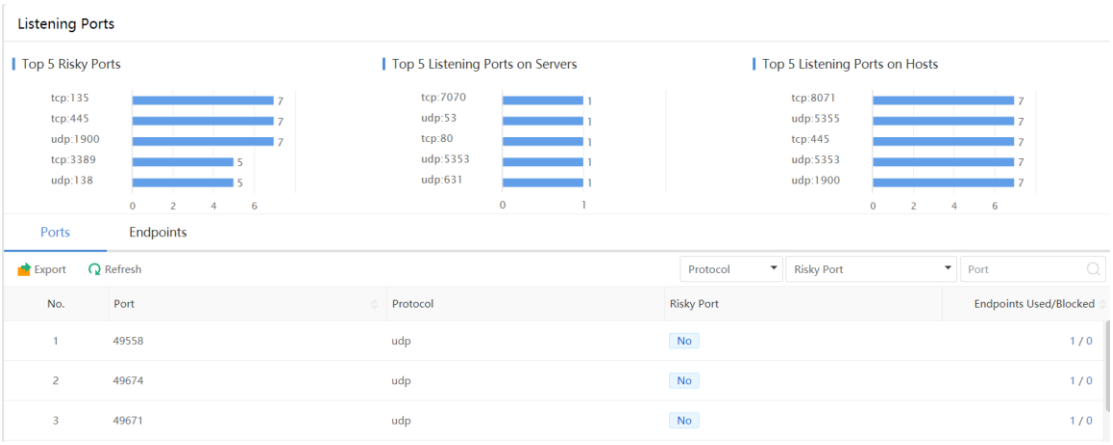
Click the number in the Applications column to view the details of all the applications installed on the endpoint, as shown below.



Click **Export** button to export as excel, which is convenient for the administrator to do further statistical analysis. In addition, you can further filter or search applications based on the application type, application name, version number, or publisher.

3.3.2.3 Listening Ports

The Listening Ports section provides a quick and easy way for administrators to view which ports are risky and open on the entire network and display information of the ports on servers and PCs, as shown in the following figure.

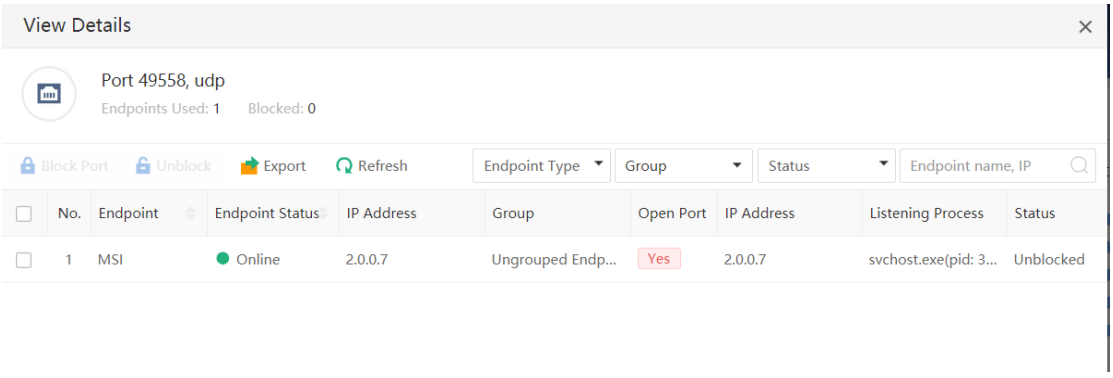


[Top 5 Risky Ports] displays the top 5 risky ports on all managed endpoints in the network. Endpoint Secure has a built-in risky ports..

[Top 5 Listening Ports on Servers] shows the top 5 listening ports on servers in the whole network.

[Top 5 Listening Ports on Hosts] displays the top 5 listening ports on hosts in the entire network.

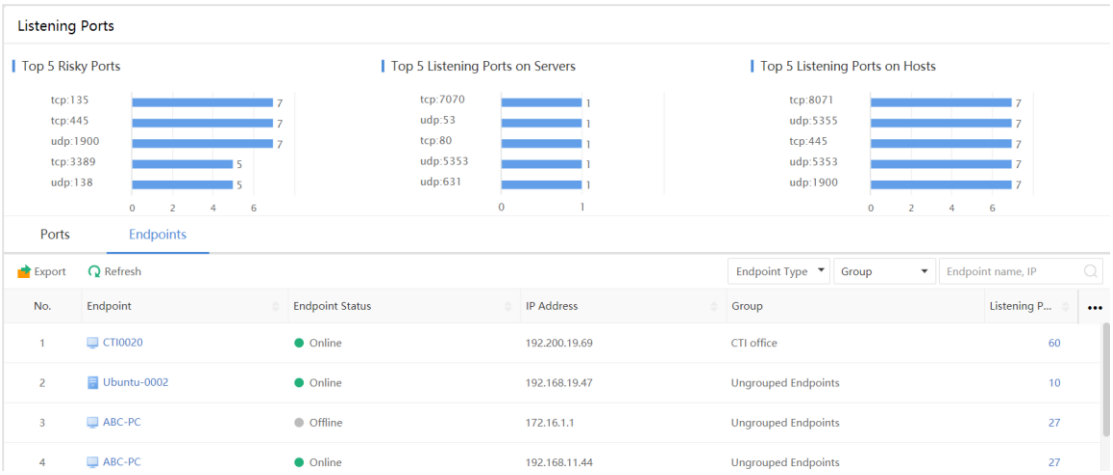
[Ports] lists the number of endpoints that have the port open. Click the number in the "Endpoints Used/Blocked" column to view the details of the endpoints that have the port open, as shown below.



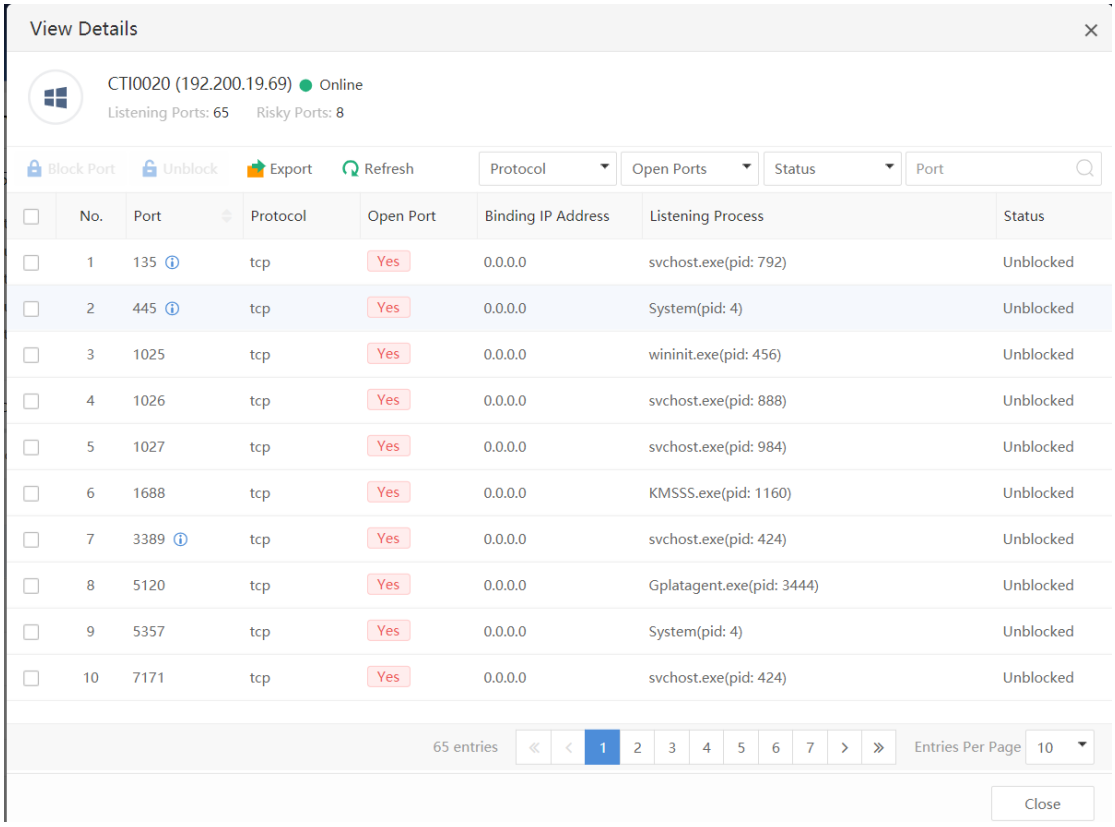
Select the endpoint that needs to block the port, click Block Port to block the risky port, and click Unblock to unblock the blocked port. Click Export button to export excel, which is

convenient for the administrator to make further statistical analysis.

[Endpoints] lists the number of listening ports on the endpoint, as shown below:



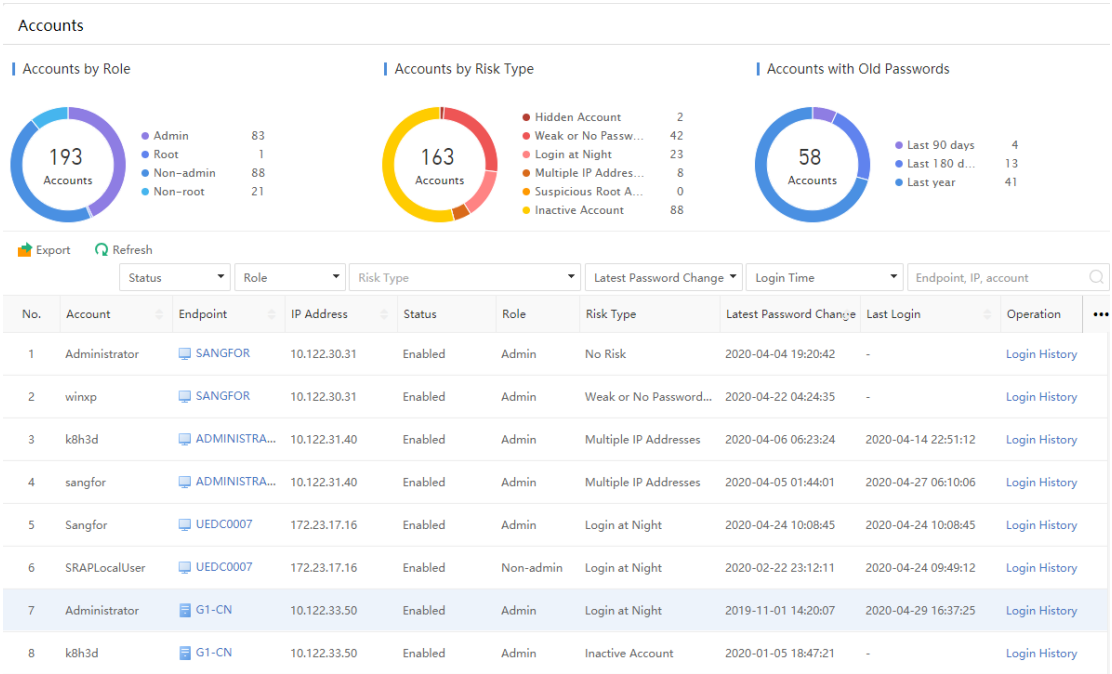
Click the number under the Listening Ports to view details of every open port on the endpoint, as shown in the figure below:



Click Block Port to block the risky port and click Unblock to unblock the blocked port. Click Export button to export as excel, which is convenient for the administrator to make further statistical analysis.

3.3.2.4 Accounts

The Accounts section provides statistics of accounts of endpoints on the entire network, such as hidden accounts, accounts with weak or no password, suspicious root accounts, inactive accounts, accounts logged in at night, accounts logged on multiple IP addresses, etc., in order to help administrators to discover risky accounts and take measures to mitigate risks, thereby minimizing host attack surface.



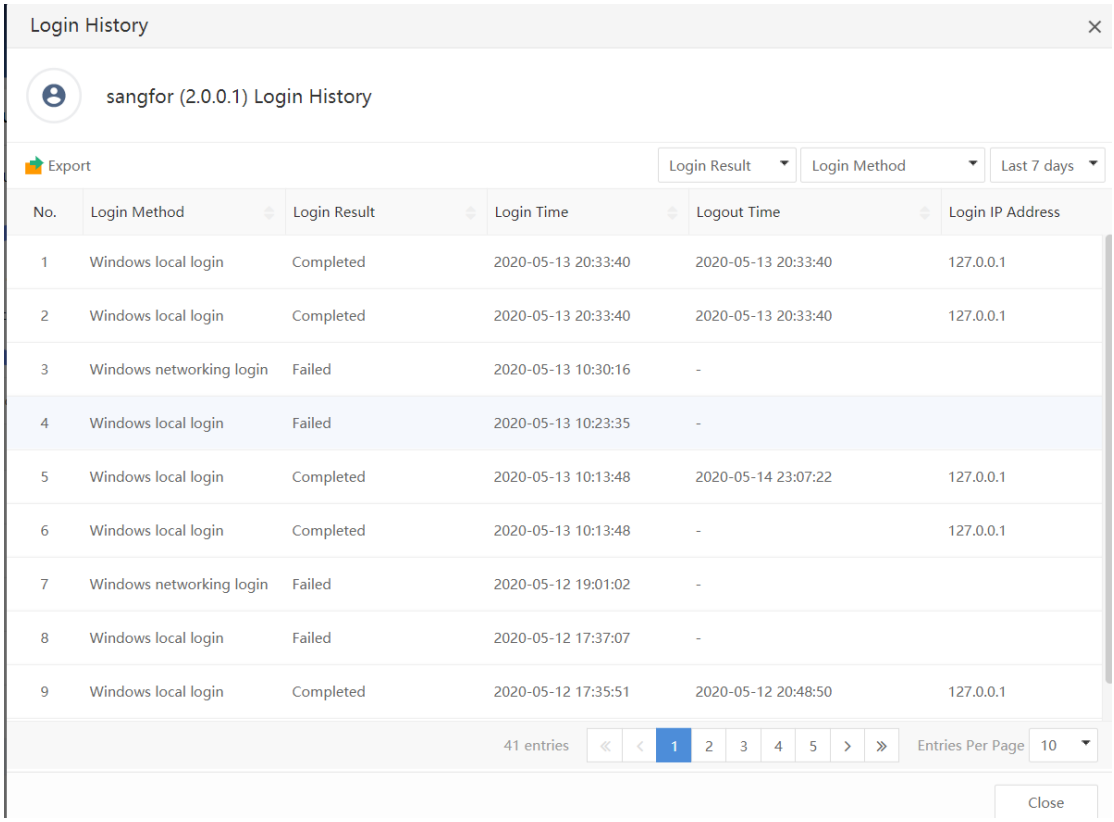
[Accounts by Role] displays the total number of accounts, and number of accounts of different roles such as Admin, Non-admin, Non-root, and Root.

[Accounts by Risk Type] displays total number of risky accounts and number of accounts with different risk types, including hidden accounts, accounts with weak or no password, suspicious root accounts, inactive accounts, accounts logged in at night, and accounts logged on multiple IP addresses,.

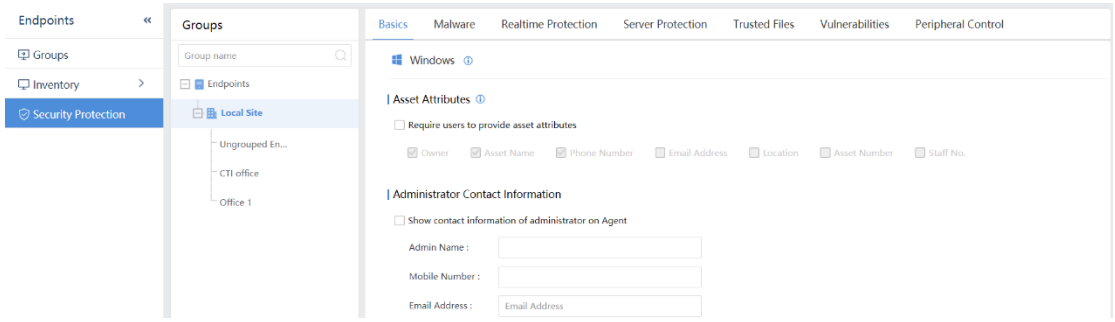
[Accounts with Old Passwords] displays the total number of accounts with old passwords and the number of accounts whose passwords have not been changed for 90 days, 180 days, and one year.

Click Export button to export as excel, which is convenient for the administrator to make further statistical analysis.

The Accounts list display the following information: account name, endpoint, IP address, account status, role, account type, risk type, ,latest password change time, last login time and operation. Click Login History to view account login history details, as shown below.



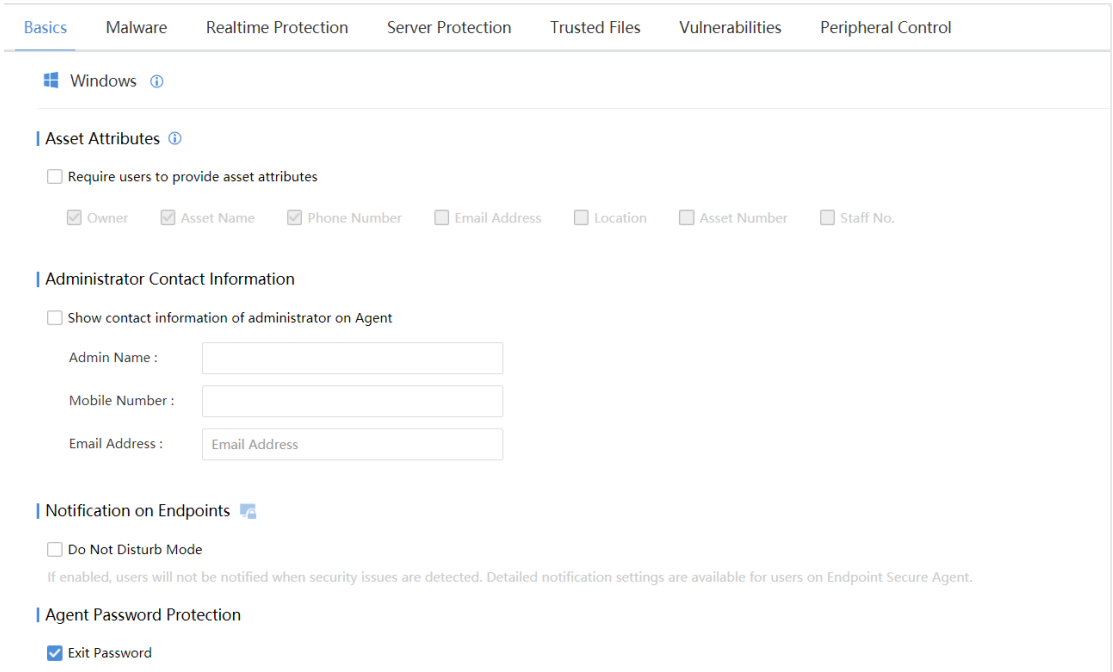
3.3.3 Security Protection

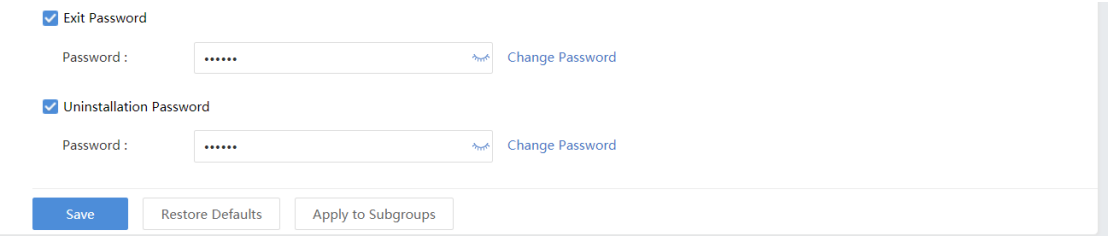


Security Protection defines security policies of endpoint groups. Select a specific group in **Endpoints > Security Protection > All Endpoints** to define the security policy of the group. There are five security policies: **Basic Policy, Malware, Realtime Protection, Server Protection, Trusted Files, Vulnerabilities and Peripheral Control**.

3.3.3.1 Basic Policy

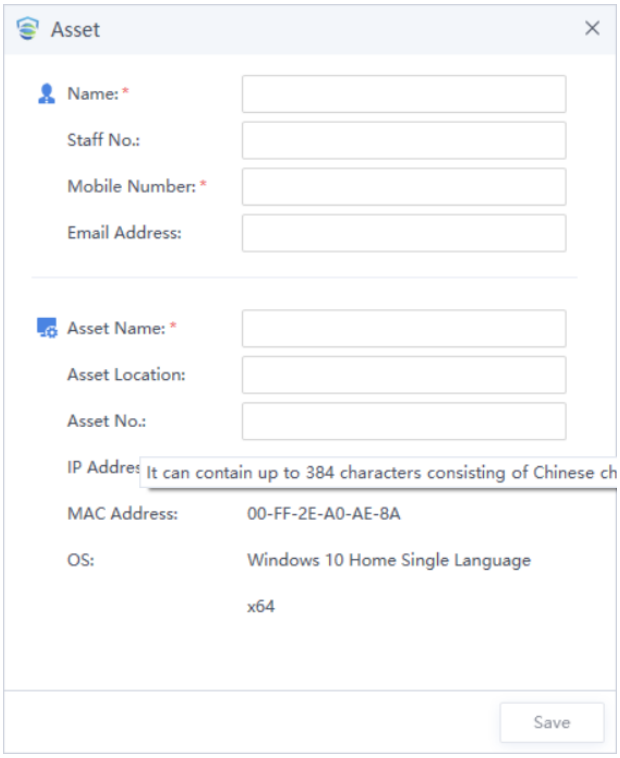
Basic Policy configures the Asset Attributes, Administration Contact Information, Pop up Message and Agent Password Protection, as shown below:





Windows OS: It describes operating system supported by basic policy. Basic policy is supported on Windows endpoints.

Asset Attributes: It describes asset information required by the Endpoint Secure Manager. If Required Asset Attributes is enabled, the following window pops up after the Agent is installed on endpoints:

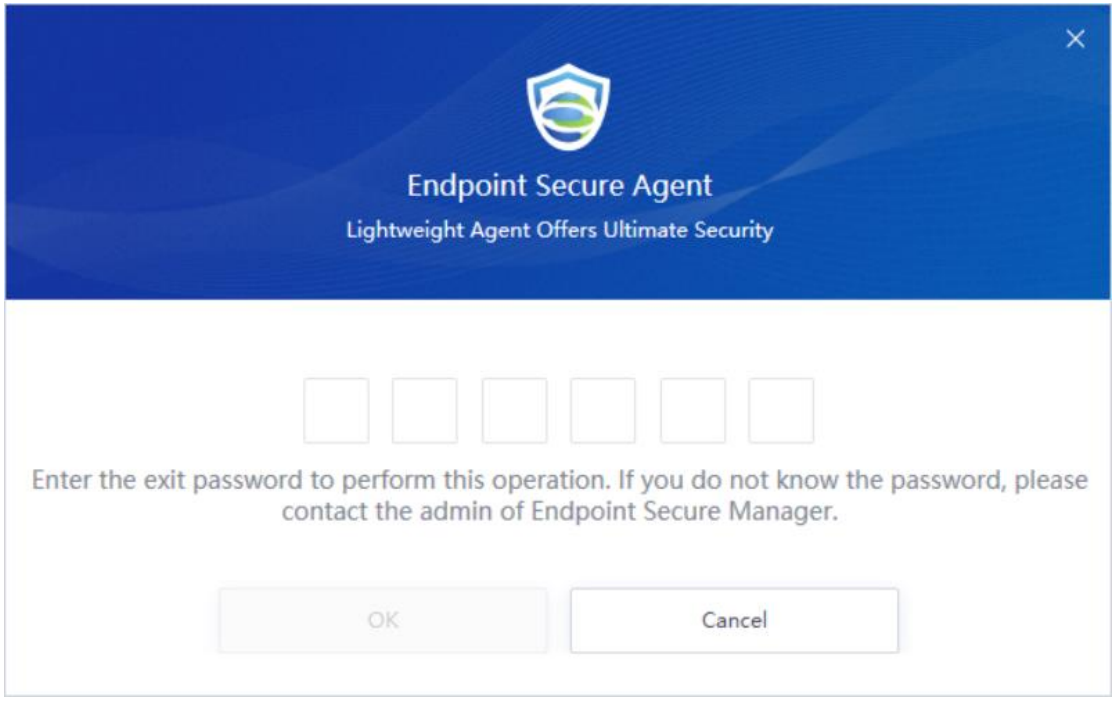


Administrator Contact Information: If there are multiple IT administrators in an enterprise and end users encounter problems with EDR and are not sure who to deal with, they can set the administrator contact information here and send them to the client. End users can view the administrator information through the client.

Pop up Message: When ES agent detects that there is a threat file on the Endpoint, a pop-up box in the lower right corner of the client will alert the user. This function can turn off or turn on whether to alert the user with one click. Configuration.

Agent Password Protection: It specifies the password used when exiting or uninstalling

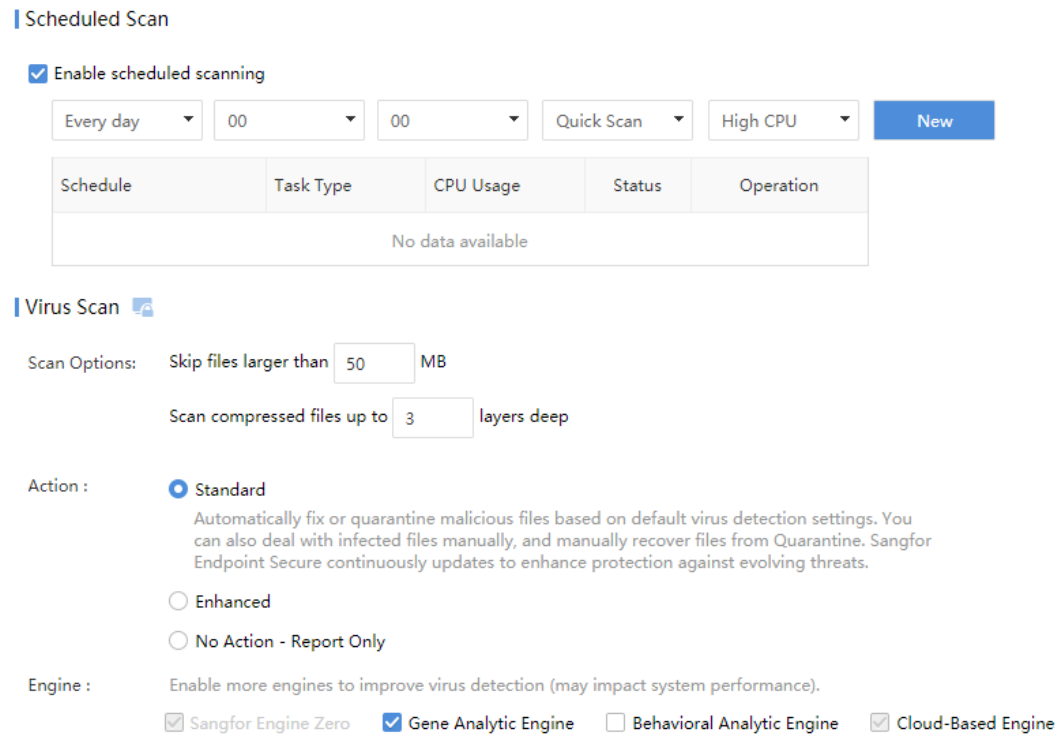
the Agent on endpoints (as shown below). You need to enter the password before exiting.



Click Save to save the current policy configuration. Click Restore Defaults to restore the current policy to defaults. Click Apply to Subgroup to let its subgroups to inherit the policies.

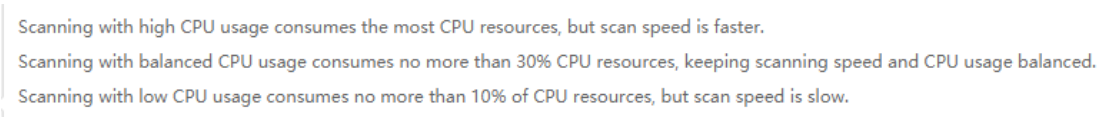
3.3.3.2 Malware

Malware protection policy provides Virus Scan and Antivirus Database Update for Windows and Linux endpoints, as shown below:



Windows OS: It defines the operating system supported by the policy. The policy supports both Windows and Linux endpoints. Click the drop-down button to select Windows or Linux OS.

Scheduled Scan: It defines the time when virus scan performed on endpoints in the network. The scan can be Quick Scan or Full scan. CPU usage can be High, Balanced and Low as shown below:



Virus Scan: It defines scanning conditions, action after malicious file detection and scan engine. You need to specify file sizes, conditions of compressed file scanning, and action on detected malicious files (No Action - Report Only is recommended).

There are three actions for virus scan:

Standard: Automatically fix or quarantine malicious files based on default virus detection s ettings. You can also deal with infected files manually, and manually restore files from Quar

antine. Sangfor Endpoint Secure continuously updates to enhance protection against evolvi ng threats.

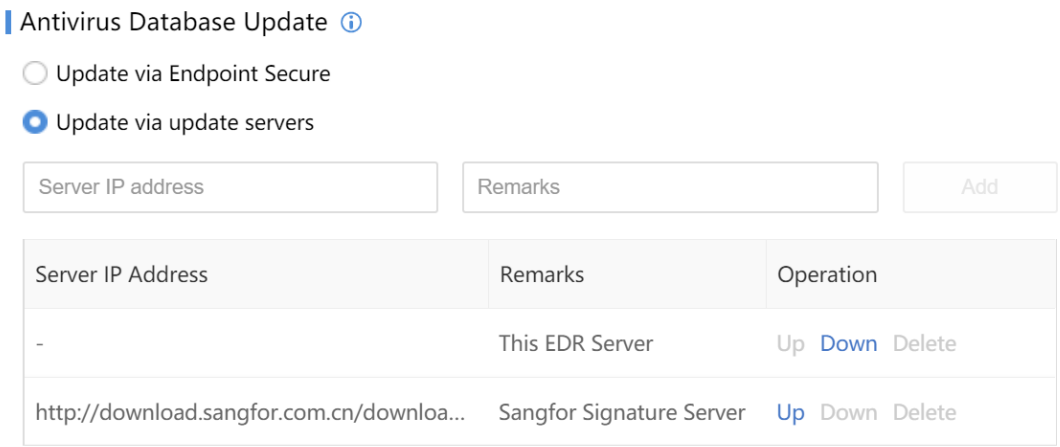
Enhanced: Fix or quarantine all suspicious files automatically, and you may restore them f rom the Quarantine. This is suitable for enhanced protection scenario

No Action-Report Only: Report information of infected files to the Manager and do not fix or quarantine infected files automatically Applicable to security guard on duty and they know how to fix threats.

Click icon to forbid policy changes on Agent and this policy can only be specified and distributed by the Manager.

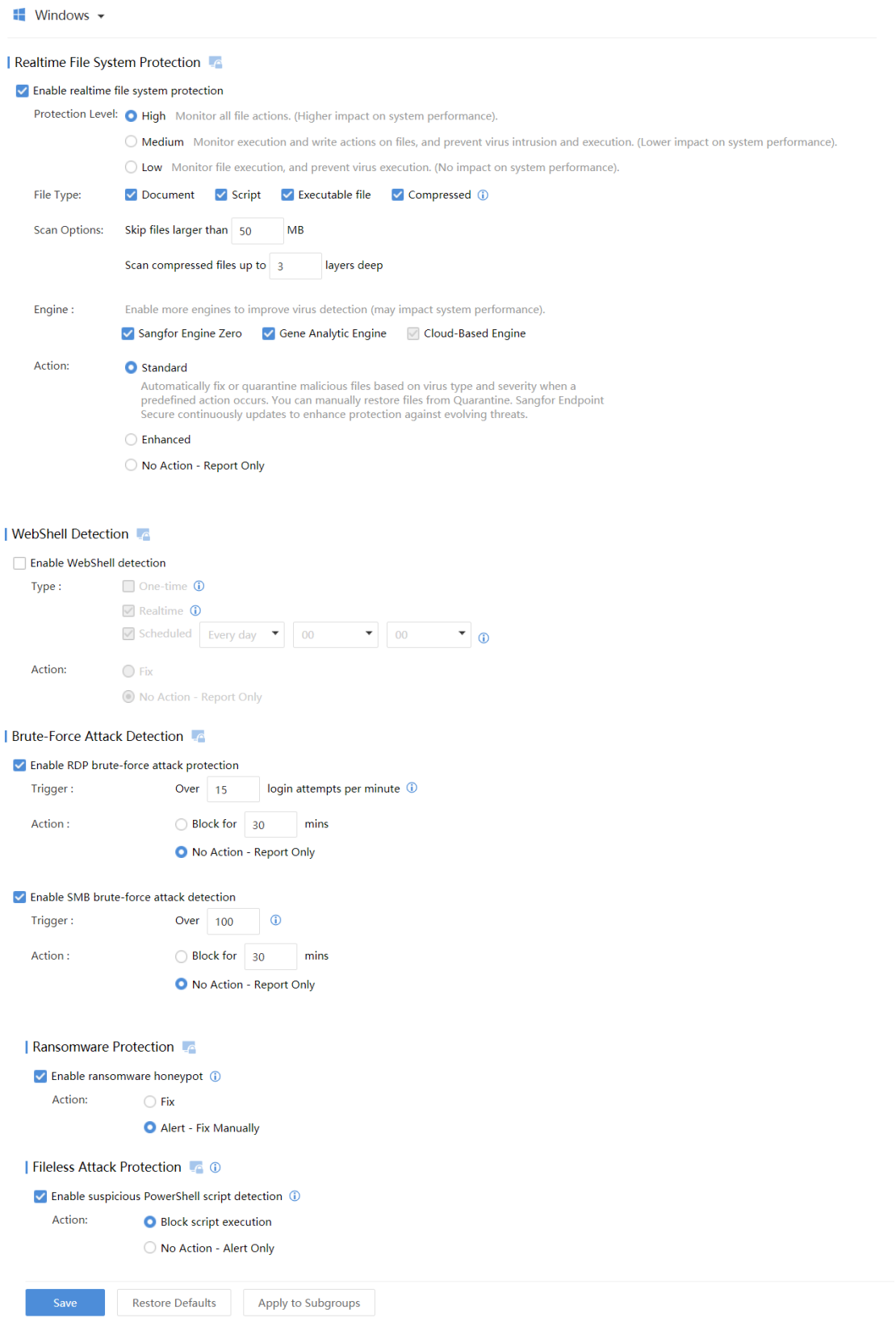
You may specify security engines used for virus scan. Sangfor Engine Zero and Cloud-based Engine is enabled by default, and the Gene engine and Behavioral Engine can be enabled or disabled as per your needs. Please note that the more security engines enabled, the more viruses detected, as well as more impacts on system performance.

Antivirus Database Update: It specifies the update serves for antivirus database update. There are two options for you: update antivirus database via endpoint secure or update antivirus database via update servers. When **Update via update servers** is selected, multiple update servers can be specified here from top to bottom, as shown below:



3.3.3.3 Realtime Protection

Realtime Protection supports Realtime Protection, Ransomware Detection, WebShell Detection, Brut-Force Attack Detection and Advanced Threat Defense on Windows OS and WebShell Detection and Brute-force Attack Detection on Linux OS, as shown below:

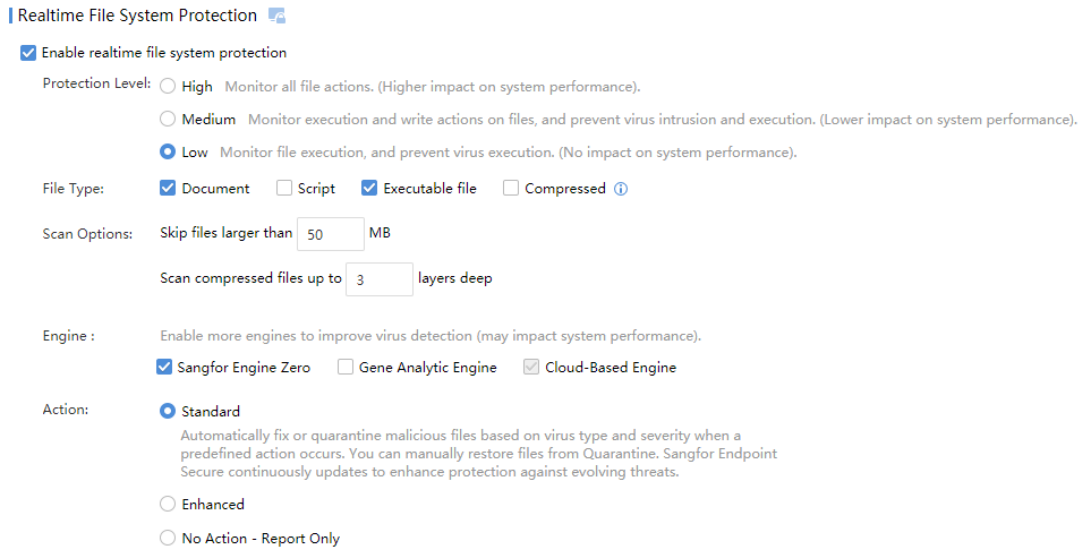


Windows OS: It defines the operating systems supported by the policy. The policy supports both Windows and Linux endpoints. However, the specific functions supported are different. Click the drop-down button to select Windows or a Linux OS. Currently, only WebShell

Detection and Brute-Force Attack Detection are supported by Linux OS.

Realtime Protection: It defines the detection conditions for real-time protection and the action after malicious file is detected.

Click  icon to forbid policy changes on Agent and this policy can only be specified and distributed by the Manager. Realtime protection can be edited on Agent by default.



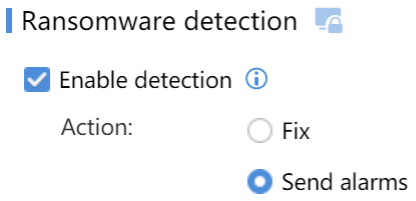
Protection Level: It allows you to select the Agent's CPU usage for malicious file detection and three level are supported: high, medium and low. Different protection levels provide different protections against malicious files and have different impacts on host performance.

File Type: You can specify the type of the files that you want to monitor.

File Scan: It allows you to skip scanning files larger than a certain size and deeper than certain compression level (malicious files are small-sized in most cases).

Engine: It specifies the security engine used by real-time protection. The Cloud-based Engine is enabled by default and cannot be disabled. The Sangfor Engine Zero and Gene Engine can be enabled or disabled as per your needs. The more engines enabled, the more detection, as well as more impacts on host performance.

Action: Choose to **Standard, Enhanced** or **No Action - Report Only** when malicious file is detected. The action function can refer to **3.3.3.2** Malware Detection.

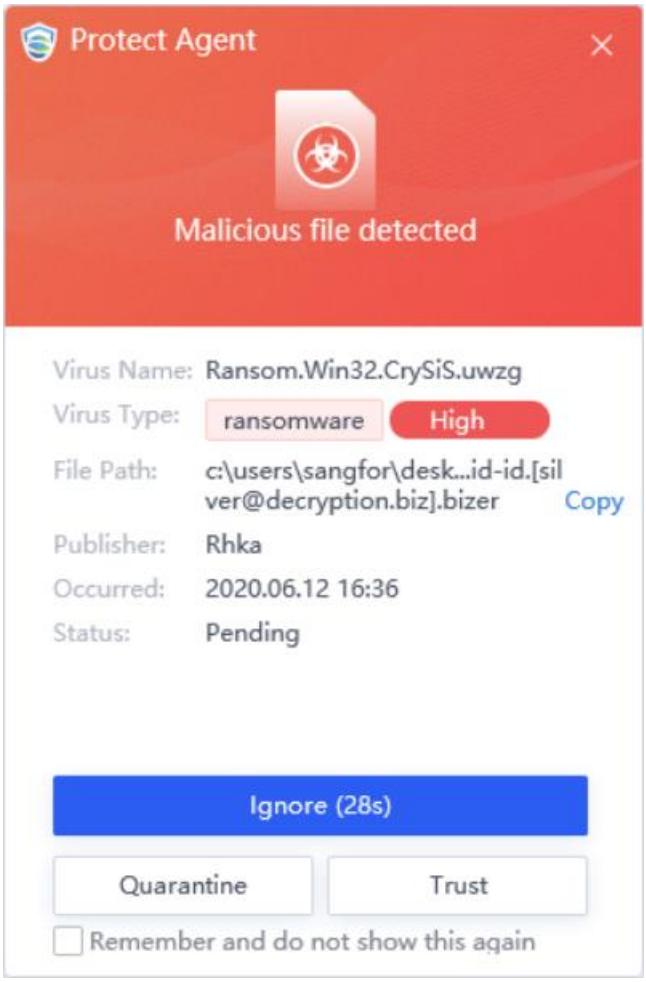


Ransomware Detection: The bait file is placed in the key directory on endpoint. When the endpoint is infected with the ransomware, the ransomware will encrypt the bait file first, and the Endpoint Secure Agent promptly intercepts and alerts to discover and clear the ransomware as soon as possible, keeping the business files on endpoints from being encrypted maliciously.

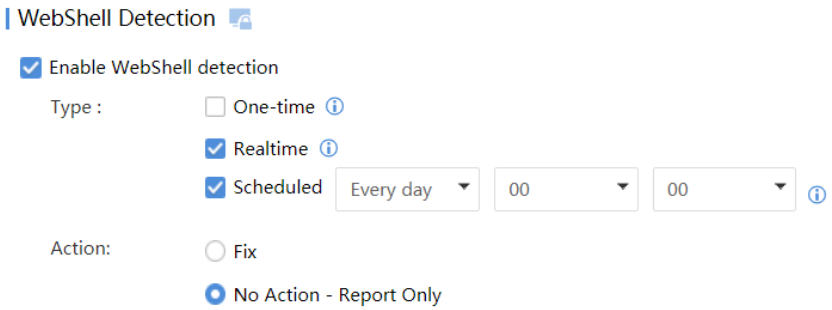
Click icon to forbid policy changes on Agent and this policy can only be specified and distributed by the Manager. Ransomware detection is allowed to be edited on Agent by default.

Enable detection: It indicates whether the ransomware detection is enabled or not. To use ransomware detection, Realtime protection should also be enabled.

Action: It specifies the action after ransomware is detected. “Send alarms” is recommended. When ransomware is detected on endpoints, the alarm will pop up at the lower right corner of the desktop, as shown below:



WebShell Detection: It specifies WebShell detection methods and action after WebShell backdoor is detected. The WebShell detection is supported on Windows servers and Linux OS, and it only detects the WebShell backdoor under root directory and its sub-directories of web servers.

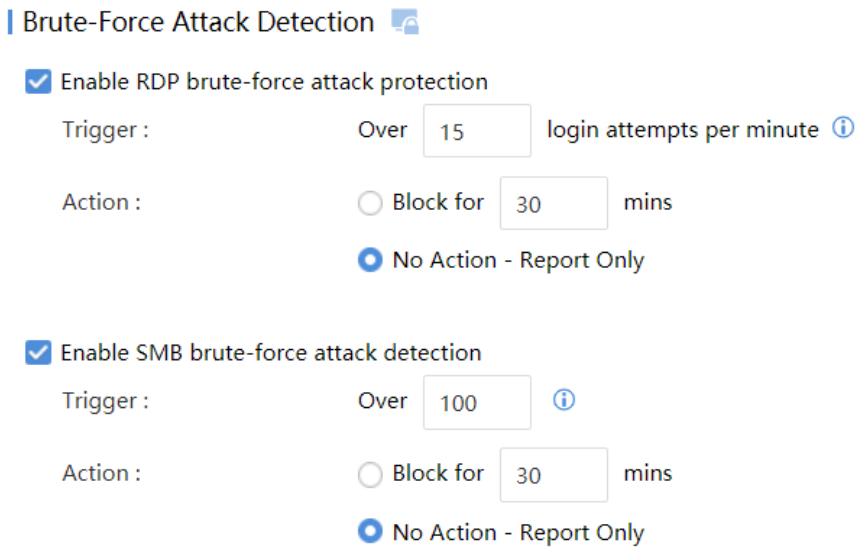


Type: There are three detection methods: One-time, Realtime, and Scheduled. One-time refers to it applies WebShell detection when Agent is first installed on endpoints and scans the website's root directory and its sub-directories. Realtime refers to that it scans the new

files in the website's root directory and its sub-directories. Scheduled refers to that it regularly scans all files in the website's root directory and its sub-directories.

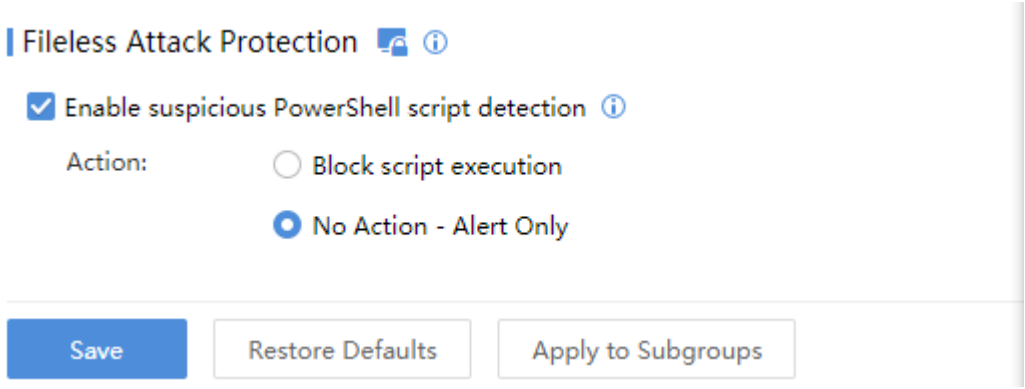
Action: It specifies the action after WebShell backdoor is detected.

Brute-Force Attack Detection: The Endpoint Secure can detect and block RDP, SMB, SSH brute-force attacks. The following figure shows whether the brute-force attack detection is enabled or not and its action after brute-force attack is detected.



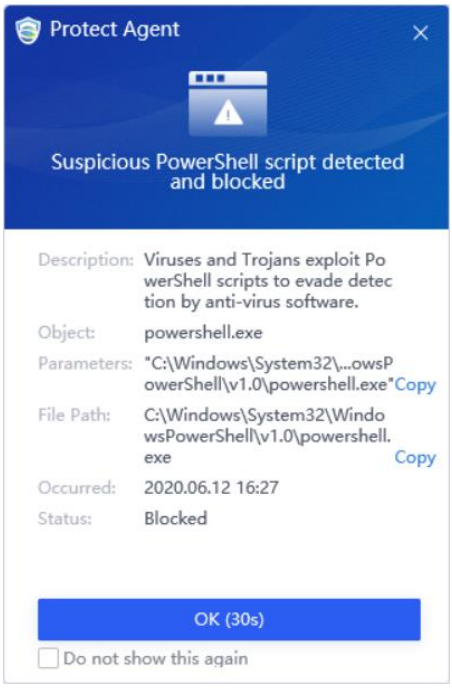
Filess Attack Protection: It specifies protection against fileless attacks. Fileless attack is an advanced attacking techniques that takes advantage of a vulnerable application, injects code into a normal system process (memory, registry, PowerShell script, MS office documents) to gain access privilege and execute attacking commands on targeted endpoints.

Click icon to forbid changes on Agent and this policy can only be specified and distributed by the Manager. Advanced threat defense is allowed to be edited on Agent by default.



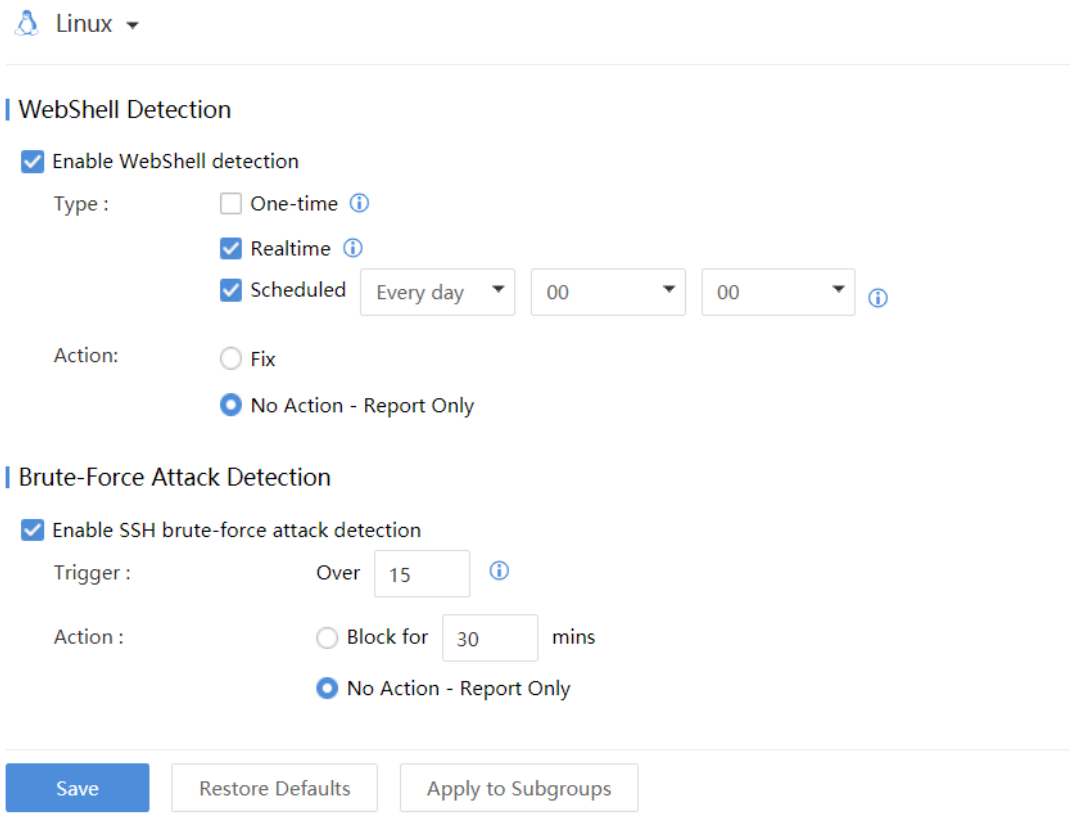
Check the option Enable s**uspicious PowerShell script detection** to enable the fileless attack protection.

The action after suspicious PowerShell script execution is detected can be set to Block script execution or No Action - Alert Only. No Action - Alarm Only is recommended. When a suspicious PowerShell script execution is detected, the following alert message pops up on Agent:



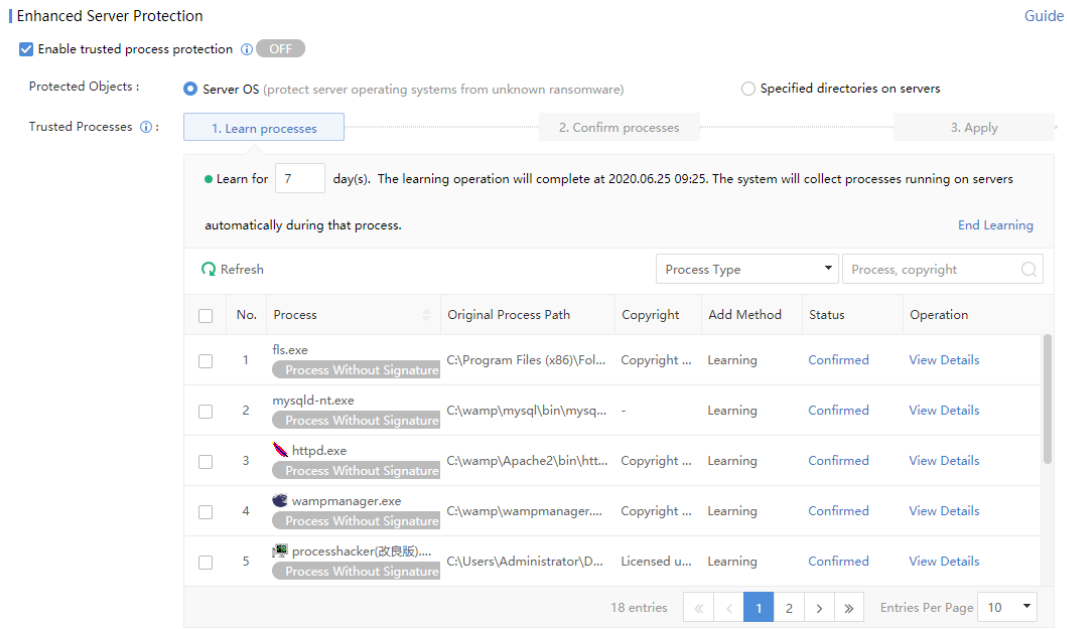
After **No Action - Alert Only** is selected, actions are different for servers and PCs. For PCs, alert message is sent when PowerShell script execution is detected and the execution is suspended, and users will determine whether the execution is allowed or blocked. For servers, alert message is sent when PowerShell script execution is detected and the execution will not be suspended and users will determine whether the execution is allowed or blocked.

For Linux endpoints, only **WebShell Detection** and **Brute-Force Attack Detection** are supported. **Realtime Protection** and **Ransomware Detection** are not supported, as shown below:



3.3.3.4 Server Protection

The Server Protection section provides protection for the server operating system or specific directories of servers, allowing only trusted processes to run, read and write operations. This function is only applicable to Windows Server, but not applicable to Windows PC and Linux systems.



Scenario 1: Server OS Protection

Applicable scenarios:

It is suitable for protecting stable server systems and preventing untrusted processes (such as ransomware and other viruses) from running on the server.

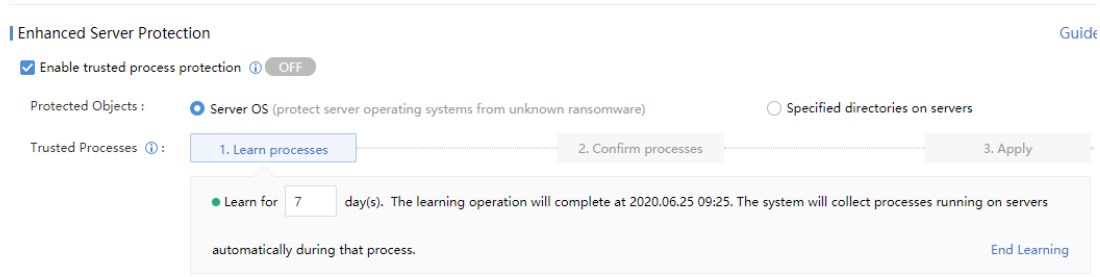
Configuration steps:

Step 1: Perform virus scan and removal on servers

First, perform virus scan on servers to ensure they are secure.

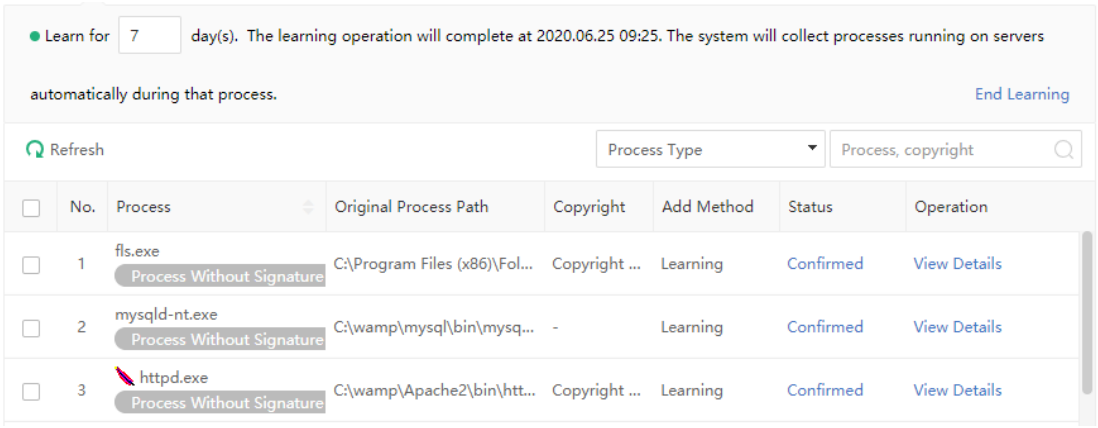
Step 2: Learn processes

Set server protection policy for the group where the server is located. Enable trusted process protection, select [Server OS] as the protection object; specify learning period which can be 1 day to 30 days. Then, click Save to save the settings.



Step 3: Confirm the processes

After the process learning is finished, a trusted process confirmation is required. The administrator analyzes the process learning results, deletes untrusted processes, adds trusted processes that have not been learned, and completes the confirmation of trusted processes.



Process: Displays process name.

Process Type: Displays process type, suspicious process or system process.

Original Process File Path: Displays the first collected process file path.

Copyright: Displays copyright information of processes.

Add Method: Displays the adding method of the process. There are three ways to add processes: by learning, by adding manually, or by template.

Status: Shows the status of the process. "Unconfirmed" means that a process has not been confirmed.

Operation: You can delete a process, view process details, or perform process analysis operation.

If you are sure that a process is an untrusted process, click the Delete to delete it.

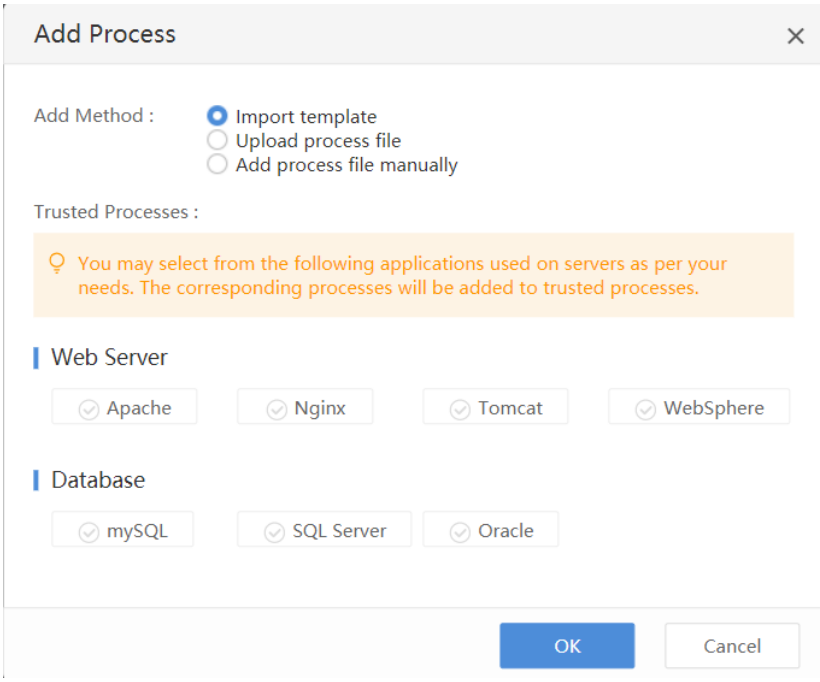
To view process details, click the Details.

If you are unable to confirm whether a process is a trusted process, you can click "Analyze" to further analyze the current process with the help of Sangfor Threat Intelligence and then confirm it.

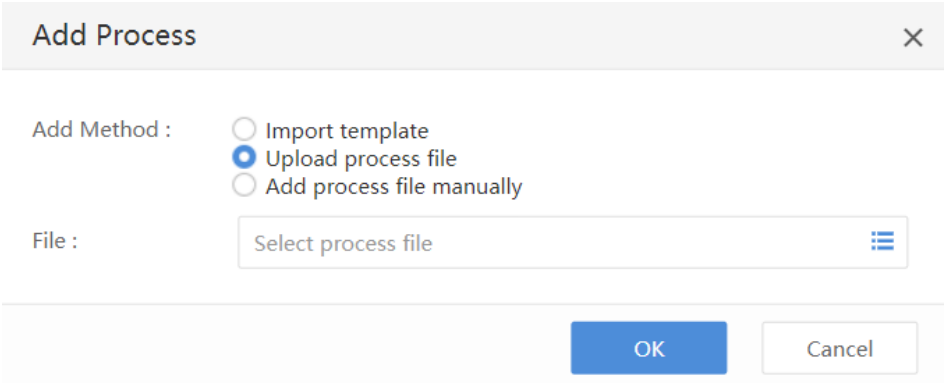
If you find that some trusted process is not in the learning result, you can click Add Process to add it.

Add Process: There are three methods of adding processes: Import template, Upload process file, and Add process file manually.

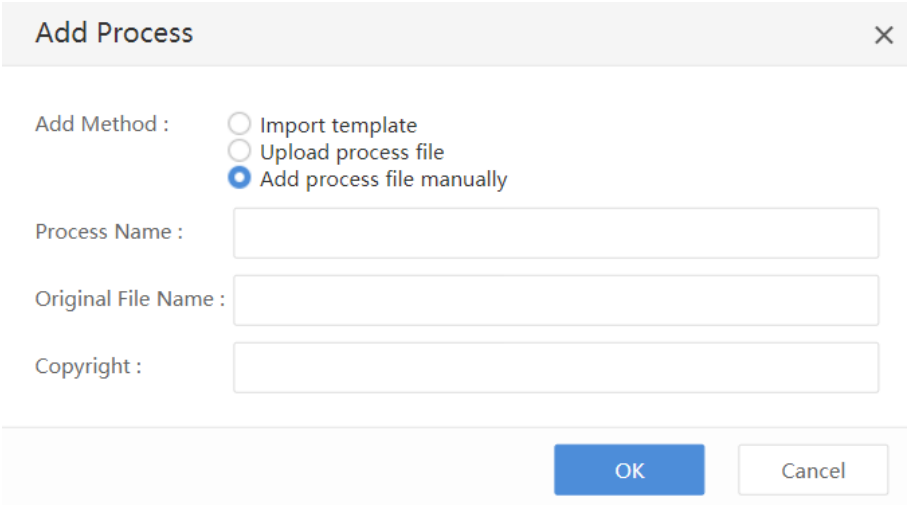
Import template: This method is applicable to the situation that the processes to be protected are those listed in the template: Web servers or database servers



Upload process file: Check this option to upload a trusted process file.

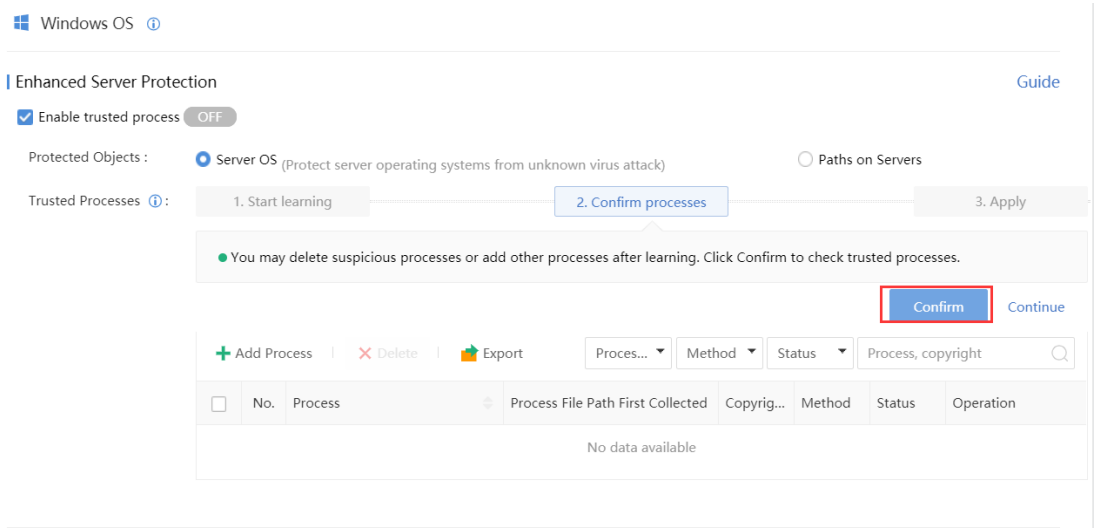


Add process file manually: Select this option to add process file manually by, specifing process name, original file name, and copyright information of the trusted process.



Step 4: Apply the trusted processes

After checking the trusted processes, click Confirm to complete the trusted process confirmation.



Click Save to save the settings and the server protection will take effect.

Scenario 2: Specific Server Directory Protection

Applicable scenarios:

This is used to protect critical server directories and files from unauthorized access and modification by ransomware.

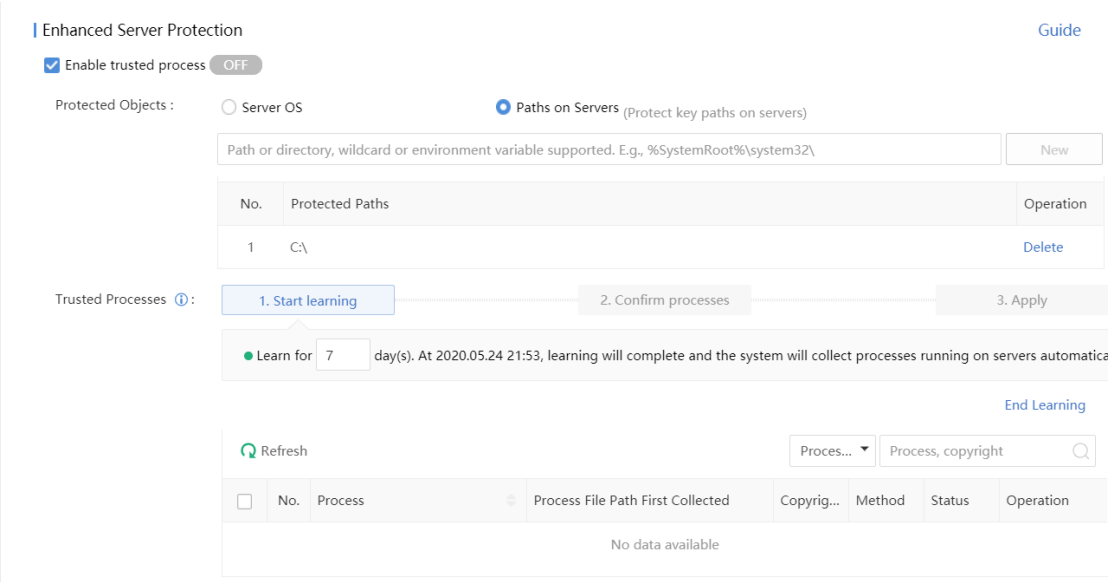
Configuration steps:

Step 1: Perform virus scan on servers

First, perform virus scan on servers to ensure they are secure.

Step 2: Add server directories

Select the group where the server is located. Check the option **Enable trusted process protection**, select **Specific directories on servers** as the protection object, and manually add important server directories to be protected. Server directory can contain * wildcard or environment variables.

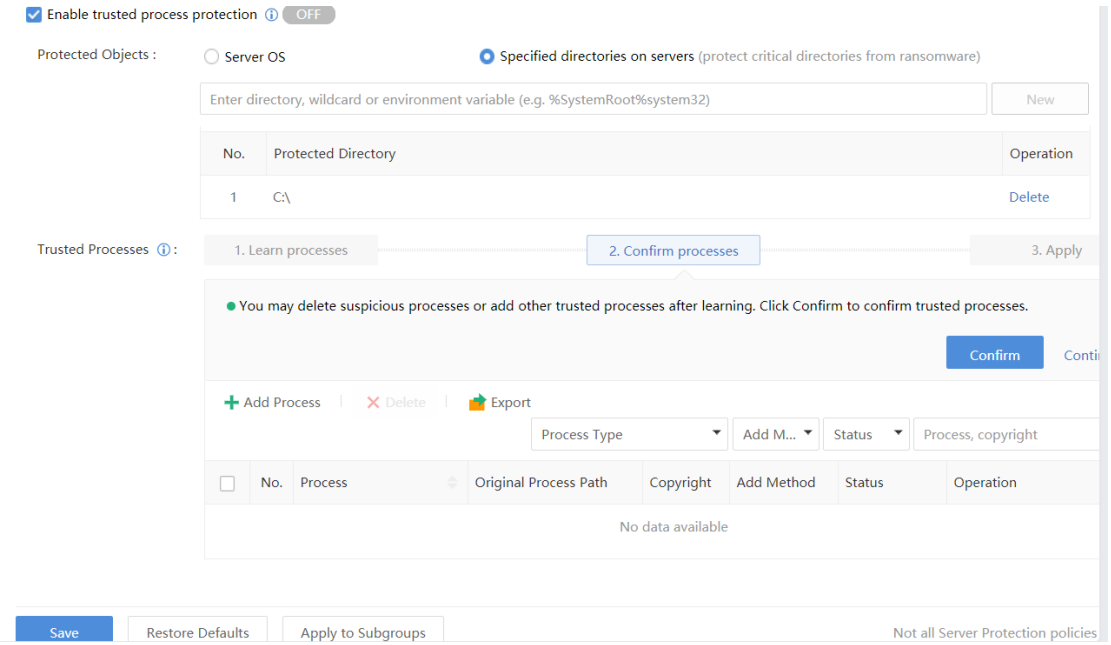


Step 3: Learn processes and confirm

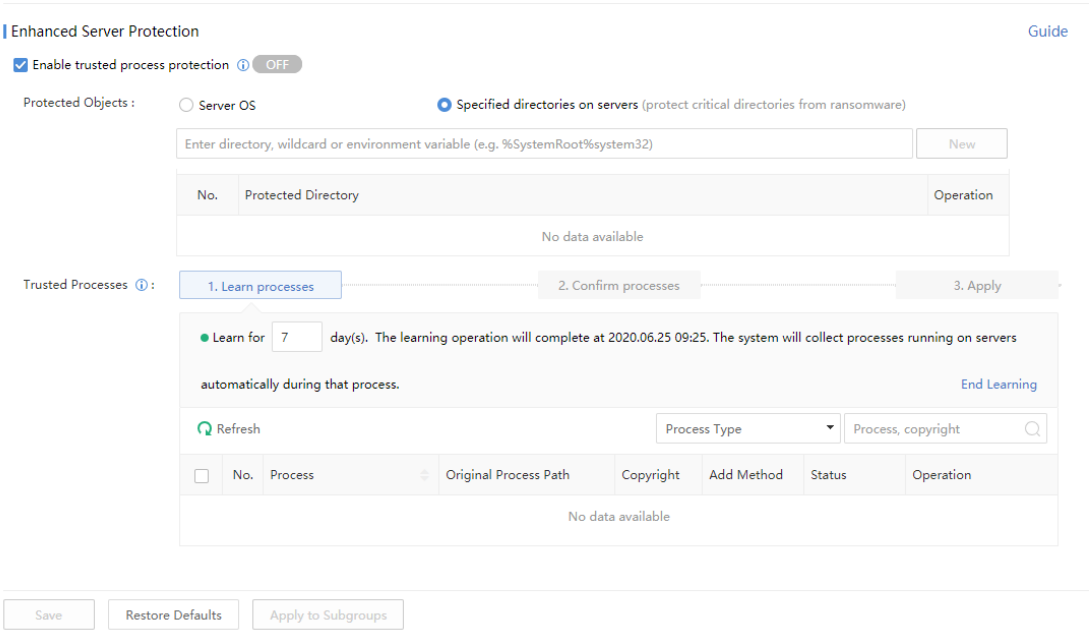
The process learning and confirmation process is the same as that described for server OS protection. Please refer to the section “Scenario 1: Server OS Protection” in this chapter.

Step 4: Apply the trusted processes

After checking the trusted processes, click Confirm to complete the trusted process confirmation.



Specify the action on untrusted processes, as shown below.

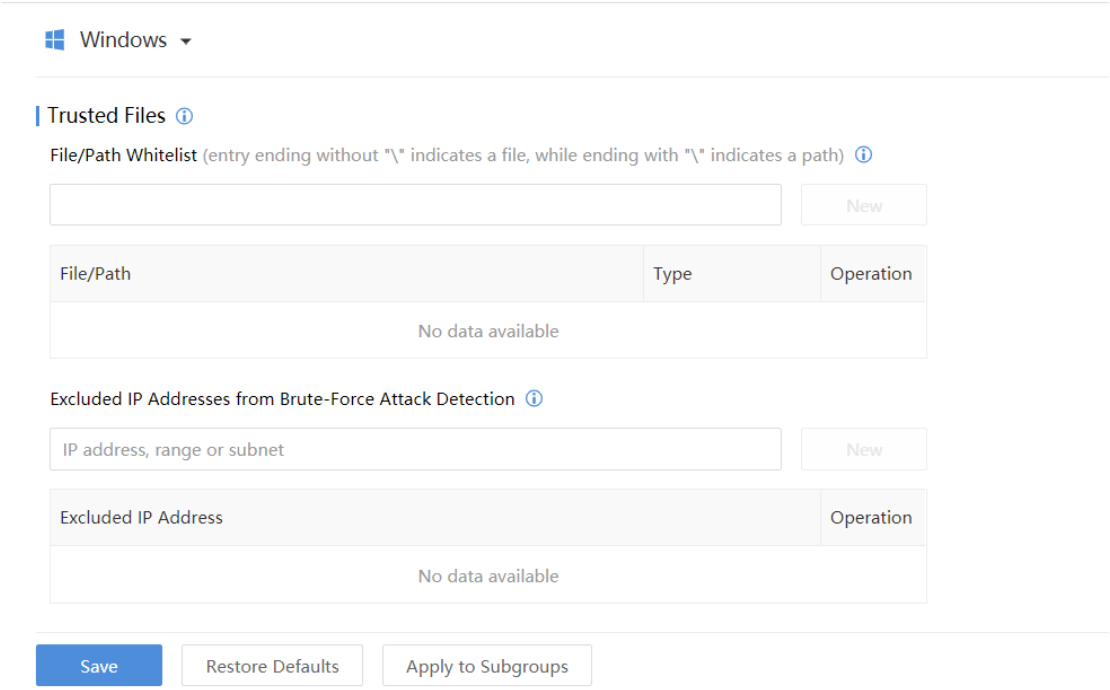


[Prohibit Untrusted Process from] There are two options: Access, Modification. If you choose Modification, untrusted processes cannot perform operation like adding, deleting or modifing against protected directories. If you choose Access, untrusted process are not allowed to access the protected directories.

[Action] There are two options: Block operation, Block operation and terminate process. When an untrusted process is found to operate on the protected directory, you can choose to block or terminate it.

3.3.3.5 Trusted Files

Trusted files specify files or directories that can be trusted and will be skipped by realtime protection and virus scan or excluded IP addresses from bruce-force attack detection, as shown below:



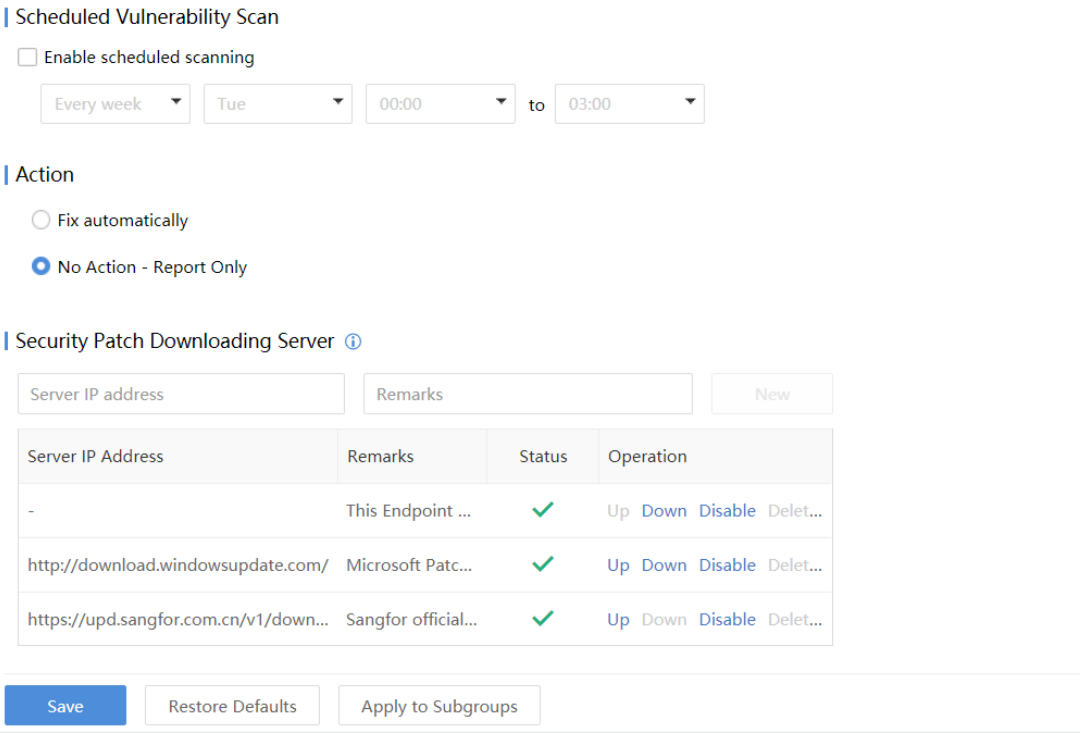
Windows: In the dropdown list, you can choose Windows or Linux. Windows systems suppport File/Path Whitelist and Excluded IP Addresses from Brute-Force Attack Detection settings while Linux systems only supports Excluded IP Addresses from Brute-Force Attack Detection settings.

File/Path Whitelist: You can add any files or directories that are trusted. Entries ending with "\" indicate a directory while ending without "\" indicate a file.

Excluded IP Addresses from Bruce-Force Attack Detection: You can add IP address to exclude it from to bruce-force attack detection.

3.3.3.6 Vulnerabilities

The Vulnerabilities page provifes Scheduled Vulnerability Scan and Security Patch Downloading Server sections, as shown below:



Windows: It indicates operating system supported by vulnerability fix. Currently only Windows OS is supported.

Scheduled Vulnerability Scan: It specifies the scheduled time to perform vulnerability scan.

Action: It specifies the actions performed after vulnerability is detected.

Security Patch Downloading Server: It specifies servers from which endpoints download security patch. The default server is Sangfor CDN Server, Microsoft Vulnerability Patch Server, and the Endpoint Secure MGR.

If the Agent on endpoint cannot connect to Internet or download security patches from the Sangfor CDN server or Microsoft security patch server, there are two solutions:

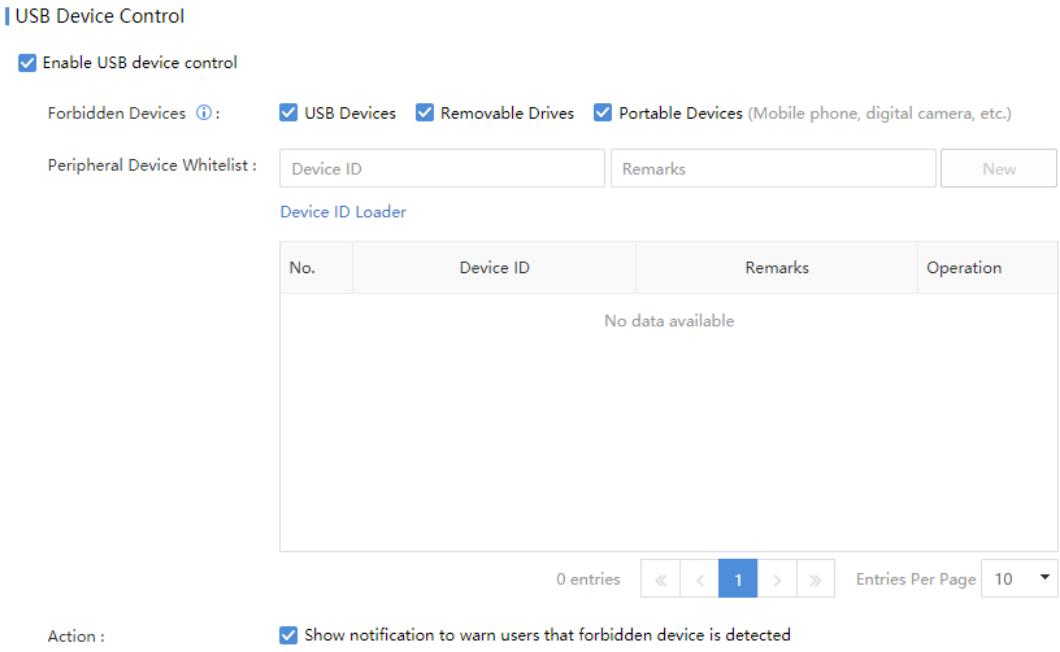
1. Establish security patch server in the intranet, and the Agent on endpoints downloads security patches from the intranet server. This solution is recommended.

2. The MGR can connect to the Internet and it downloads security patches. And then the Agent on endpoints downloads security patches from the Manager. Go to **System** > **System** >

General and enable Security Patch Download on Endpoint Secure Manager, as shown below:

3.3.3.7 Peripheral Control

Peripheral Control is used to control which USB devices can be inserted into endpoints. This is only applicable to Windows OS.



Forbidden Devices: Select the USB device that are not allowed to insert to endpoints.

Peripheral Device Whitelist: Add USB devices to whitelist that are allowed to insert to endpoints.

Action: Show notification when forbidden USB device is detected.

1. The section is only applicable to Windows OS, not the Linux OS.

2. No Action-Report Only is recommended and manual fix can be performed as per

your needs.

3. Security protection supported on different operating systems and endpoint type is shown as below:

Security Policies	Windows PC	Windows Server	Linux
Basics	√	√	×
Malware	√	√	√
Realtime Protection	√	√	×
WebShell Detection	×	√	√
Ransomware Detection	√	√	×
Brute-Force Attack Detection	√	√	√
Fileless Attack Protection	√	√	×
Trusted Files	√	√	×
Vulnerabilities	√	√	×
Server Protection	×	√	×
Peripheral Control	√	√	×

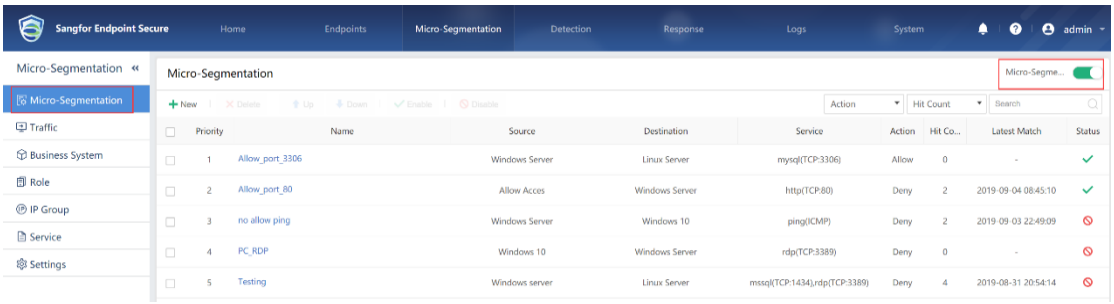
3.4 Micro-segmentation

The micro-segmentation function can allow necessary service ports and disable all unnecessary ports to improve business security and protect servers. Traffic segmentation status is visualized.

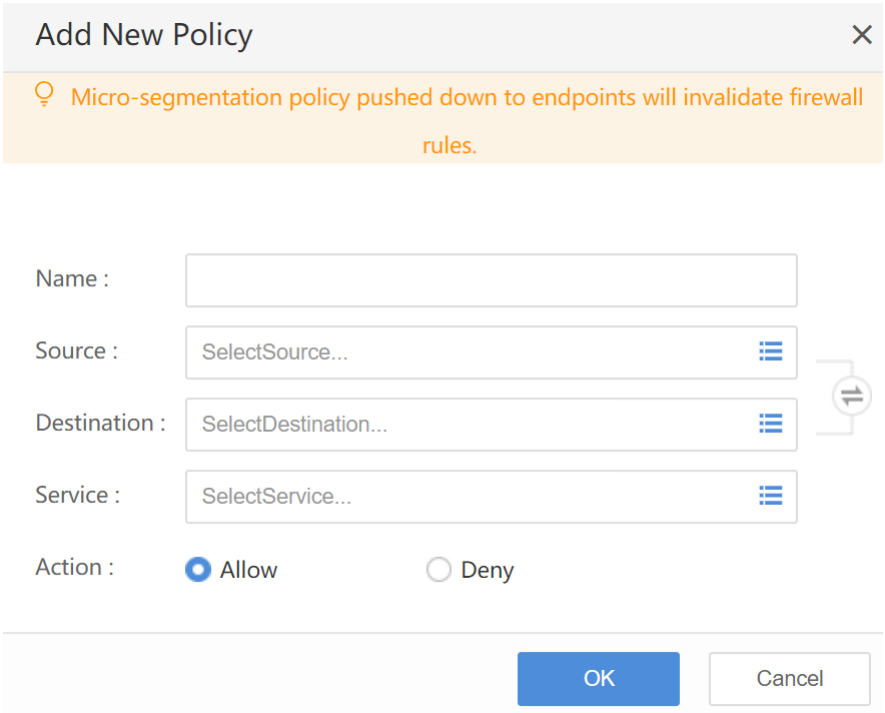
3.4.1 Micro-segmentation Policy

Click Micro-segmentation switch on the right top corner to turn on or turn off micro-segmentation.

Micro-Segmentation Policy: Policies can be added, deleted, or disabled, and based on the quintuple matching data, it allows or denies the access.



Click New to configure the micro-segmentation policy as shown below:



Name: It defines the name of the micro-segmentation policy.

Source: It indicates the source that accesses the target service. You can select the business system, role, server, and IP group as the source.

Destination: It indicates the target endpoint to be accessed.

Service: It indicates the service port of the target endpoint.

Action: The action of the micro-segmentation policy can be selected as **Allow** or **Deny**.

Click ⇌ to interchange the source with the destination

Click OK to submit.

Delete: Select a policy to be deleted and click Delete to delete the policy.

Up: Select a policy to be moved up and click Up to move the policy. Only one policy can be moved at a time.

Down: Select the policy to be moved down and click Down to move the policy. Only one policy can be moved at a time.

Enable: Select a policy to be enabled and click Enable to enable the policy.

Disable: Select a policy to be disabled and click **Disable** to disable the policy.

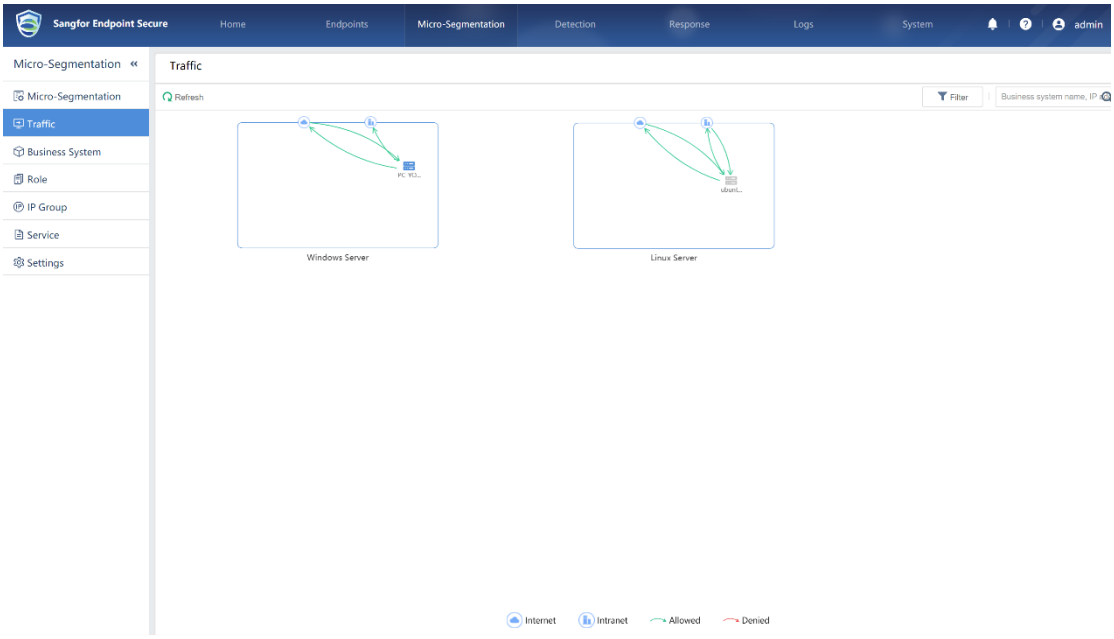
Hit Count View the number of logs matching the policy.

Matches: It indicates the number of logs matching the policy.

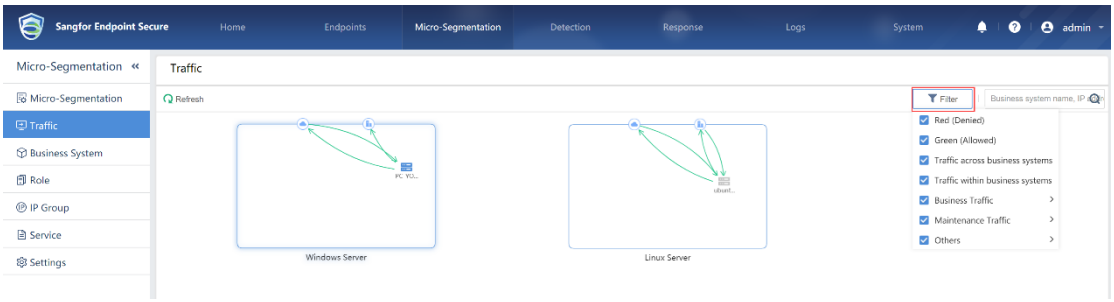
Status: Click ✓ or ⊘ to enable or disable policy.

3.4.2 Traffic Statistics

This page supports visually displaying traffic statistics of endpoints, access to public network, internal accesses and allowed and denied traffic. You can view traffic statistics by filtering the criteria. Configure **Micro-segmentation Policy, Business Systems, IP Groups, Services** and view when there is any traffic generated.



Click Filter. The filtering conditions are as shown below:



Denied traffic(Red): It indicates the denied traffic.

Allowed traffic (Green): It indicates the allowed traffic.

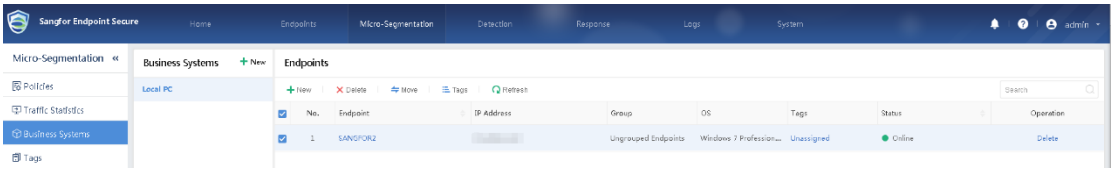
Inter-business system traffic: The access traffic between business systems.

Intra-business system traffic: The access traffic within the business system.

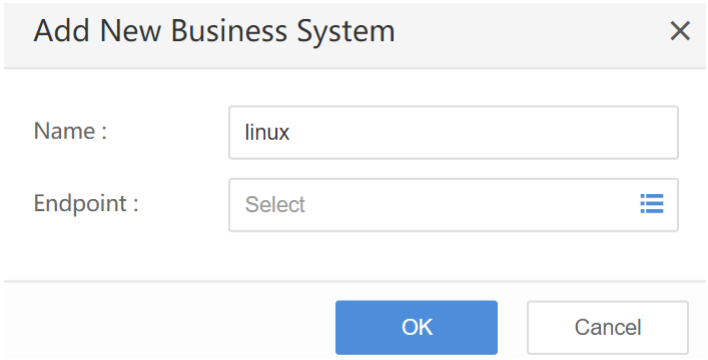
Business traffic, Maintenance traffic and Other traffic need to be defined via **Services**. For details, see **Section 3.4.6 Service.**

3.4.3 Business System

Configure business system and add multiple endpoints into one business system. One endpoint can only be added into one business system. This can be used by micro-segmentation policy and display of traffic segmentation status.

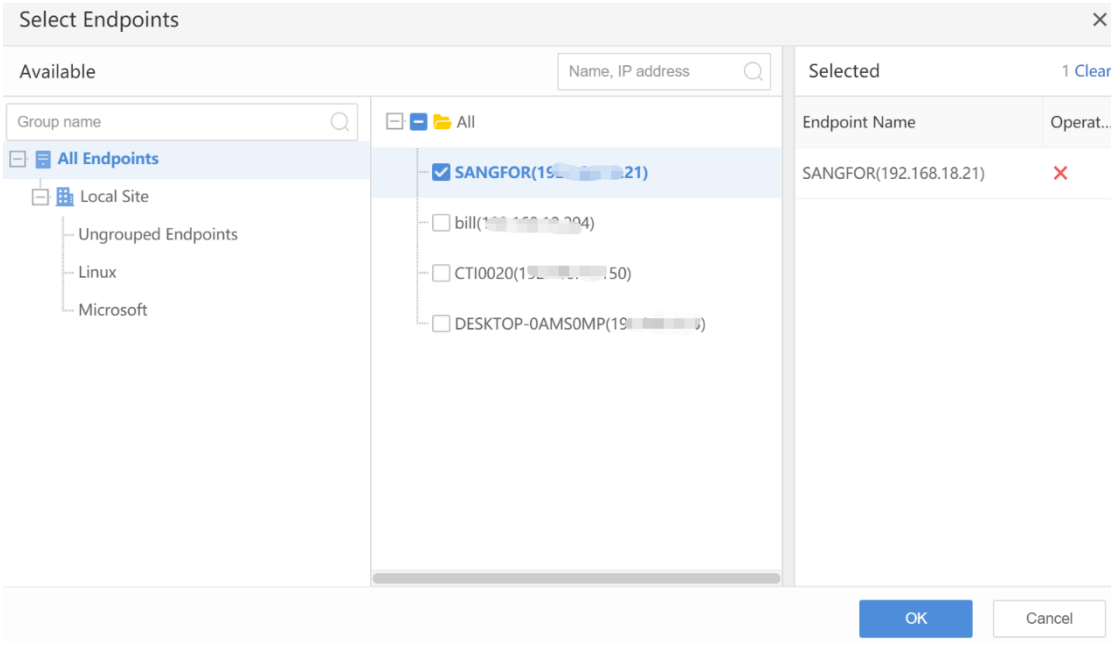


Click Add to create a new business system and add endpoint to the business system.

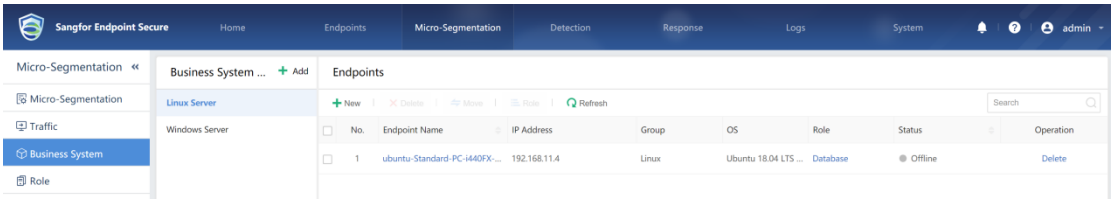


Name: It defines the name of new business system.

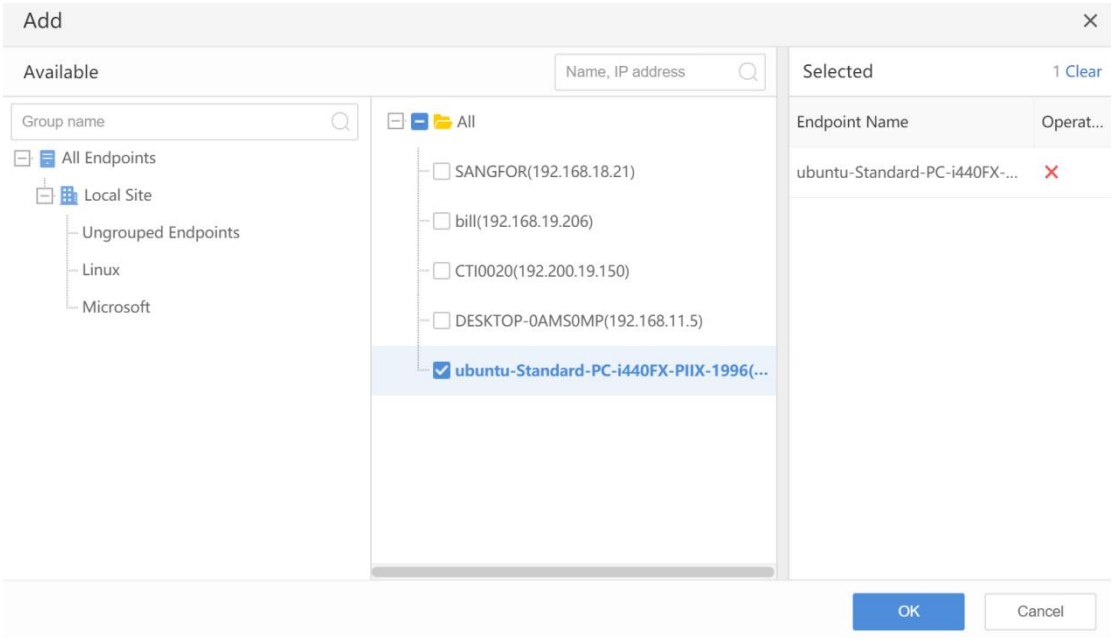
Endpoint: click to select online endpoints, as shown below:



Check the endpoints to be added in the business system, click OK to submit.



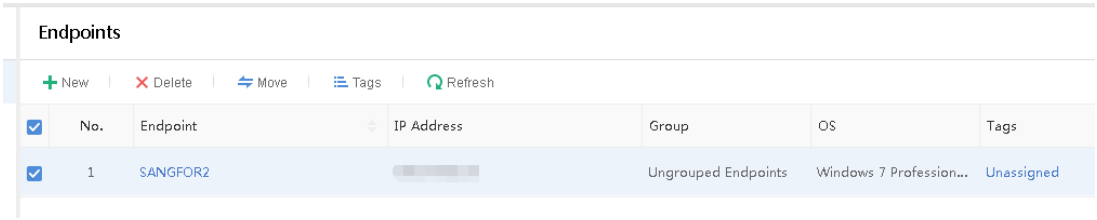
New: Click New in **Endpoints** to add endpoints to business system after business system is configured, as shown below:



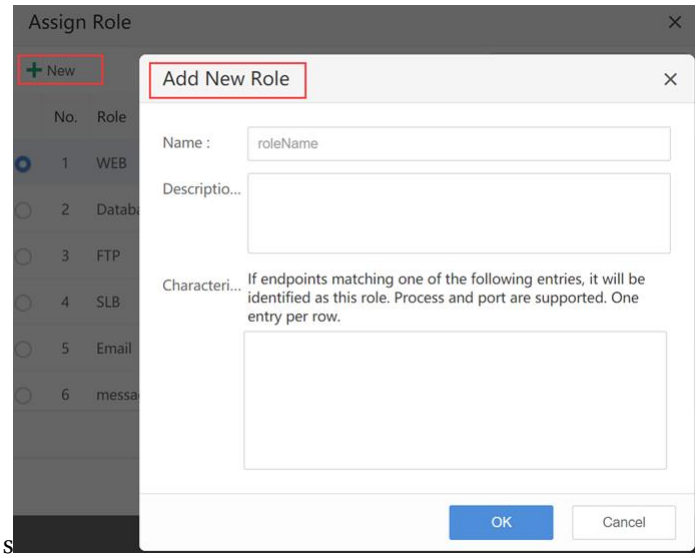
Delete: Click to delete endpoint added to the corresponding business system.

Move: Click to move the selected endpoints to another business system.

Tag: It defines the category of endpoints, such as web, database. The tags can be customized, and only one tag can be assigned to one endpoint. Click Tags to show as below:

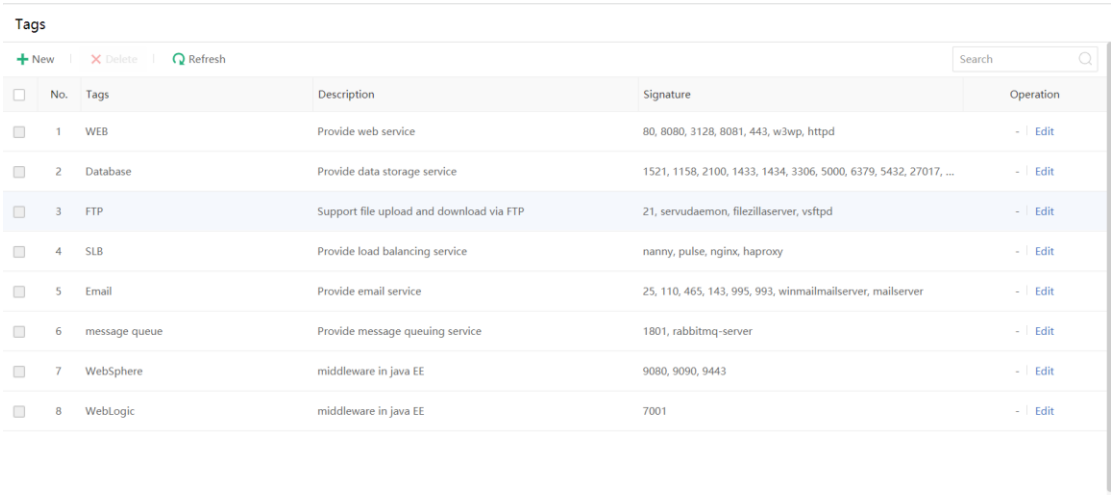


Click New, as shown below. For the detailed description, refer to Section 3.4.4 Role.

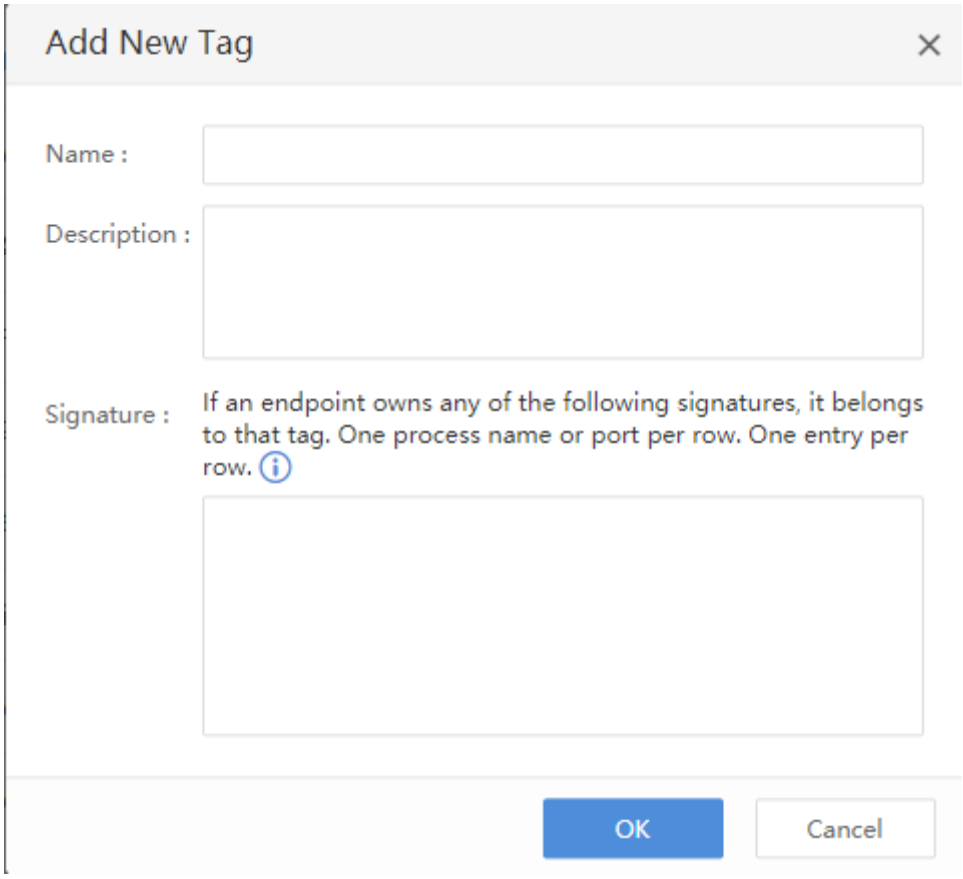


3.4.4 Tags

This is used to define the category (the service provided by endpoint) of endpoints in the business system. The signatures of different tags cannot be the same. There is built-in WEB, Database, FTP, SLB, Email, Message Queue, WebSphere, WebLogic tags with their own signatures in the manager.



Click **New** to add a new tag, as shown below:

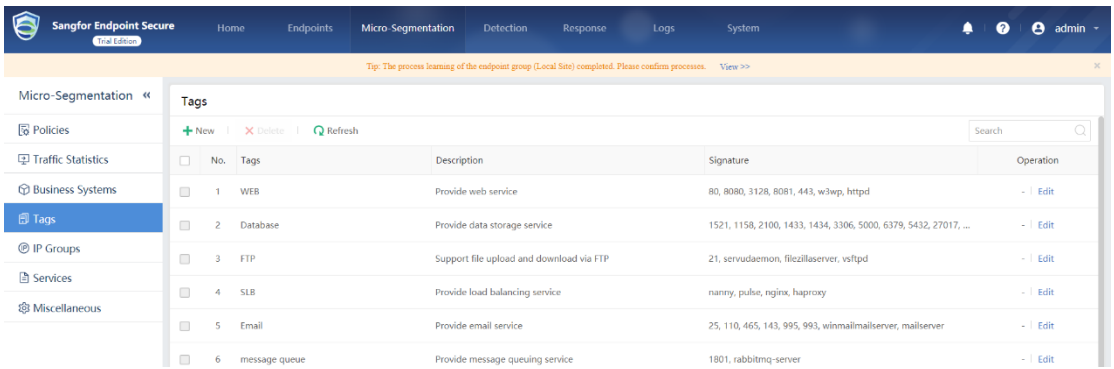


Name: It defines tag name, which is generally the service name provided by the endpoint in the business system.

Description: It describes the category of tags.

Signature: It specifies process or port that will be matched with endpoint. And if endpoint is matched with the signature, it is considered as the tag.

Click OK to submit.



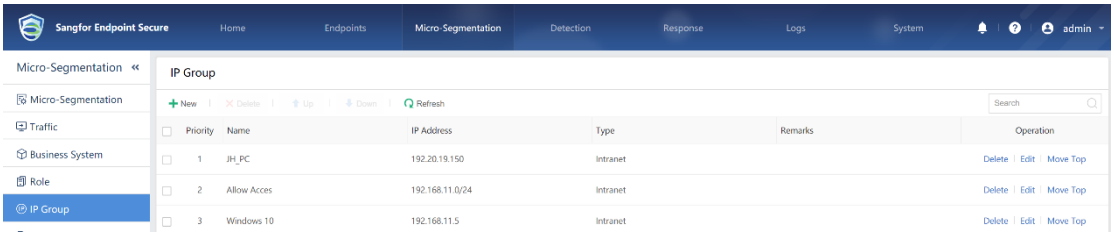
Delete: Click it to delete a customized tag, but the built-in role cannot be deleted.

Operation: The tag signature can be modified. The customized roles can be deleted, and the

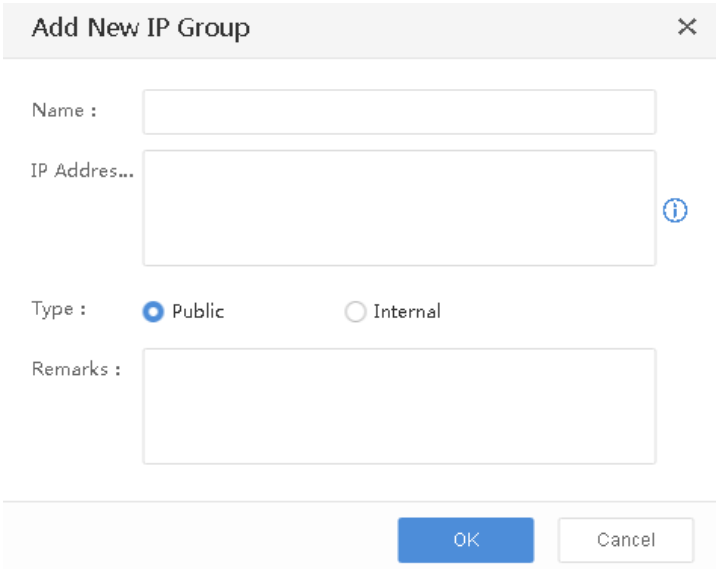
name of customized tag can be modified.

3.4.5 IP Groups

IP Groups: You can assign public or internal IP addresses into different IP groups. The default internal IP addresses in the manager are: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16. The default Public IP addresses in the manager are: 0.0.0.0-255.255.255.255. The micro-segmentation policy matches the IP addresses from top to bottom. The IP addresses are used for micro-segmentation policies.



Click New to add new IP group, as shown below:



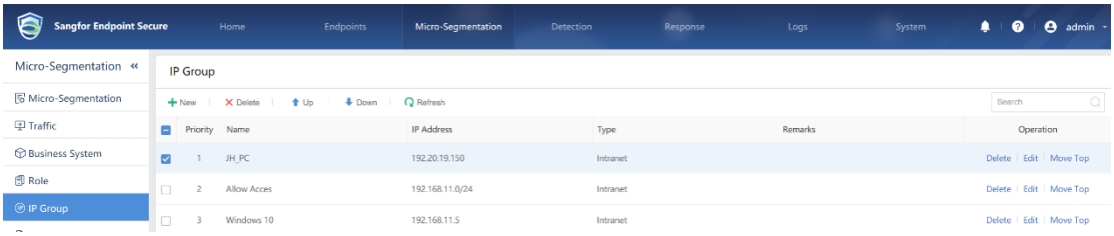
Name: It defines the name of the IP group.

IP Address: It assigns IP address segment into a IP group, and the format is as shown above.

Type: It can be public and internal.

Remarks: It indicates the purpose of the IP group.

Click OK to submit.



Delete： It deletes a customized IP group.

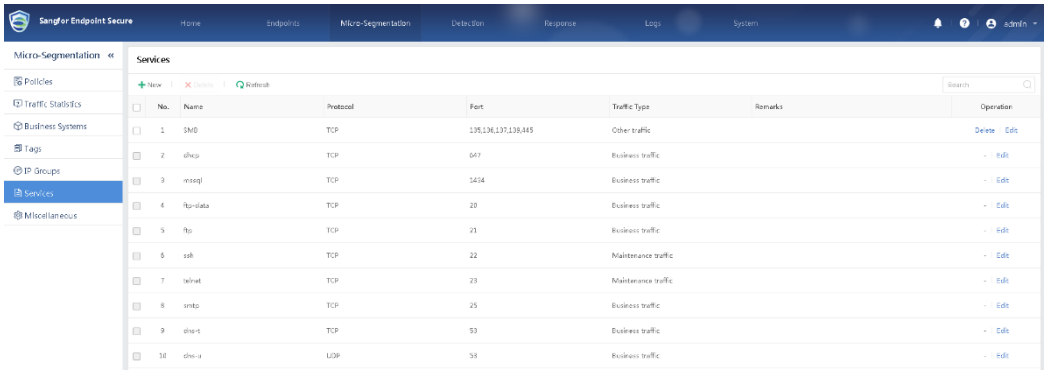
Up: It moves the customized IP groups up. The policy matches the IP address groups from top to bottom. Only one IP group can be selected for one policy.

Down: It moves the customized IP groups down. The policy matches the IP address groups from top to bottom. Only one IP group can be selected for one policy.

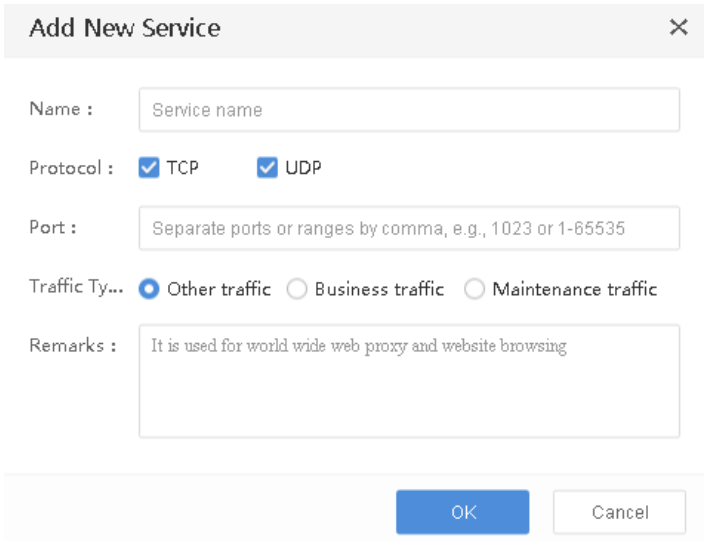
Operation: The IP groups can be deleted, moved up or edited, and cannot be moved down.

3.4.6 Services

Services define the port used in micro-segmentation policy. There are 35 built-in services, and you can also add your own services. The customized service ports cannot be conflicted with the existing ports.



Click New to add a new service, as shown below:



Name: It defines the service name.

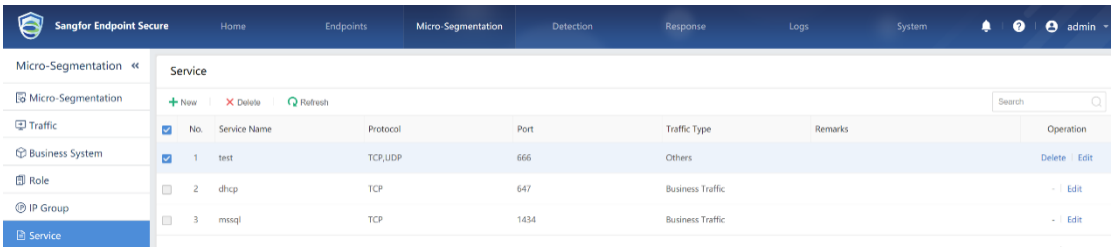
Protocol: It selects a protocol for the service.

Port: It indicates the port used by the service.

Traffic Type: It defines whether the traffic of a service is for business, maintenance or others, and this is displayed in **Traffic Statistics page**.

Remarks: It indicates the purpose of a service.

Click OK to submit.

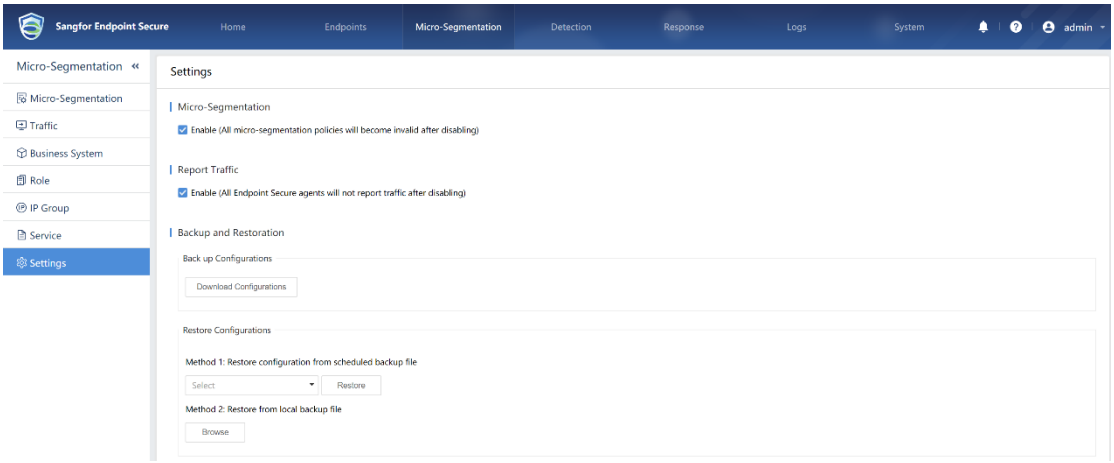


Delete: It deletes a customized service. The built-in services cannot be deleted.

Edit: It deletes or edits a customized service custom service. The built-in service can only be edited and cannot be deleted.

3.4.7 Miscellaneous

Miscellaneous is global settings for micro-segmentation, including enable and disable micro-segmentation, turn on and off traffic report, and back up and restore micro-segmentation policies.



Micro-Segmentation: You can check the option to enable the micro-segmentation function. If it is unchecked, the micro-segmentation policies for all the business systems will be disabled.

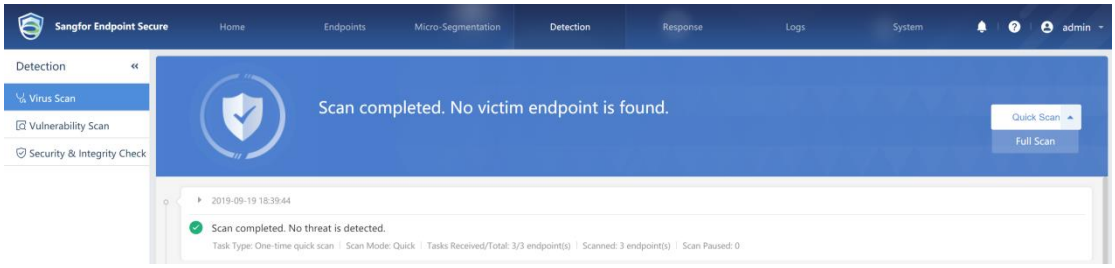
Report Traffic Statistics: You can view traffic access details in Traffic Statistics page when it is enabled**.** After it is disabled, the traffic report will be disabled and affect the display of **Traffic**.

Backup and Restore: It exports the micro-segmentation configuration files and restore from the exported configuration files. The system automatically performs the backup of configuration at 0 o'clock every day.

3.5 Detection

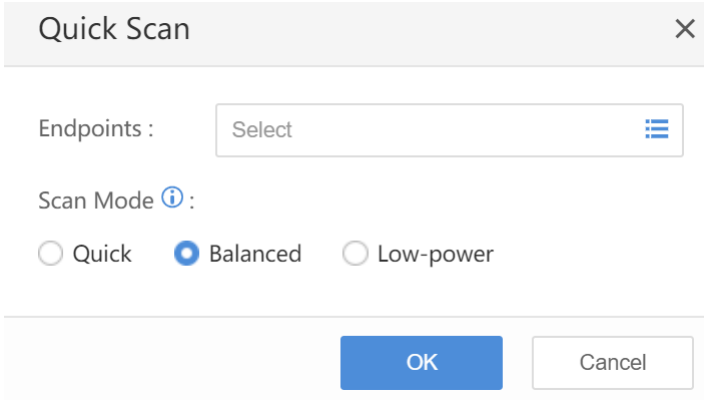
3.5.1 Virus Scan

After the endpoint connects to the Endpoint Secure server, the server will send a task to the endpoint through the **Detection** > **Virus Scan** page. With file reputation database, multiple security engines such (Sangfor Engine Zero, behavioral engine, the signature database and the cloud-based engine, the malicious files can be scanned and the results are displayed then. The major security check results include task type, scan mode, number of endpoints have successfully received, completed, paused scan, endpoint name and IP address, group, operating system, endpoint status, pending/total number of virus files and scan progress.

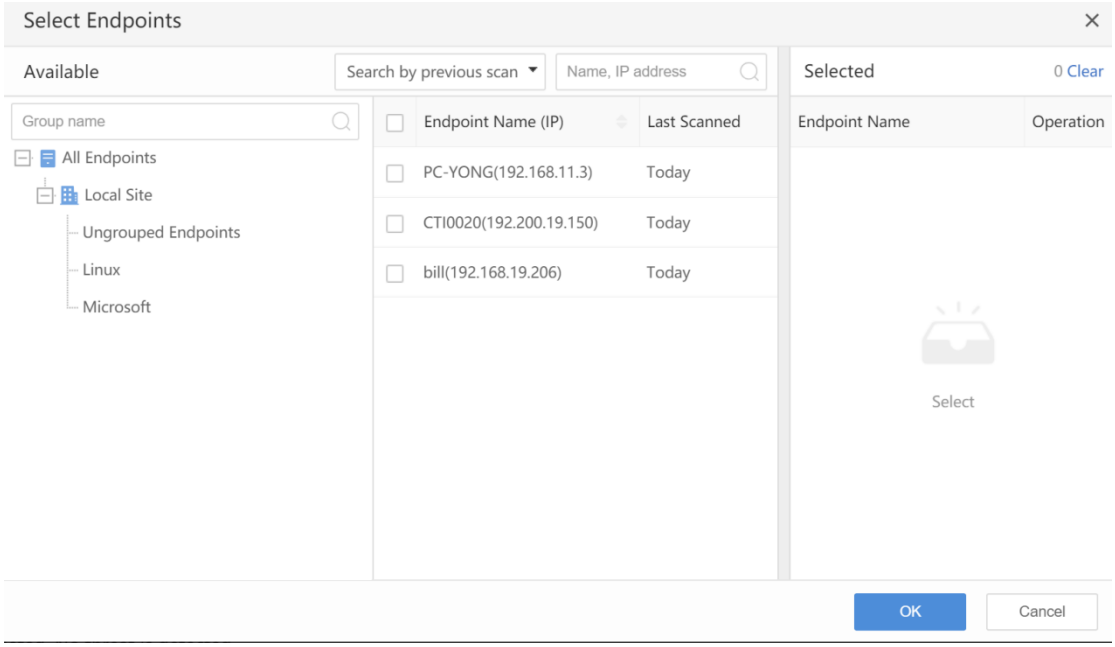


You can choose **Scheduled Scan** or **Quick Scan**. The difference is that Full Scan scans all the hard disk files on endpoint and Quick Scan scans some important file directories in the system disk.

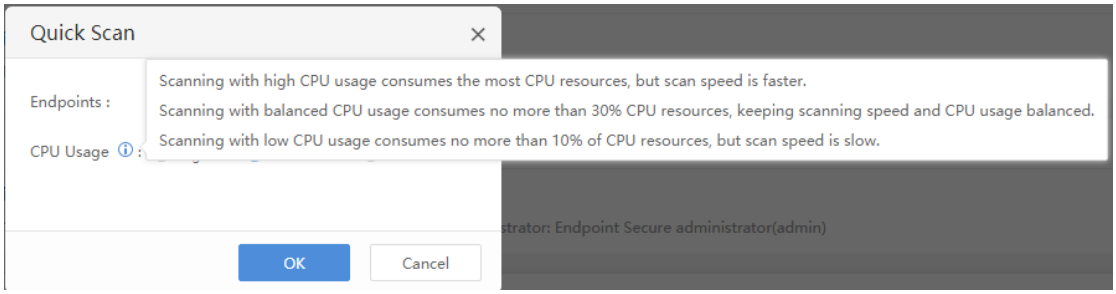
Click Quick Scan, as shown below:



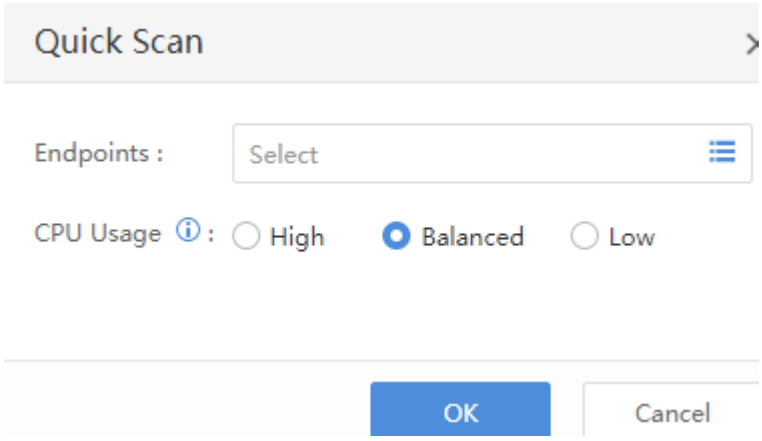
Endpoints are the endpoints that need to perform quick scan. You can view the last scanned time, which allows the administrator to intuitively know which endpoints are not scanned and how long they have not been scanned, as shown below.



CPU Usage includes High, **Balanced**, or **Low**. Click on the icon ⓘ to see the description.

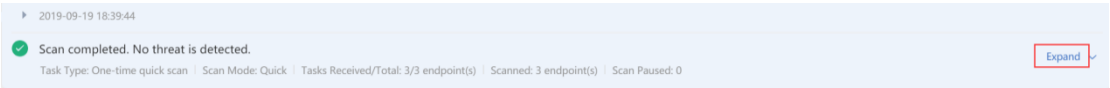


Click Full Scan to go the page, as shown below:

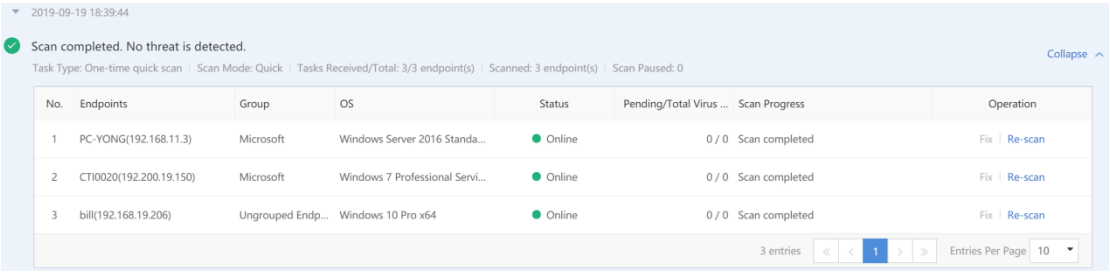


Endpoints are the endpoints that need to perform full scan.

CPU Udage includes High, **Balanced**, or **Low**. The results will be available after the above configuration and the virus removal completes.



Click Expand on the right to view the detailed results.



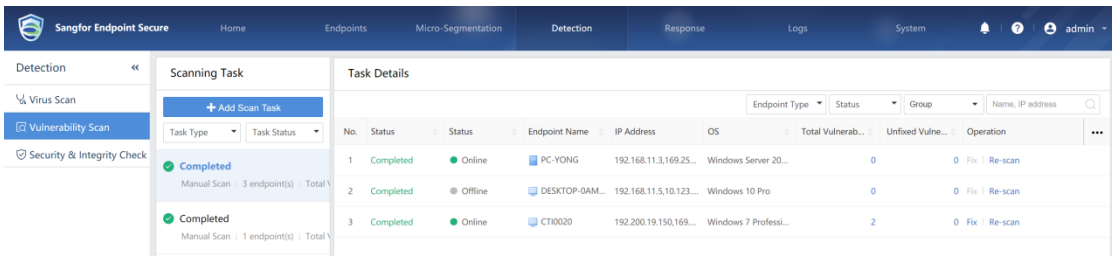
Click Fix to fix virus infected files or click Re-scan.

1. The quick scan directories on Windows computer include: /Windows, /Windows/system32, /Windows/system32/drivers and its subdirectories

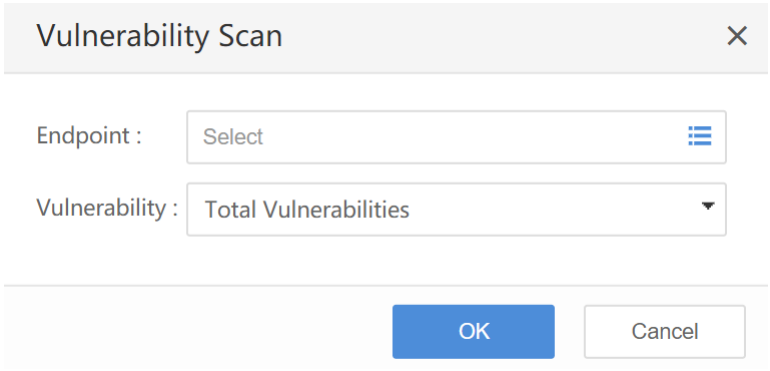
2. The quick scan directories on Linux computer include: /bin, /sbin, /usr/sbin, /usr/bin, /lib, /lib64, /usr/lib/usr/lib64, /usr/local/lib, /usr/local/lib64, /tmp, /var/tmp, /dev, /proc

3.5.2 Vulnerability Scan

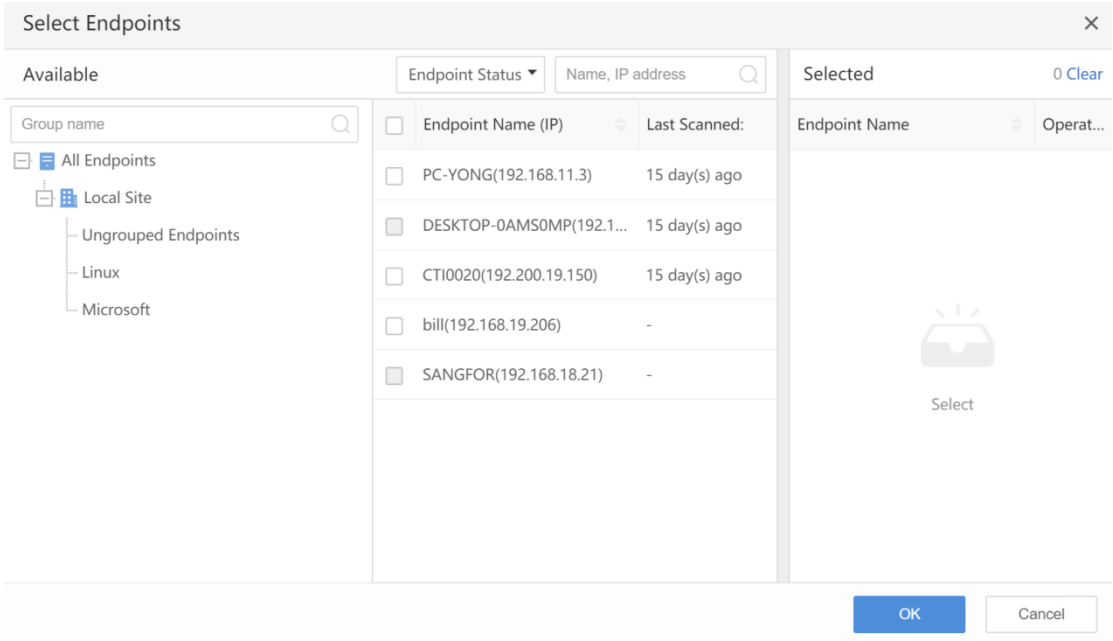
You can detect and patch system vulnerabilities on Windows endpoints through **Detection** > **Vulnerability Scan** page. Currently, it can check and fix five types of vulnerabilities (remote execution, denial of service, privilege elevation, security function bypass, information leakage).



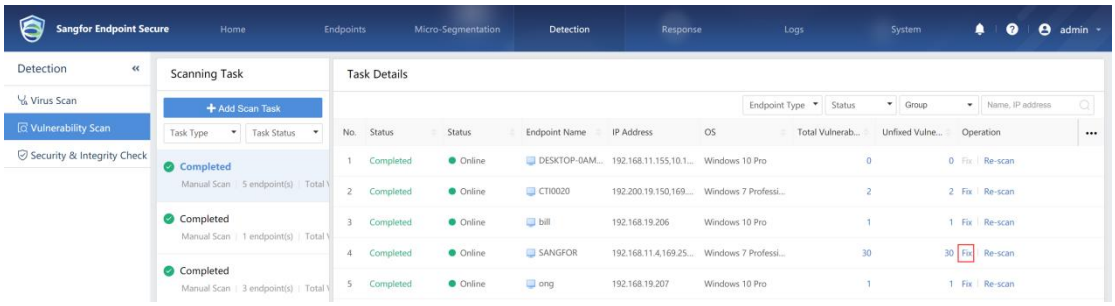
Scan Task: You can add a manual vulnerability scan task and task performing results are showed. Click New Scan Task ,as shown below, to select endpoints for scan and the vulnerabilities to scan for.



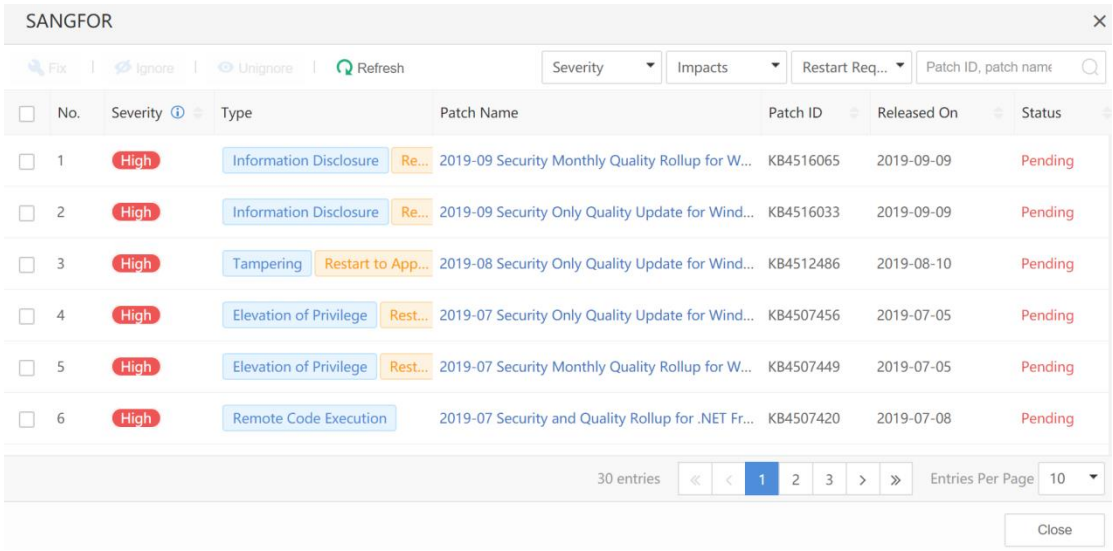
Select endpoints to be scanned for vulnerability, as shown below:



Click a scan task result to view the task details, as shown below. The task details show the scanned endpoints, as well as the total number of vulnerabilities and the vulnerabilities that are not fixed on the endpoints. You can patch the vulnerabilities or re-scan the endpoints.



Click Fix to patch vulnerabilities on endpoints or ignore vulnerabilities, as shown below:



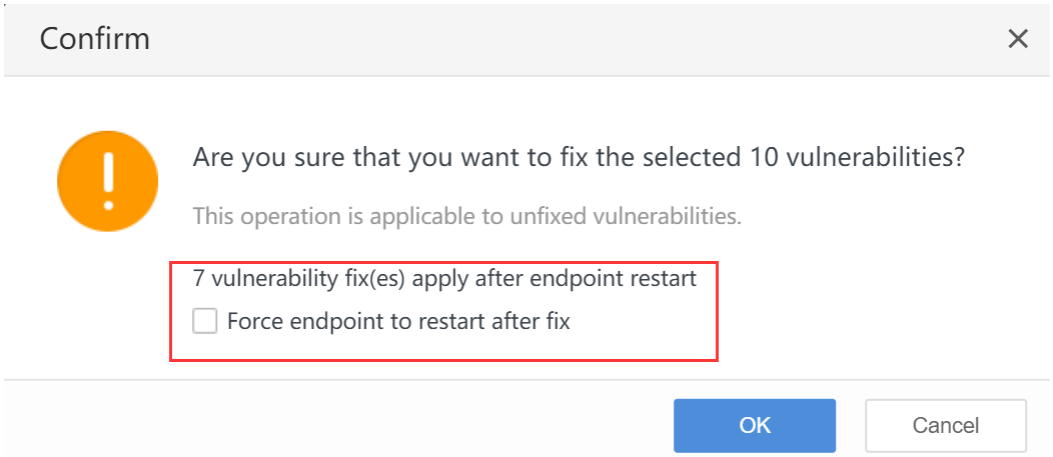
The suggestions for High-threat, Medium-threat and Low-threat vulnerabilities are shown as follows.

High-threat: Immediate fix is recommended because they may be exploited to damage your endpoints

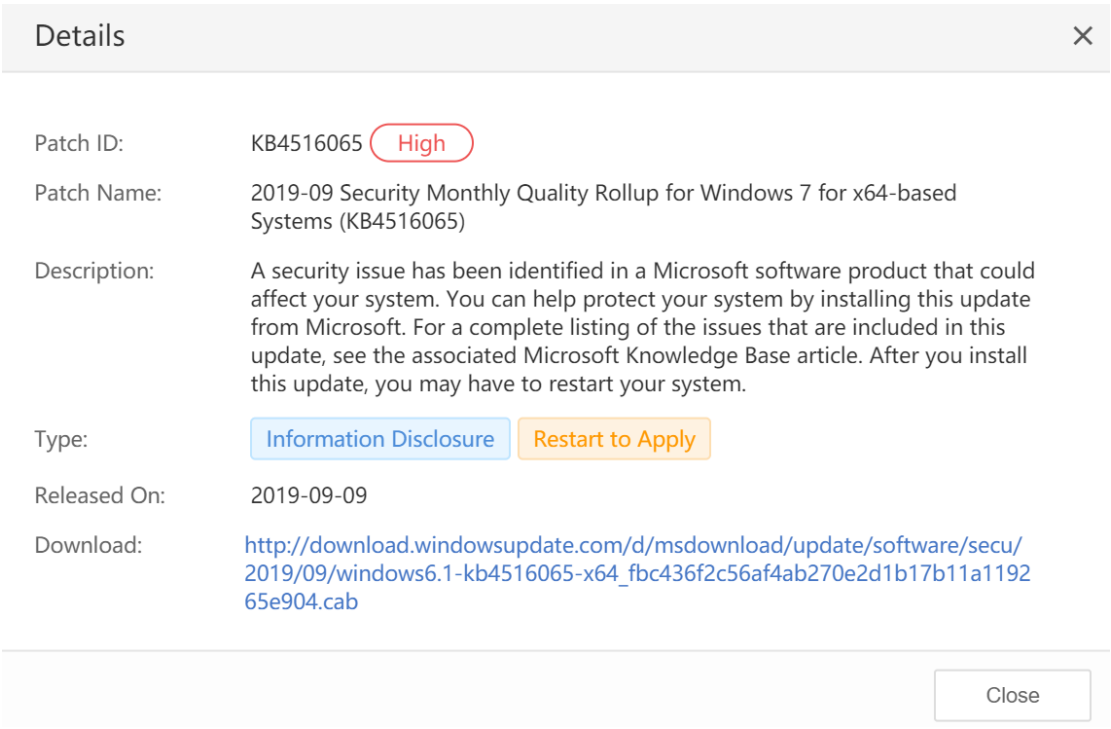
Medium-threat: Analysis and fix are recommended because they can cause risks to your endpoints

Low-threat: Fix as per your need

Select a vulnerability to be fixed and click Fix. The computer is required to be restarted for the vulnerability patch to take effect, and the following prompt will be shown. Administrator can check “Force endpoint to restart after this operation” to enforce endpoint restart or choose to restart the computer later. It is not recommended to check “Force endpoint to restart after this operation” Administrator shall specify that the endpoint restarts during non-business hours for the vulnerability fixing to take effect.



Click the Patch Name of a specific vulnerability to show patch details. The details are helpful to understand the vulnerability risks and the patch download address, as shown below:



The vulnerability patching requires that endpoints have access to the Internet and that the connectivity to the following servers works.

auth.sangfor.com.cn

upd.sangfor.com.cn

download.sangfor.com.cn

analysis.sangfor.com.cn

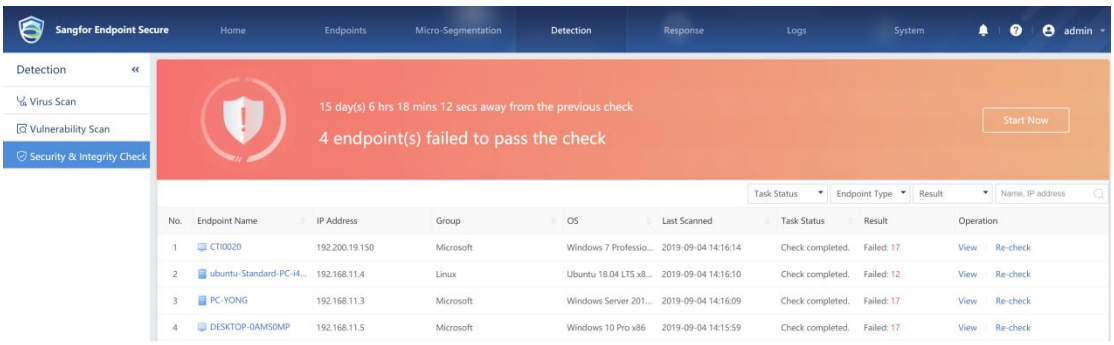
clt.sangfor.com.cn

download.windowsupdate.com

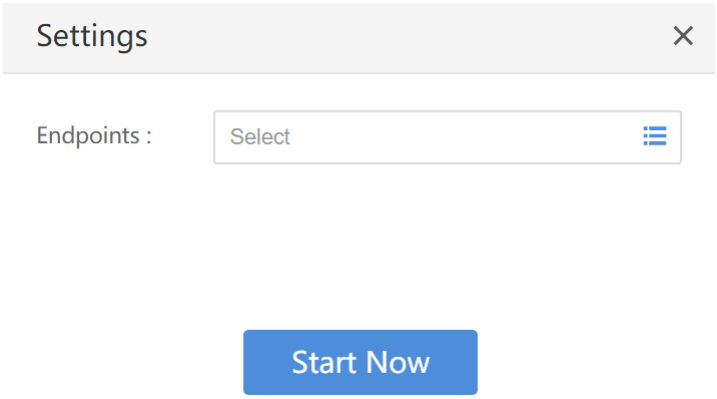
3.5.3 Security & Integrity Check

In Detection > Security & Integrity Check, you may perform integrity checks on endpoints. The check items are different from endpoint to endpoint. The items for Windows endpoints include account, access control, security audit, history information protection,

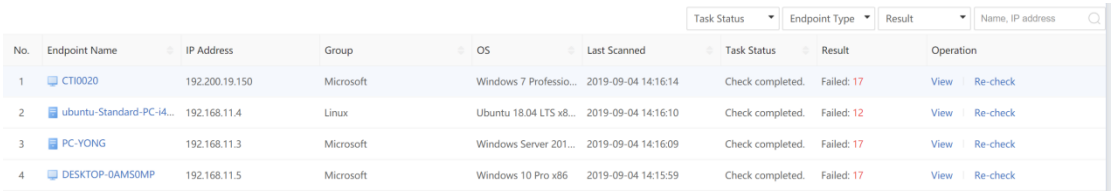
intrusion prevention and malicious code prevention. The check items for Linux endpoints include: account, access control, security audit, SSH policy detection, intrusion prevention and malicious code prevention, as shown below:



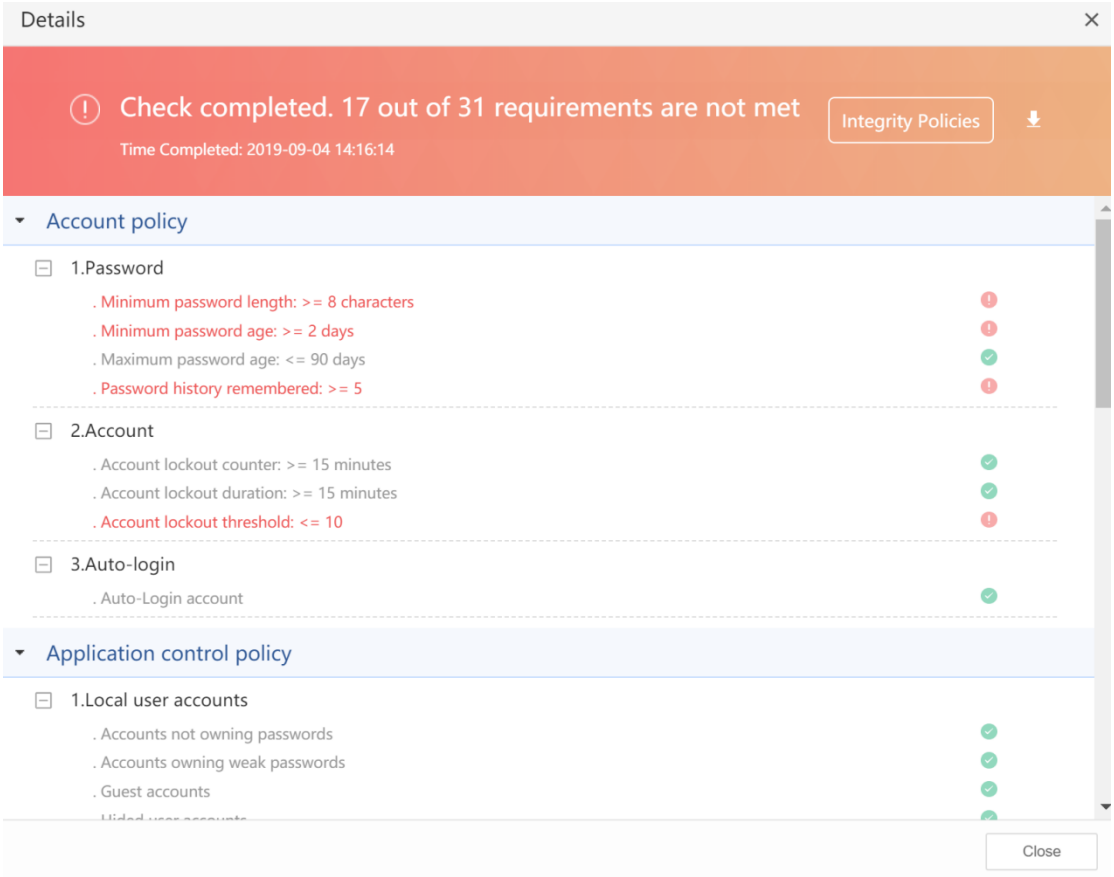
Click Start Now and select the endpoints that need to perform the integrity check to send task, as shown below:



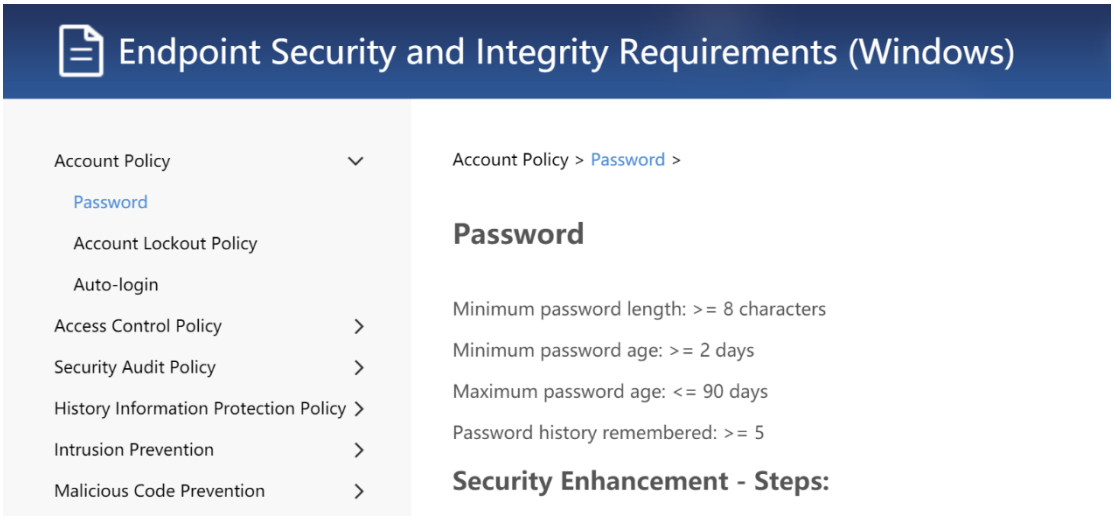
Once the check is completed, you can view the check results:



Click View to view the results of integrity check or each item to view details.



Click Integrity Policies to view the configuration requirements defined for the compliance check.



After client computer is reconfigured according to Integrity Policies, you can click Re-check.

Click  to download the integrity check report.

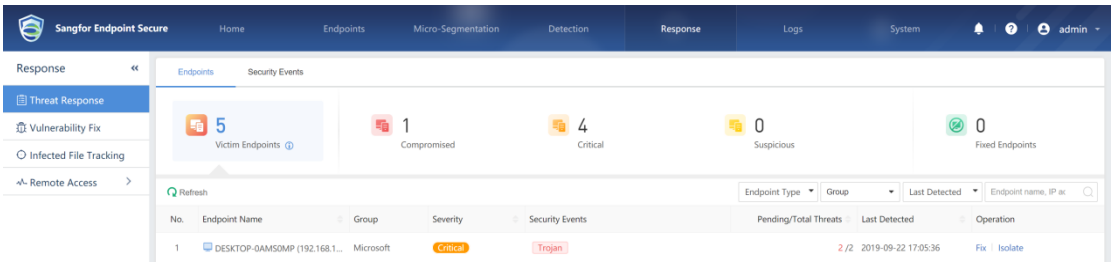
The highlighted integrity check items need specially attention.

3.6 Response

3.6.1 Threat Response

3.6.1.1 Endpoints

You can filter endpoints by threat severity, **All, Compromised, Critical, Suspicious** and **Isolated** endpoints, you may also find specified endpoints by filtering Endpoint **Type, Group, Last Detected** or by directly searching for the endpoint name or IP address.



Endpoint name: The name of the online endpoint.

Group: The group in which the endpoint is included.

Severity: Compromised, Critical and Suspicious. They are defined as follows:

Compromised	It indicates endpoints involved in high-threat viruses, WebShell backdoor or botnet.
Critical	It indicates endpoints involved in moderate-threat virus, botnet and brute-force attacks detected on endpoints.
Suspicious	It indicates endpoints involved in low-threat viruses, WebShell backdoor or botnet.

Security Event: It provides the security event occurred on hosts by tags.

Pending/Total threats: The number of pending threats and the total number of threats found on the endpoint.

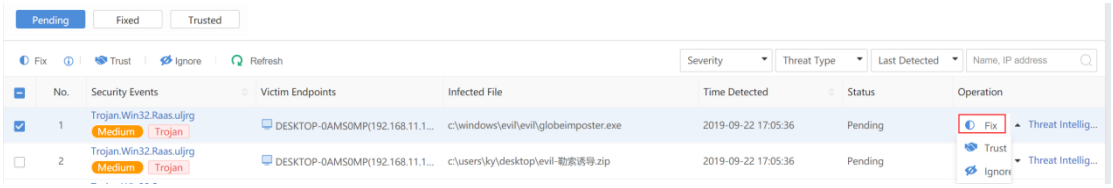
Last Detected: The time when the threat was last detected.

Operation: You can process the discovered threats or directly isolate the endpoint before processing.

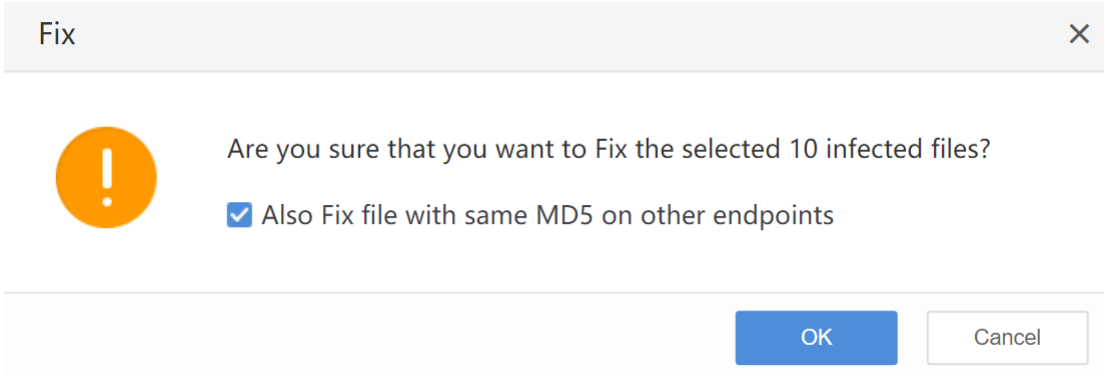
Isolate: After the isolation, the endpoint will not be able to access any network. Please ensure

that the isolation will not affect the business system. The endpoint can be restored from "Isolated".

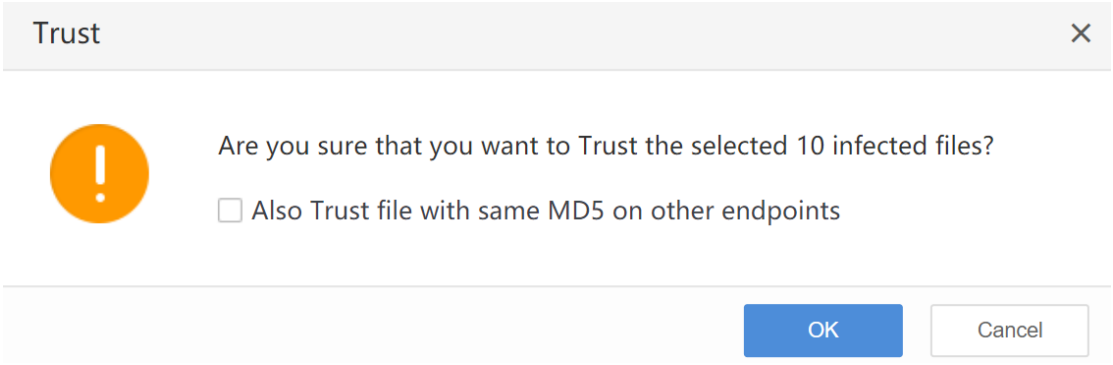
Click Fix to go to the page as shown below:



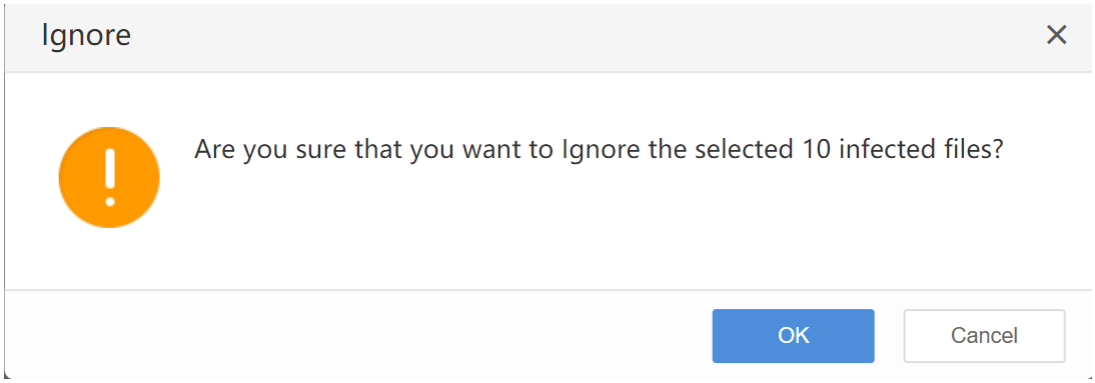
Fix: Select endpoints to be fixed to isolate the virus-infected files and remove macro virus or infectious virus. At least two security events are selected. Blacklisting IP addresses that initiate brute-force attacks in batch is so risky, so blacklisting IP address one by one is recommended, as shown below:



Trust: Select the endpoint security events to be trusted and add the scanned files or Attacker IP addresses to the trusted file list.

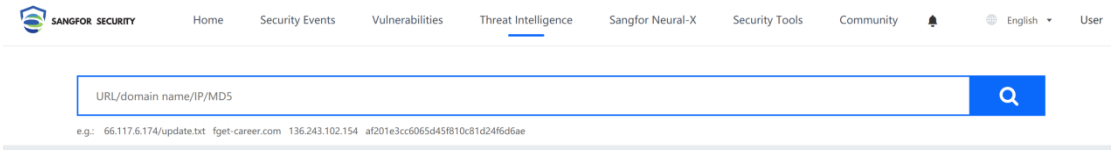


Ignore: Select the endpoint security events to be trusted and ignore the scanned files or attacker IP addresses.



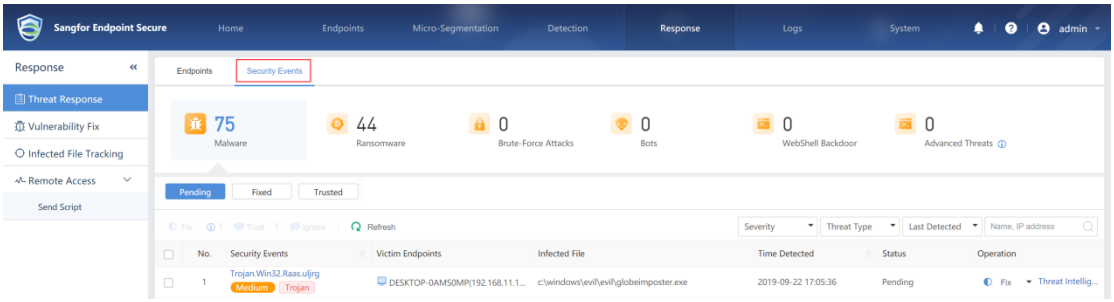
For a single threat, you can **Isolate, Trust, Ignore** or view its **Threat Intelligence**.

Click Threat Intelligence, to go to the **Sangfor Security Center** > **Threat Analysis Platform**.

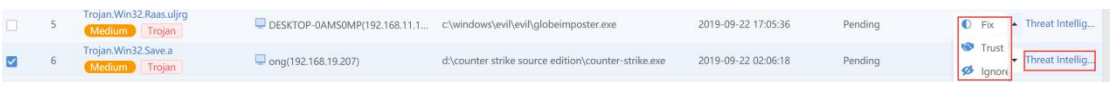


3.6.1.2 Security Events

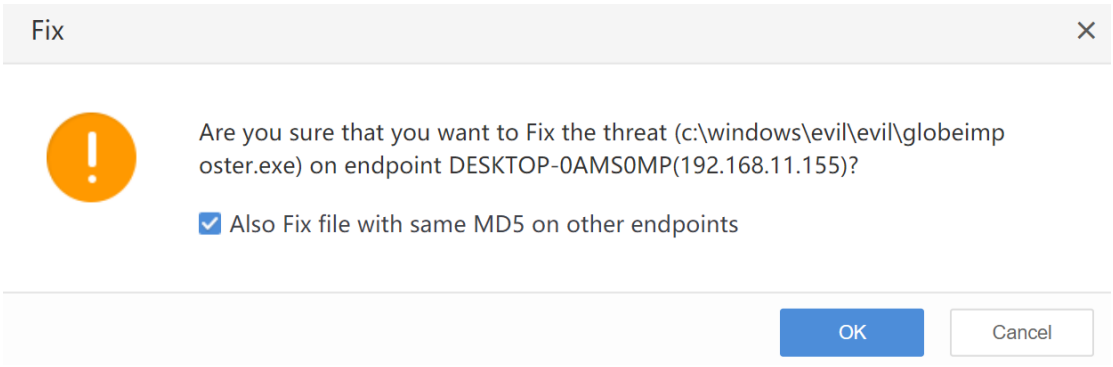
From the perspective of the detected security events, you can filter by **Malware, Ransomware, Brute-Force Attacks, Bots, WebShell Backdoor and Advanced Threats**. Each option can also be filtered by **Pending**, **Fixed** and **Trusted**.



For the malicious files found, choose **Fix, Trust, Ignore** and **Threat Intelligence**, as shown below:

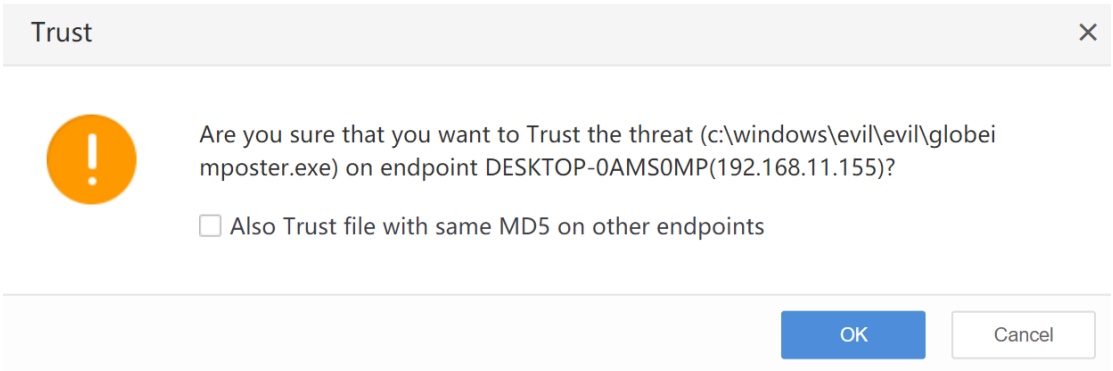


Choose a specific threat file, and click Fix, the following window will pop up.



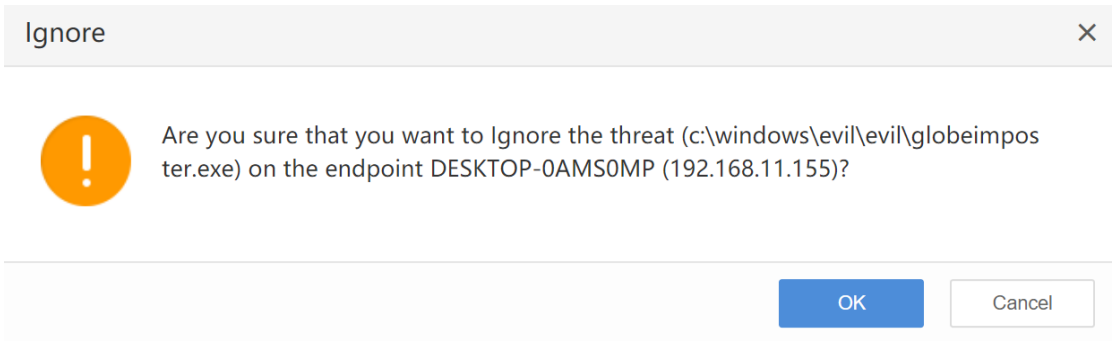
Check "Also Fix file with same MD5 on other endpoints " to perform the batch processing for the same files on other endpoints.

If you select Trust when detected file is confirmed as a false alarm, the following window will pop up.

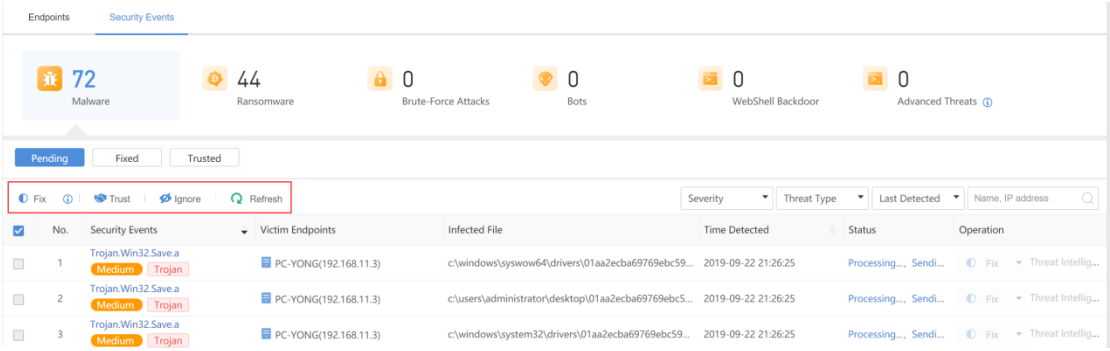


Check "Also Trust file with same MD5 on other endpoints" to perform the batch processing for the same files on other endpoints.

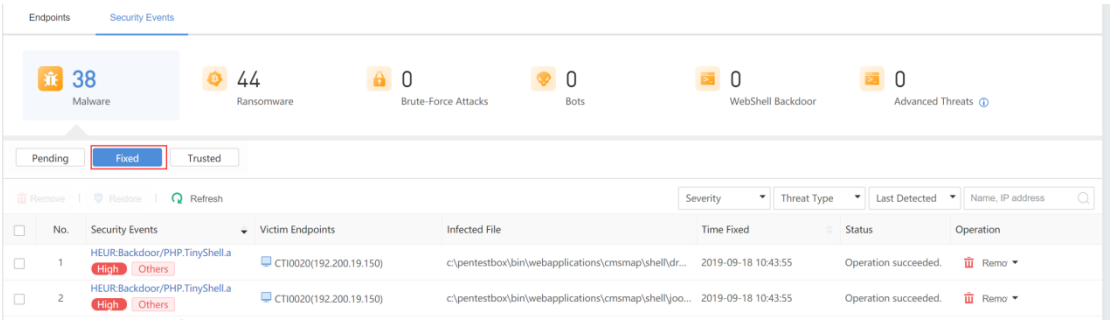
If you select Ignore for threats to be ignored, the following window will pop up, and the manager will no longer display the ignored threats.



You can select multiple threat files and fix them by clicking **Fix**, **Trust** and **Ignore**, as shown below:



Click Fixed to show fixed specific security event, as shown below:



Security Events: The name of detected malicious program.

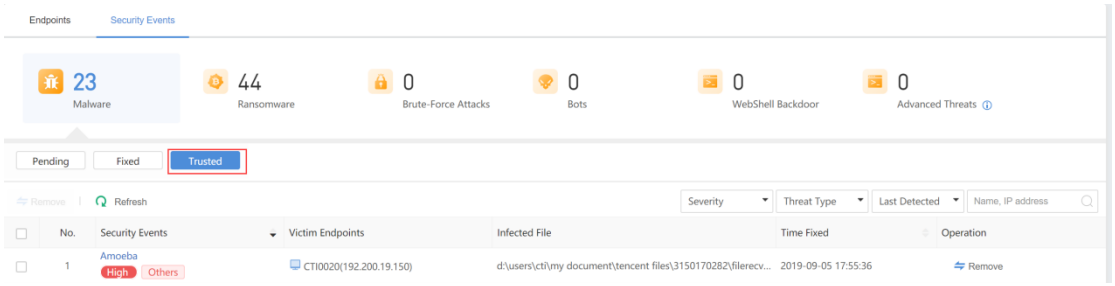
Victim Endpoints: The name of endpoints infected by the virus.

Infected File: The endpoint infected by virus and the path of the corresponding file on the endpoint.

Time Fixed: The time when the event is fixed.

Operation: You can select "**Remove**" when you confirm that the file is a virus infected file, or "**Restore**" when you confirm it is not after manual analysis.

Click Trusted to view the malicious files that that have been added to the trusted file list.



Security Events: The name of detected malicious program.

Victim Endpoints: The name of the endpoint infected by the virus.

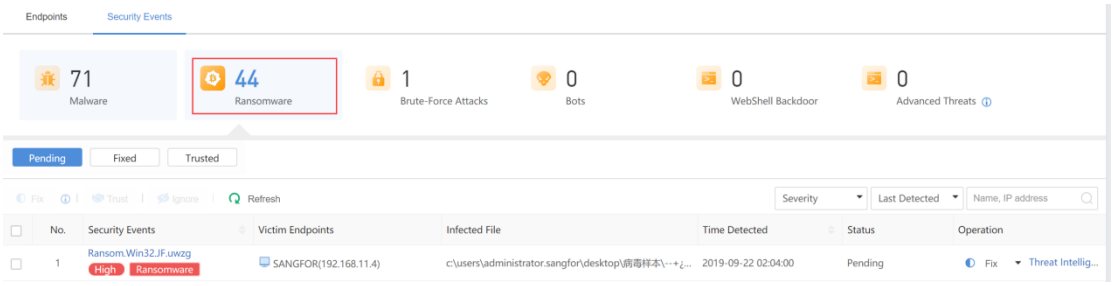
Infected File: The endpoint infected by virus and the path of the corresponding file on the endpoint.

Time Fixed: The time when the event is fixed.

Operation: When the file is confirmed as malicious after manual analysis, it can be removed from the trusted file list.

Click 

to show ransomware attacks.



Security Events: The name of ransomware.

Victim Endpoints: The name of endpoints infected by the virus.

Infected File: The endpoint infected by virus and the path of the corresponding file on the endpoint.

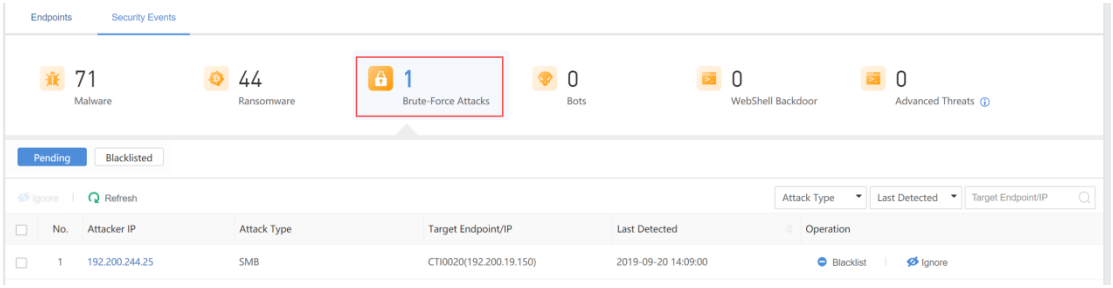
Time Fixed: The time when the event is fixed.

Status;View the current status. It is recommended to fix the threats immediately.

Operation: You can isolate ransomware infected files after confirmation, choose to trust or ignore when it is not malicious, or perform the threat analysis if you are not sure.

Click 

to show brute-force attacks.



Ignore: It allows you to ignore selected security events that are confirmed to be normal service behaviors after manual analysis.

Attacker IP: The source IP address from which the brute-force attack has been initiated.

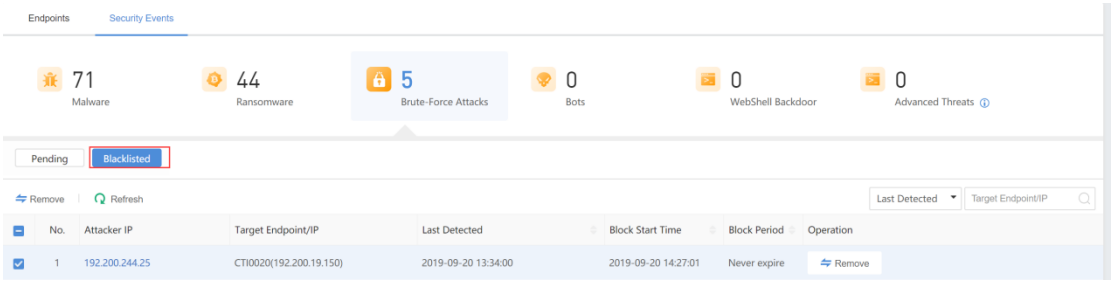
Attack Type: Type of Brute-force attack, such as RDP and SSH.

Target Endpoint/IP: The endpoint that is being attacked.

Last Detected: An attack is generally a continuous action, here shows the time of the latest attack event.

Operation: For a single event, you can blacklist, ignore or perform the threat analysis on attacker IP.

Click Blacklisted to view the IP addresses that have been blacklisted, as shown below:



Remove: For Brute-force attacks that have been confirmed to be false after manual analysis, you can choose to remove the IP addresses from the blacklist to unblock them.

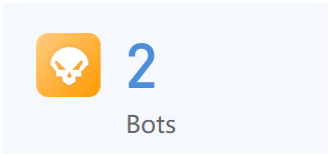
Attacker IP: The source IP address that initiated the Brute-force attack on the host.

Attack Type: Type of Brute-force attack, such as RDP, SMB and SSH.

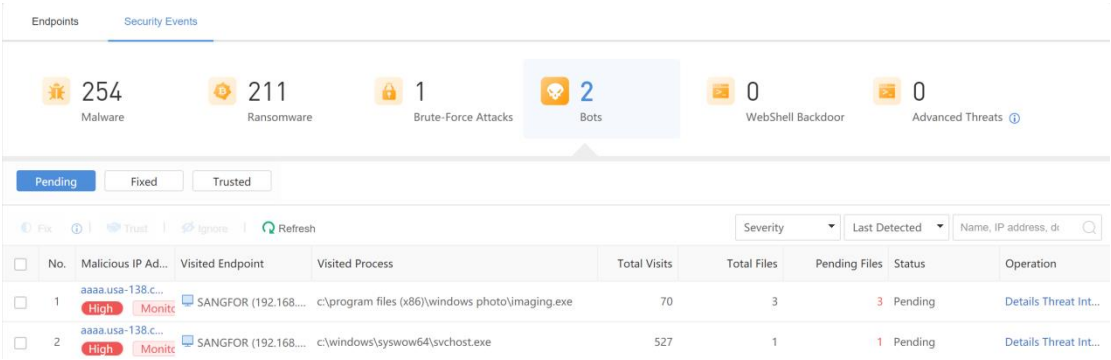
Target Endpoint IP: The endpoint that being attacked.

Last Detected: An attack is generally a continuous action, here shows the time of the latest attack event.

Operation: For a single event, you can blacklist or ignore the attacker IP.

Click 

to show the security events caused by the botnet attacks. By default, display the unfixed bot attacks.



Fix: If processes that access a malicious domain and related files are malicious, select multiple botnet attack events to perform batch fixing for all the processes/related files on all endpoints that access the malicious domain. If it is an infectious virus, first fix it and then perform the disinfection. Quarantine other Trojans directly. View the results or restore in 

.

Trust: If the related files that access a malicious domain name are system files, select multiple botnet events to trust all processes/related files on all endpoints that access the malicious domain name. View the results in 

.

Ignore: Select multiple botnet attack events to ignore all processes/related files on all endpoints accessing the malicious domain. After ignoring, the botnet threat event will not be displayed.

Malicious IP Address: A malicious domain name initiate botnet attack.

Visited Endpoint: The name of endpoint that accesses malicious domain.

Visited Process: The name of process that accesses malicious domain.

Process File Path: The path to the process file that accesses malicious domain.

Total Visits: The number of times the process accessed malicious domain.

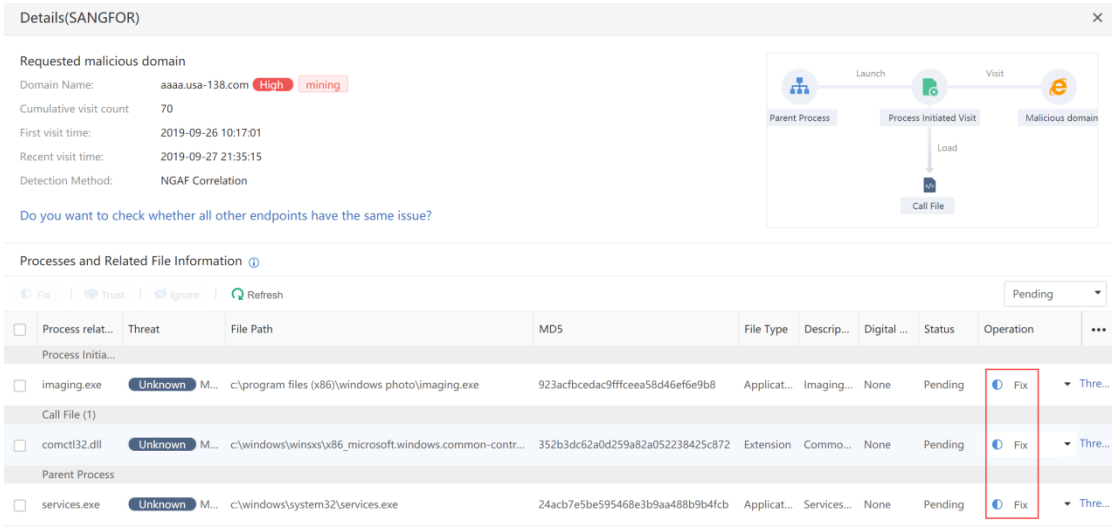
Total Files: Total number of the files related to process that accesses malicious domain.

Pending Files: The number of pending files related to this security event.

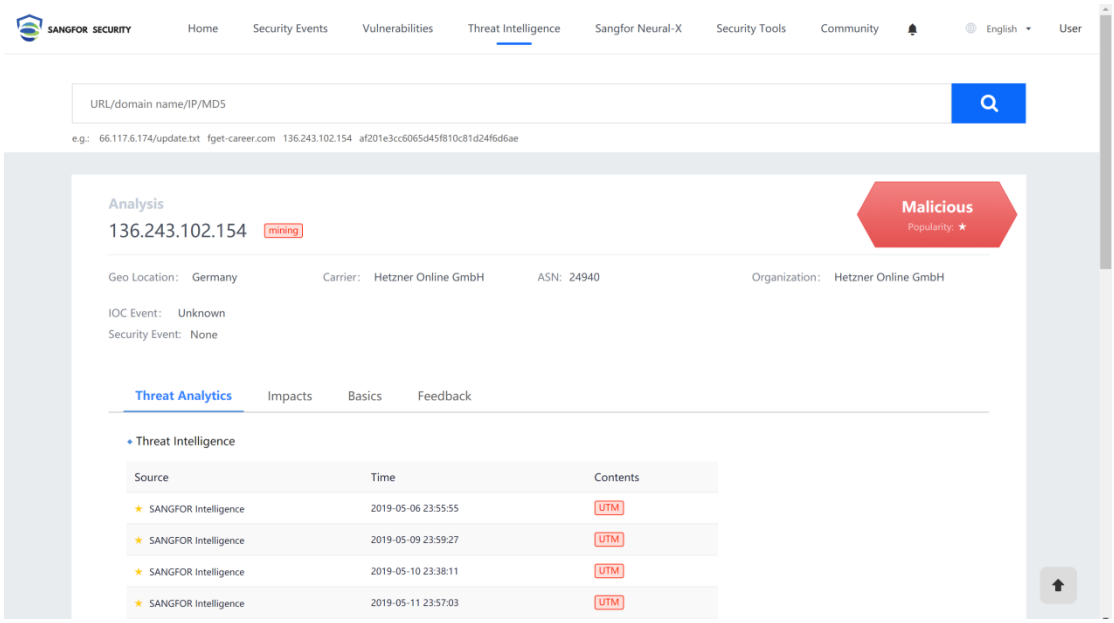
Status: The processing status of all related files, such as Pending, Fixed and Some are pending.

Operation: View the threat details or threat intelligence.

Click Threat Details to view the process accessing the malicious domain on endpoint, and you can **Fix, Trust** or **Ignore** the threat process/related file, as shown below:

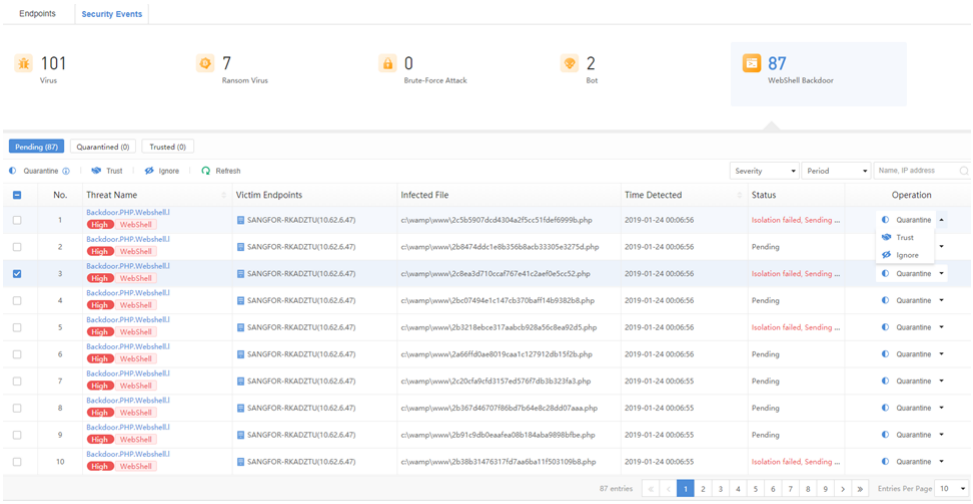


Click Threat Intelligence to connect to the Sangfor Threat Intelligence Center in order to identify the severity of malicious domain, as shown below:



Click 

to show WebShell Backdoor intrusions. The pending WebShell Backdoor intrusions are shown by default.



Threat Name: The name of the WebShell backdoor file detected.

Affected Endpoint: The name of the endpoint where the WebShell backdoor exists.

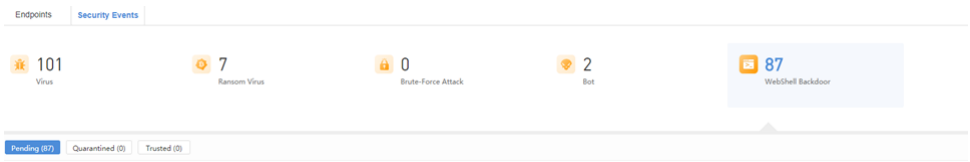
Infected File: The endpoint infected by virus and the path of the corresponding infected file on the endpoint.

Time Detected: The time when the WebShell backdoor is detected.

Status: The current status

Operation: You can choose to **Isolate**, **Trust**, **Ignore** or or perform Threat Analysis.

Click Isolated to further fix the WebShell backdoor.



Remove: Remove two or more WebShell backdoor that are checked.

Restore: For files that have been confirmed to be false by manual analysis or have an impact on the system after isolation, you can restore them.

Threat Name: The name of the WebShell backdoor file detected.

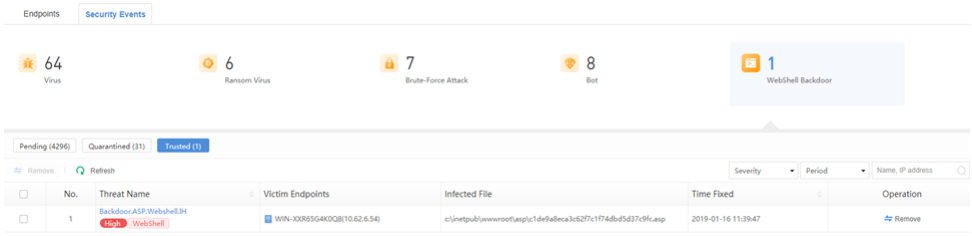
Affected Endpoint: The name of the endpoint where the WebShell backdoor intruded.

Infected File: The endpoint infected by virus and the path of the corresponding infected file on the endpoint.

Time Fixed: The time when the WebShell backdoor is fixed.

Operation: You can choose to "Remove" or "Restore" the current file.

Click Trusted to view the trusted WebShell backdoor intrusions or to perform removal action.



Remove: For files that confirmed to be false after manual analysis or have an impact on the system after isolation, you can remove them from the Trusted file list.

Threat Name: The name of the WebShell backdoor detected.

Affected Endpoint: The name of the endpoint infected by the virus.

Infected File: The endpoint infected by virus and the path of the corresponding infected file on the endpoint.

Time Fixed: The time when the backdoor is detected.

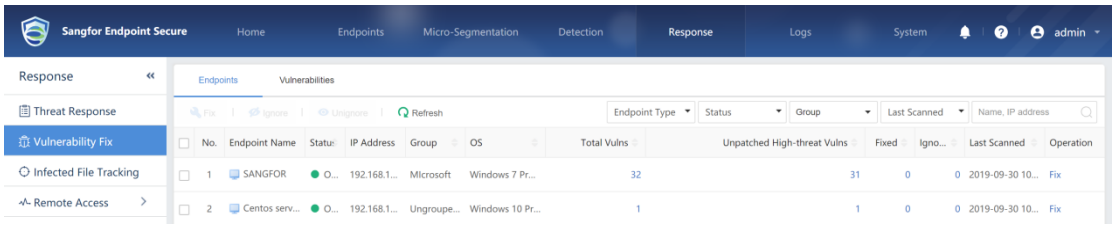
Operation: You can choose to "**Remove**" the current file.

3.6.2 Endpoint Patching

As the response to vulnerability, vulnerabilities can be analyzed and patched from endpoint perspective or vulnerability perspective.

3.6.2.1 Endpoints

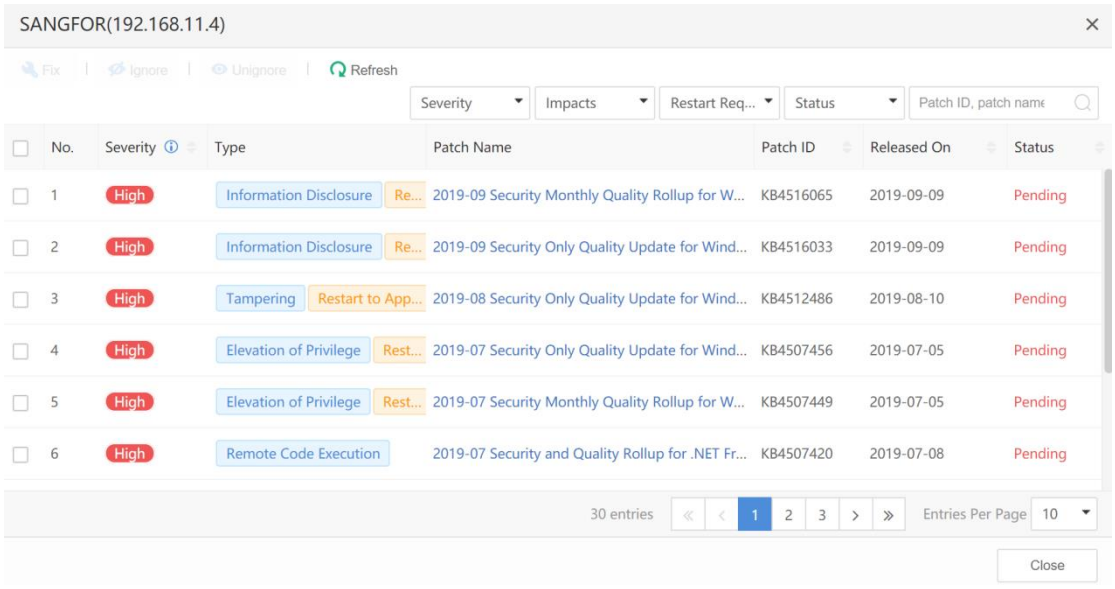
Send vulnerability detection task to endpoints across the network, and complete vulnerability scan. Vulnerability details are shown through **Response** > **Endpoint Patching** > **Endpoints** page, including Total Vulnerabilities, Unpatched High-threat Vulnerabilities, Patched, Ignored, "Last Scanned and Operation, as shown below:



Select multiple endpoints, click Patch to fix vulnerabilities on multiple endpoints.

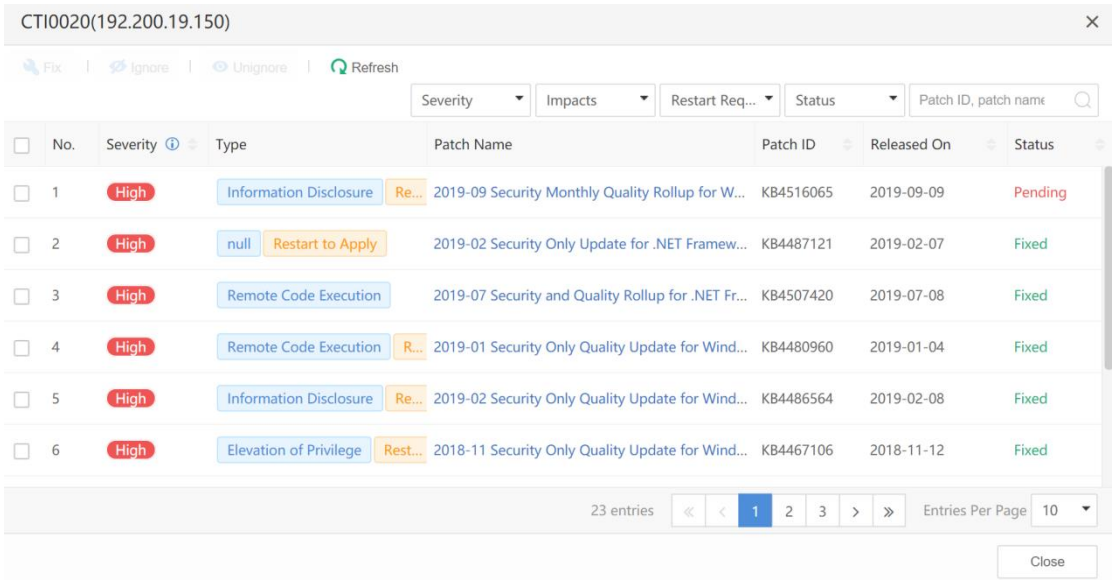
Select multiple endpoints, click Ignore to ignore vulnerabilities on multiple endpoints.

Total Vulnerabilities, Unpatched High-threat Vulnerabilities, Fixed, and Pending list the number of vulnerabilities related to the endpoint. Click the number to show the specific vulnerabilities on the endpoint, as shown below:



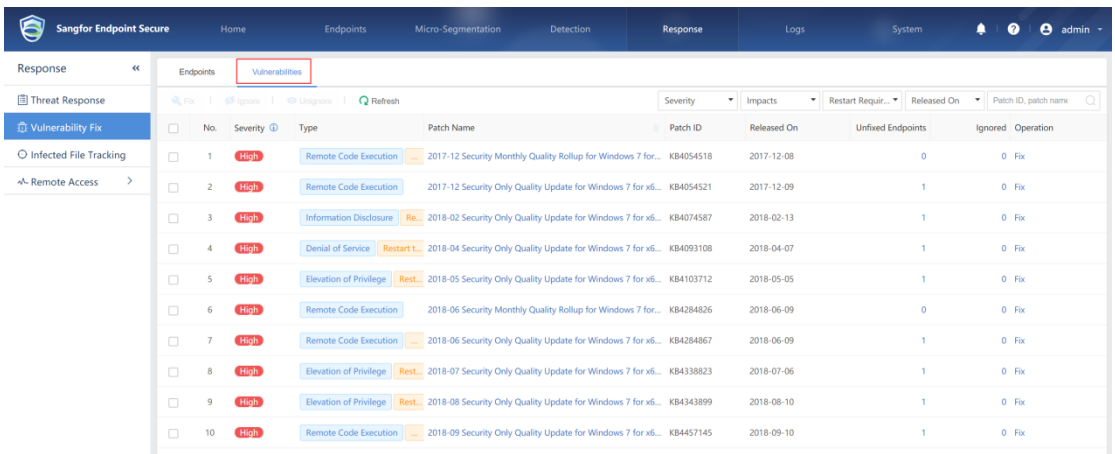
Click Fix to view vulnerability details on specific endpoint and fix vulnerability. The

vulnerability fixing is described in section 3.5.2.



3.6.2.2 Vulnerabilities

Send vulnerability detection task to endpoints across the network, and complete vulnerability scan. Vulnerability details are shown through **Response** > **Endpoint Patching** > **Vulnerabilities** page, including Severity, Patch Type, Patch Name, Patch ID, Unpatched Endpoints and Ignored as shown below:



Severity: There are three types of severity: High, Medium and Low. The suggestions for different severity of vulnerability are as follows:

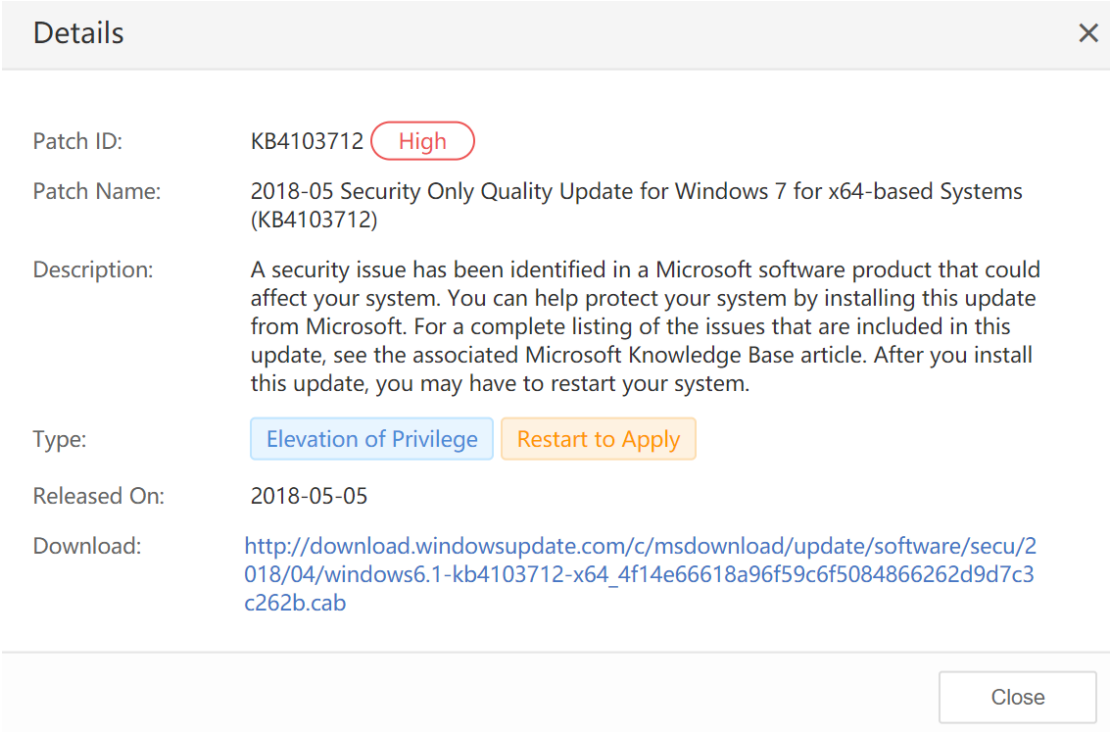
High: Immediate fix is recommended because they may be exploited to damage your endpoints.

Medium: Analysis and fix are recommended because they can cause risks to your endpoints.

Low: Fix as per your need.

Patch Type: The detection and fix functions are currently available for the five vulnerability types: remote execution, denial of service, privilege escalation, bypass of security function, information leakage. If the computer is required to restart for the patch to take effect, the patch type will be followed by a Restart to Apply tag.

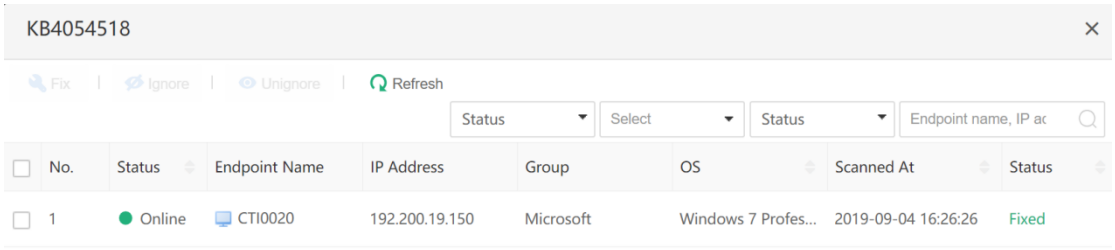
Patch Name: Click the patch name to display the details. From the vulnerability details, you can understand the vulnerability risks and the patch download address, as shown below:



Unpatched Endpoint: The number of endpoints related to this vulnerability and that have not been patched.

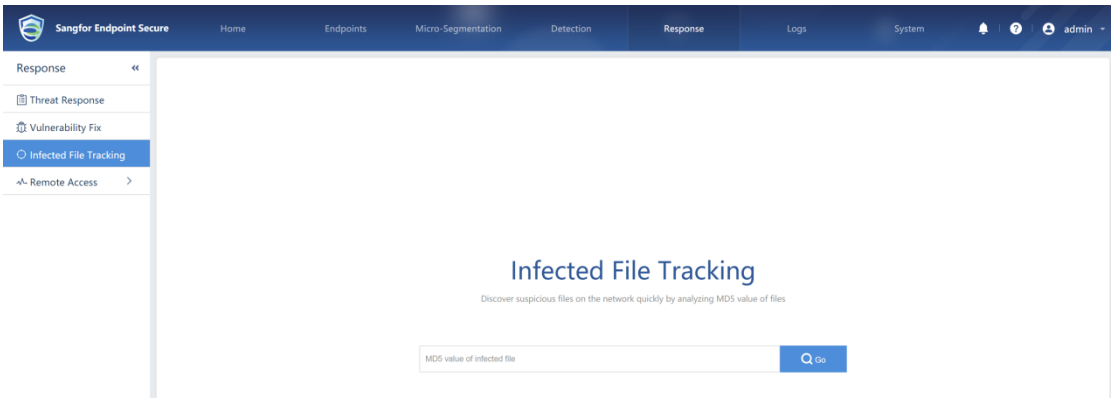
Ignored: The number of endpoints related to this vulnerability and that have been ignored.

Operation: Click Fix to show endpoints related to the vulnerability, as shown below. You can select multiple endpoints to be fixed in batch.

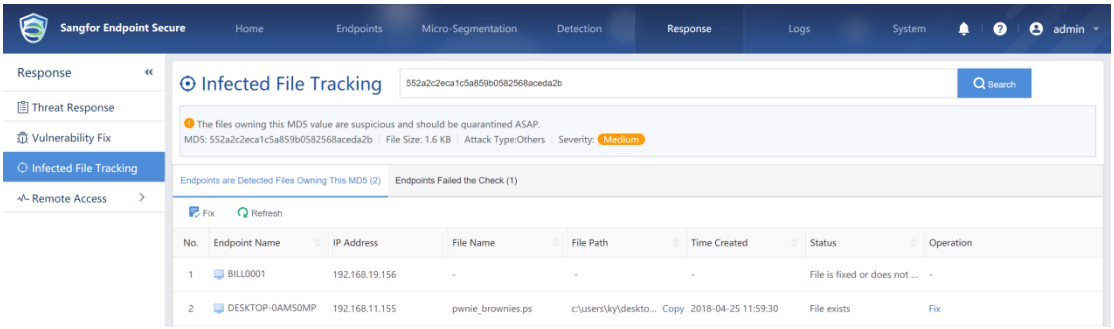

KB4054518
Fix
Ignore
Unignore
Refresh
Status
Select
Status
Endpoint name, IP ac
No.
Status
Endpoint Name
IP Address
Group
OS
Scanned At
Status
1
Online
CTI0020
192.200.19.150
Microsoft
Windows 7 Profes...
2019-09-04 16:26:26
Fixed

3.6.3 Infected File Tracking

Based on malicious file md5 and malicious domain name, the threat location helps users quickly and accurately locate the endpoints infected by the same threat file across network or the endpoints that accesses the same threat domain.



Enter the MD5 value of the threat file into the search field and click the button to go.



Endpoint Name: The name of the endpoint with virus file.

IP Address: The IP address of endpoint

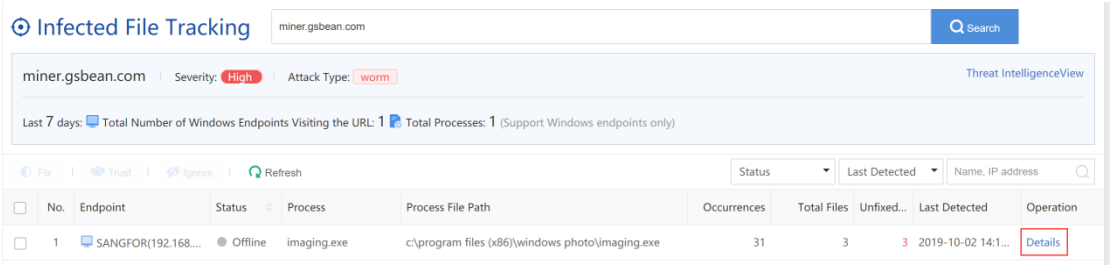
File Name: The file name owning the md5 value

File Path: The path to the virus file on the endpoint

Status: The current status of a file

Operation: Quarantine virus files. Select **Fix** the virus on multiple endpoints.

Enter the threat domain name into the field and click Search button to go.



Endpoint: The name of endpoint that accesses the domain.

Status: Whether the endpoint is online.

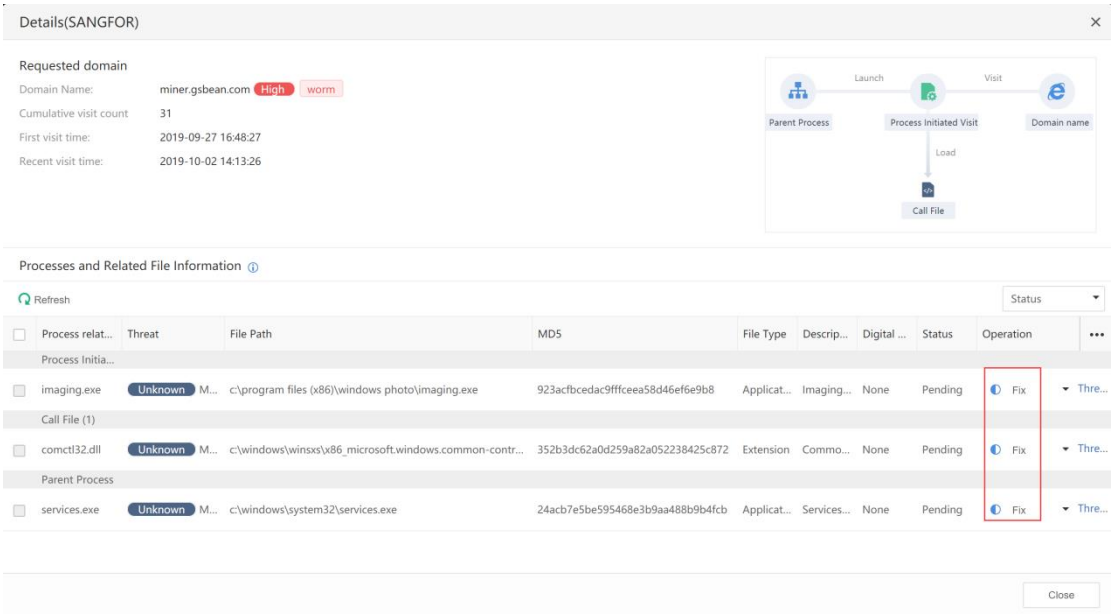
Process: The name of process that accesses the domain.

Process File Path: The path to the process file that accesses the domain.

Occurrences: The number of times the process accessed the domain.

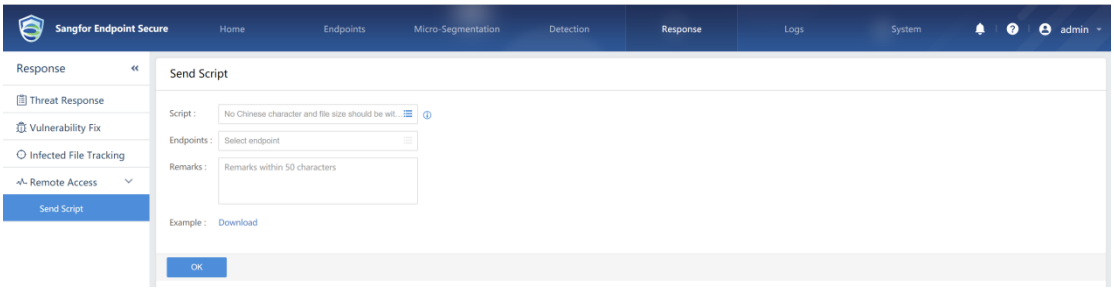
Total files: Total number of the files related to the process that accesses the domain.

Operation: Click Threat Details to view details and the process on endpoints that access the domain. Fix, trust or ignore threat processes/related files, as shown below:



3.6.4 Remote Access

Send Script page supports sending scripts to endpoints and execute them on Linux and Windows endpoints.



Script: Upload the script files to be sent to the endpoints, and its size is no more than 1MB.

Endpoints: It specifies endpoints to be sent the scripts.

Use this function with caution. If the script and its execution on endpoint are undetermined, endpoint will be affected. It is recommended to be used by Sangfor developers.

Script Location:

For Windows: C:\Program Files\Sangfor\EDR\agent\var\abs directory.

For Linux: var/abs.

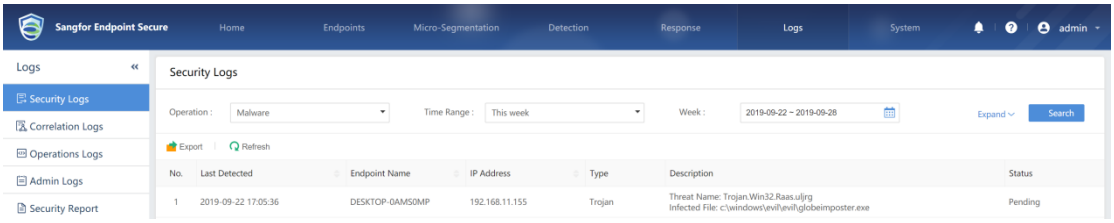
Script sent must be executed to generate the above directory.

3.7 Logs

3.7.1 Security Logs

Retrieve the security logs on the Endpoint Secure server.

Query for **Virus Scan** results. You can search those by day, by week, by month or by specified period. You can also perform an advanced search. Use **Endpoint Name** to filter the endpoints to you want to search. Use IP Address to find the endpoints you want to search, as shown below:



Last Detected: The time the virus was scanned.

Endpoint Name: The endpoint where the virus is found.

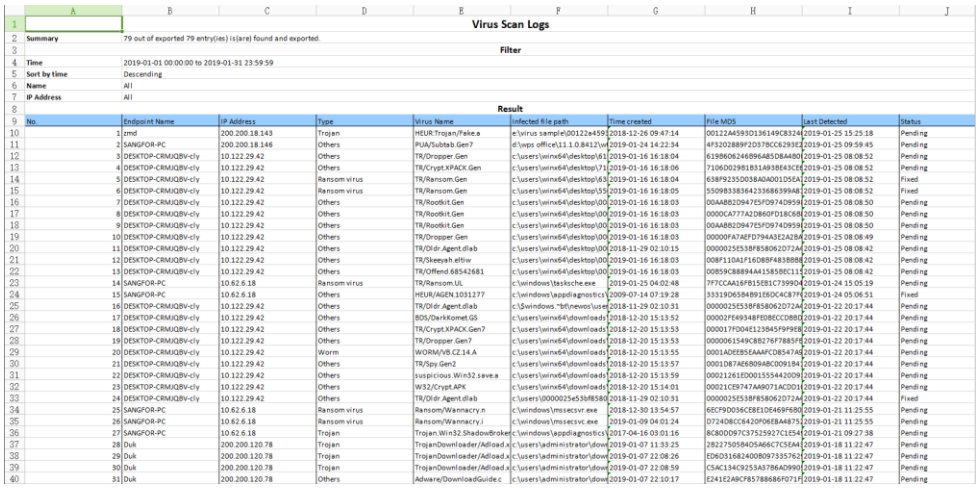
IP Address: The IP address of the endpoint.

Type: The type of virus found.

Description: The name of the virus found and the infected file path on the endpoint

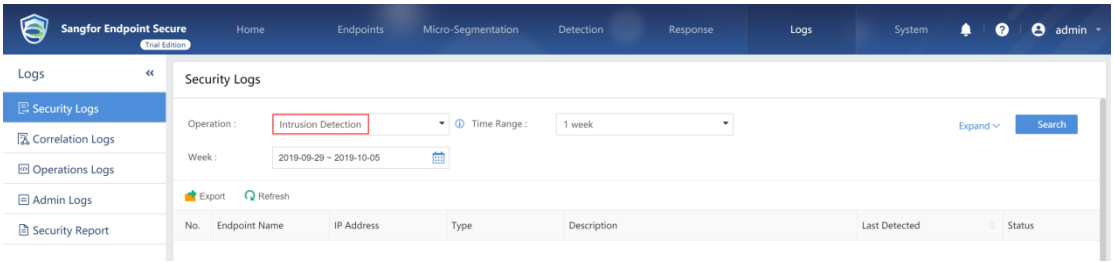
Status: The current status, including pending and Fixed.

Click Export to download an Excel log file. From this file, you can view important information such as the infected file and MD5 value of the file. The security operator can confirm the MD5 value through the third-party threat intelligence Endpoint Secure server.



	A	B	C	D	E	F	G	H	I	J
1					Virus Scan Logs					
2	Summary	79 out of exported 79 entry(ies) is(are) found and exported.								
3					Filter					
4	Time	2019-01-01 00:00:00 to 2019-01-31 23:59:59								
5	Sort by time	Descending								
6	Name	All								
7	IP Address	All								
8					Result					
9	No.	Endpoint Name	IP Address	Type	Virus Name	Infected file path	Time created	File MD5	Last Detected	Status
10	1	zmd	200.200.18.143	Trojan	HEUR:Trojan/Fake.a	e:\virus sample\00122e459	2018-12-26 09:47:14	00122A4593D136149C83240	2019-01-25 15:25:18	Pending
11	2	SANGFOR-PC	200.200.18.146	Others	PUA/Subtab.Gen7	d:\wps office\11.1.0.8412\w	2019-01-24 14:22:34	4F3202889F2037BCC6293E	2019-01-25 09:59:45	Pending
12	3	DESKTOP-CRMJQBV-cly	10.122.29.42	Others	TR/Dropper.Gen	c:\users\winx64\desktop\61	2019-01-16 16:18:04	619860624689 6AB5D8A480	2019-01-25 08:08:52	Pending
13	4	DESKTOP-CRMJQBV-cly	10.122.29.42	Others	TR/Crypt.XPACK.Gen	c:\users\winx64\desktop\71	2019-01-16 16:18:06	7106D029B1831A93BE43CE	2019-01-25 08:08:52	Pending
14	5	DESKTOP-CRMJQBV-cly	10.122.29.42	Ransom virus	TR/Ransom.Gen	c:\users\winx64\desktop\63	2019-01-16 16:18:04	638F92350D38A0A001D5EA	2019-01-25 08:08:52	Fixed
15	6	DESKTOP-CRMJQBV-cly	10.122.29.42	Ransom virus	TR/Ransom.Gen	c:\users\winx64\desktop\55	2019-01-16 16:18:05	5509B338364233686399AB	2019-01-25 08:08:52	Fixed
16	7	DESKTOP-CRMJQBV-cly	10.122.29.42	Others	TR/Rootkit.Gen	c:\users\winx64\desktop\00	2019-01-16 16:18:03	00AAB820947E5F0974D959	2019-01-25 08:08:50	Pending
17	8	DESKTOP-CRMJQBV-cly	10.122.29.42	Others	TR/Rootkit.Gen	c:\users\winx64\desktop\00	2019-01-16 16:18:03	0000CA777A2D860FD1BC6B	2019-01-25 08:08:50	Pending
18	9	DESKTOP-CRMJQBV-cly	10.122.29.42	Others	TR/Rootkit.Gen	c:\users\winx64\desktop\00	2019-01-16 16:18:03	00AAB820947E5F0974D959	2019-01-25 08:08:50	Pending
19	10	DESKTOP-CRMJQBV-cly	10.122.29.42	Others	TR/Dropper.Gen	c:\users\winx64\desktop\00	2019-01-16 16:18:03	00000FA7AEFD794A3E2A28A	2019-01-25 08:08:49	Pending
20	11	DESKTOP-CRMJQBV-cly	10.122.29.42	Others	TR/Oldr.Agent.dlab	c:\users\winx64\desktop\00	2018-11-29 02:10:15	000002SE53BF858062D72A4	2019-01-25 08:08:42	Pending
21	12	DESKTOP-CRMJQBV-cly	10.122.29.42	Others	TR/Skeeyah.eltiw	c:\users\winx64\desktop\00	2019-01-16 16:18:03	008F110A1F16D88F4838888	2019-01-25 08:08:42	Pending
22	13	DESKTOP-CRMJQBV-cly	10.122.29.42	Others	TR/Offend.68542681	c:\users\winx64\desktop\00	2019-01-16 16:18:03	00859C88894A4158580C11	2019-01-25 08:08:42	Pending
23	14	SANGFOR-PC	10.62.6.18	Ransom virus	TR/Ransom.UL	c:\windows\tasksche.exe	2019-01-25 04:02:48	7F7CCAA16F8151E81C7399D4	2019-01-24 15:05:19	Pending
24	15	SANGFOR-PC	10.62.6.18	Others	HEUR/AGEN.1031277	c:\windows\appdiagnostics\	2009-07-14 07:19:28	33319D65B4B91E6DC4C87F	2019-01-24 05:06:51	Fixed
25	16	DESKTOP-CRMJQBV-cly	10.122.29.42	Others	TR/Oldr.Agent.dlab	c:\$windows.~bt\newos\use	2018-11-29 02:10:31	000002SE53BF858062D72A4	2019-01-22 20:17:44	Pending
26	17	DESKTOP-CRMJQBV-cly	10.122.29.42	Others	BDS/DarkKomet.GS	c:\users\winx64\downloads	2018-12-20 15:13:52	00002FE49348FE08ECCD8BD	2019-01-22 20:17:44	Pending
27	18	DESKTOP-CRMJQBV-cly	10.122.29.42	Others	TR/Crypt.XPACK.Gen7	c:\users\winx64\downloads	2018-12-20 15:13:53	000017FD04E123B45F9F9EB	2019-01-22 20:17:44	Pending
28	19	DESKTOP-CRMJQBV-cly	10.122.29.42	Others	TR/Dropper.Gen7	c:\users\winx64\downloads	2018-12-20 15:13:53	000006154 9CBB276F78B5F6	2019-01-22 20:17:44	Pending
29	20	DESKTOP-CRMJQBV-cly	10.122.29.42	Worm	WORM/VB.CZ.14.A	c:\users\winx64\downloads	2018-12-20 15:13:55	0001ADEE85EAAAFCDB547A	2019-01-22 20:17:44	Pending
30	21	DESKTOP-CRMJQBV-cly	10.122.29.42	Others	TR/Spy.Gen2	c:\users\winx64\downloads	2018-12-20 15:13:57	0001D87AE6809ABC0091B4	2019-01-22 20:17:44	Pending
31	22	DESKTOP-CRMJQBV-cly	10.122.29.42	Others	suspicious.Win32.save.a	c:\users\winx64\downloads	2018-12-20 15:13:59	00021261ED0015554420D9	2019-01-22 20:17:44	Pending
32	23	DESKTOP-CRMJQBV-cly	10.122.29.42	Others	W32/Crypt.APK	c:\users\winx64\downloads	2018-12-20 15:14:01	00021CE9747AA9071ACDD1	2019-01-22 20:17:44	Pending
33	24	DESKTOP-CRMJQBV-cly	10.122.29.42	Others	TR/Oldr.Agent.dlab	c:\users\00000225e53bf8580	2018-11-29 02:10:31	000002SE53BF858062D72A4	2019-01-22 20:17:44	Fixed
34	25	SANGFOR-PC	10.62.6.18	Ransom virus	Ransom/Wannacry.n	c:\windows\mssecsvr.exe	2018-12-30 13:54:57	65CF9D036CEBE1D6469F68D	2019-01-21 11:25:55	Pending
35	26	SANGFOR-PC	10.62.6.18	Ransom virus	Ransom/Wannacry.i	c:\windows\mssecsvc.exe	2019-01-09 04:01:24	D724D8CC6420F06E8A4875	2019-01-21 11:25:55	Pending
36	27	SANGFOR-PC	10.62.6.18	Trojan	Trojan.Win32.ShadowBroker	c:\windows\appdiagnostics\	2017-04-16 03:01:16	8C80DD97C37525927C1E54	2019-01-21 09:27:38	Pending
37	28	Duk	200.200.120.78	Trojan	TrojanDownloader/Adload.x	c:\users\administrator\dow	2019-01-07 11:33:25	282275058 4D5A66C7C5E4A1	2019-01-18 11:22:47	Pending
38	29	Duk	200.200.120.78	Trojan	TrojanDownloader/Adload.x	c:\users\administrator\dow	2019-01-07 22:08:26	ED6D31682400809733576 2	2019-01-18 11:22:47	Pending
39	30	Duk	200.200.120.78	Trojan	TrojanDownloader/Adload.x	c:\users\administrator\dow	2019-01-07 22:08:59	C5AC194C9253A3786AD990	2019-01-18 11:22:47	Pending
40	31	Duk	200.200.120.78	Others	Adware/DownloadGuide.c	c:\users\administrator\dow	2019-01-07 22:10:17	E241E2A8CF857888 6F071F	2019-01-18 11:22:47	Pending

Query for **Intrusion Detection** results. You can search those by day, by week, by month or by **Specified** period. It also supports advanced searches for endpoint names and IP addresses, source IP address that initiated the Brute-force attack, as shown in the following figure:



Endpoint Name: The name of the endpoint under intrusion.

IP address: The IP address of the endpoint under intrusion.

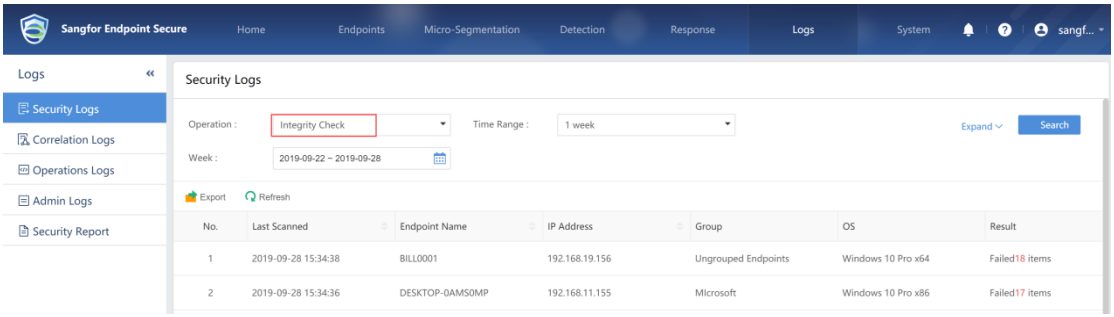
Type: A description of the type of event.

Description: The name of the discovered virus and its location on the endpoint.

Last Detected: The time the intrusion event is detected.

Status: Pending or Fixed.

Query for **Integrity check** results. You can search those by day, by week, by month or by custom. It also supports advanced searches by endpoint names and IP addresses.



Last Scanned: The latest scan time of the endpoint.

Endpoint Name: The endpoint that performs integrity check.

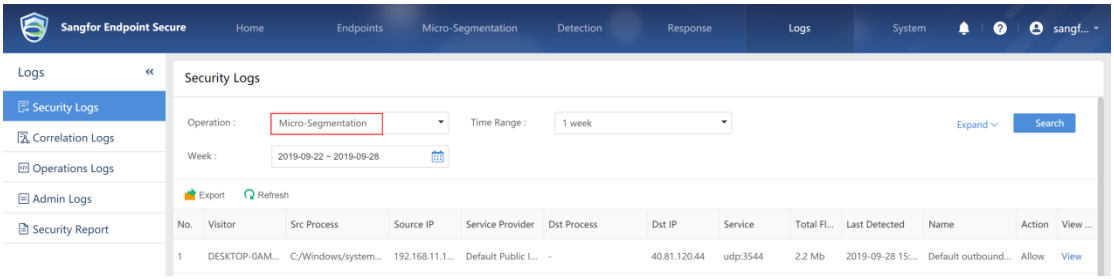
IP Address: The IP address of the endpoint.

Group: The group that the endpoint belongs to.

OS: The operating system information of the endpoint.

Result: An overview of the results of the integrity check.

The results of **Micro-Segmentation** can be searched by day, by week, by month, or by custom. The advanced searches for visitors, service providers, services, IPs, processes and access actions are also available.



Visitor: The originator of access request.

Src process: The requested process by access.

Service Provider: The provider of service accessed by visitor.

Dst Process: The process used by targeted service.

Dst IP: The IP address of service provider.

Services: The accessed service.

Total Flow Size: Traffic statistics for accesses.

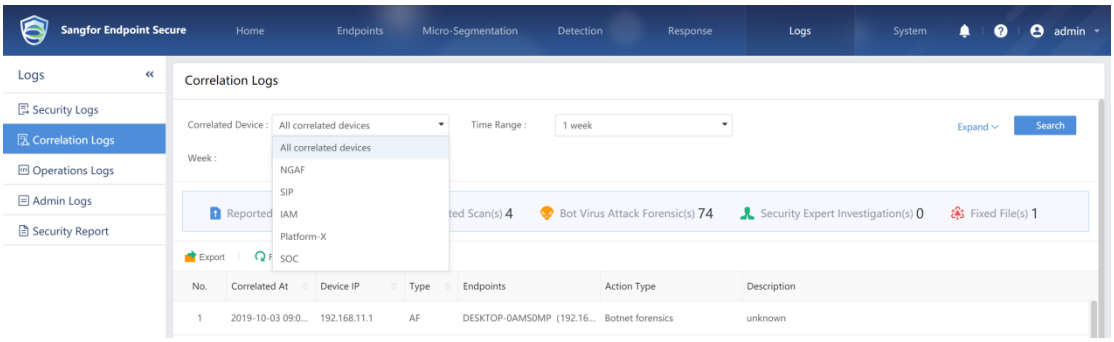
Last Detected: The latest time recorded in the log.

Name: The name of policy that matches the access.

Action: The operation that initiated the access is allowed or denied.

3.7.2 Correlation Logs

View logs that Endpoint Secure correlates to other security products.



Correlation Time: The time when correlation occurred.

Device IP: The IP address of device to be correlated to Endpoint Secure.

Device Type: The type of device to be correlated to Endpoint Secure.

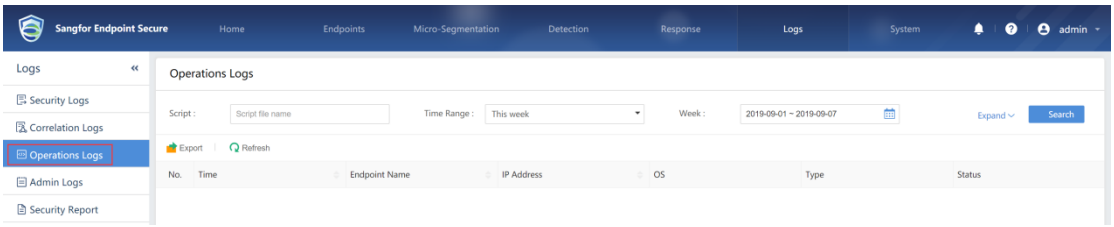
Endpoints: Endpoints that receive correlated policies from correlated policy.

Action Type: The Type of actions correlated device perform.

Description: Correlation details.

3.7.3 Operations Logs

Recorded operation and maintenance log entries when performing the remote operation and maintenance. Advanced search can be performed by period, endpoint name, IP address, script file name and execution status.



Time: The time when the operation and maintenance script was sent.

Endpoint: The endpoint where the script is executed.

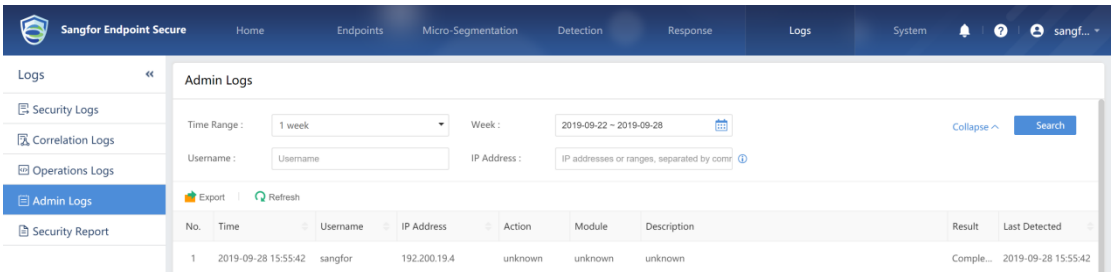
IP Address: The IP address of endpoint.

OS: Operating system information.

Type: The type of sent script.

3.7.4 Admin Logs

Query for the admin logs, which can be used to analyze whether there is any improper operation.

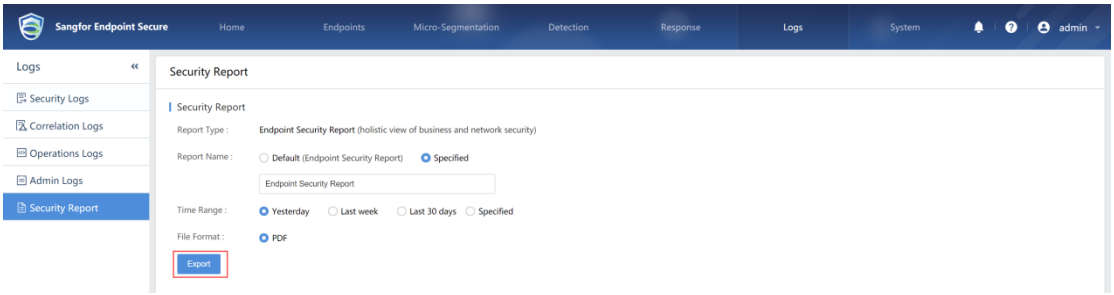


Username: The administrator who logged in to the Endpoint Secure server.
IP Address: The IP address from which administrator logged in.
Action: Classify the operation performed.
Module: The object on which the operation is performed.
Description: Description of the operation content.
Result: It indicates whether the operation was completed.
Last Detected: The time when the operation is performed.

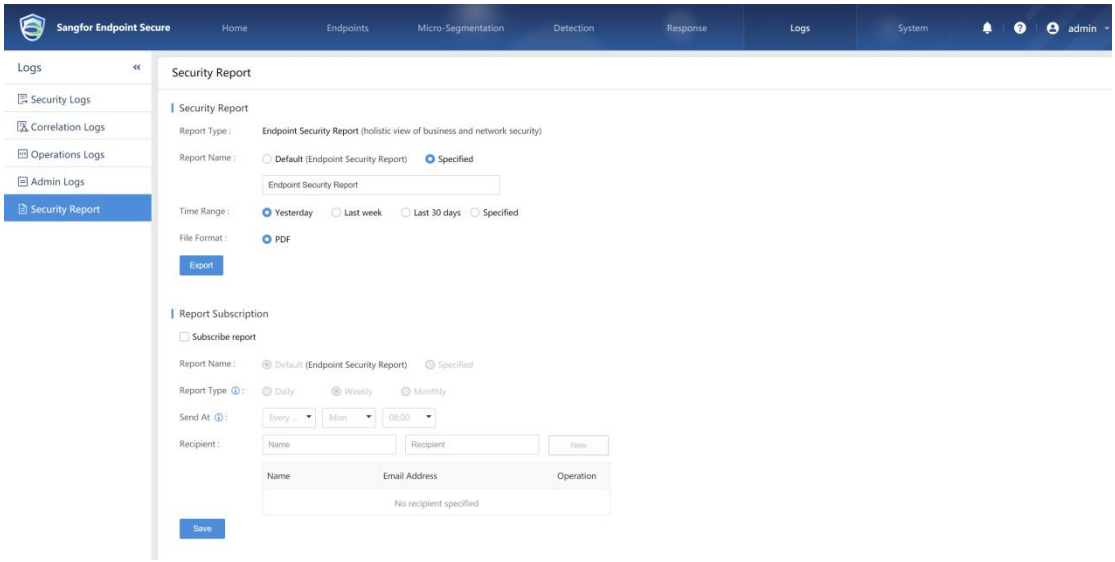
3.7.5 Security Report

The Security Report is available by report export and report subscription.

Security Report You can specify report name and time range, and export the endpoint security report as PDF.



Report Subscription You can subscribe the daily, weekly, and monthly security report, and send the subscribed report to the recipient's inbox at specified time.



You need to configure the SMTP server first before sending subscribed report. For the SMTP server settings, refer to Section 3.8.6.1.

Report Name: It configures the name of the subscribed report, which can be either default or customized name.

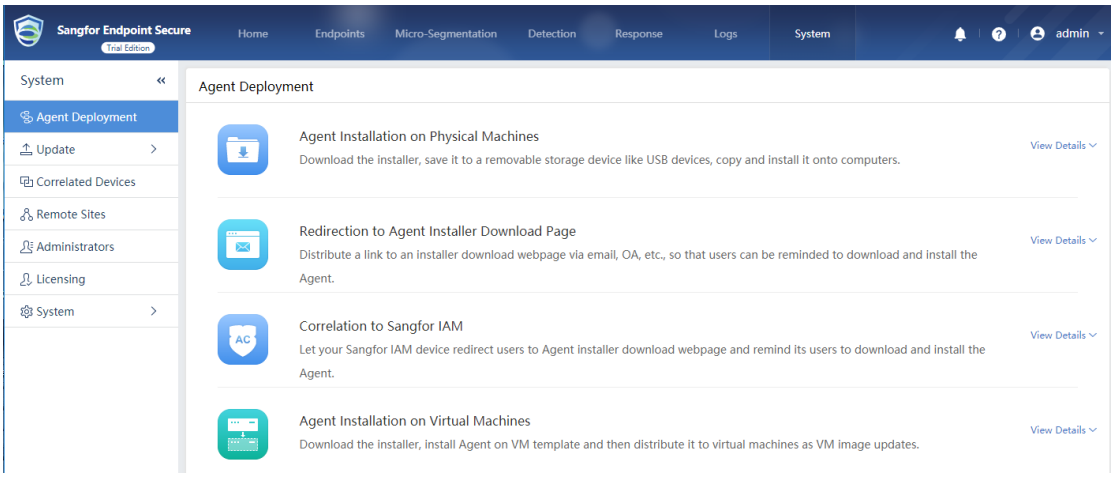
Periodic: It specifies the report type, which can be daily, weekly or monthly report.

Send At: It configures the time when the daily, weekly, and monthly report will be sent.

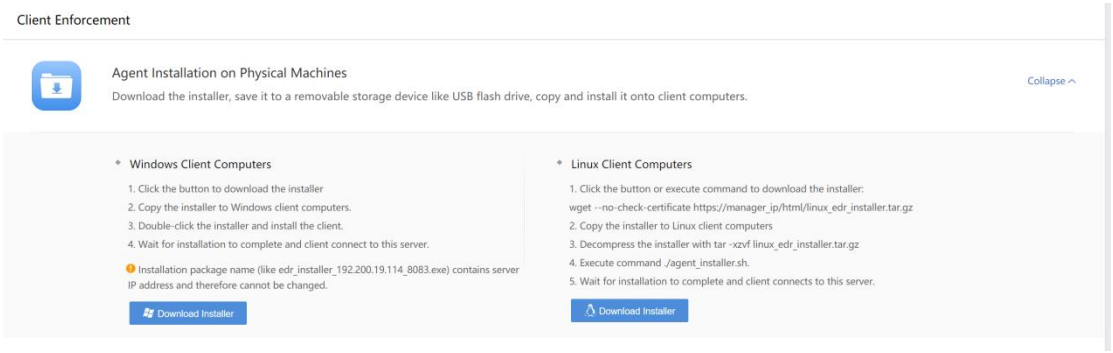
Recipient: It configures the report recipient name and email address. Multiple email addresses are supported.

3.8 System

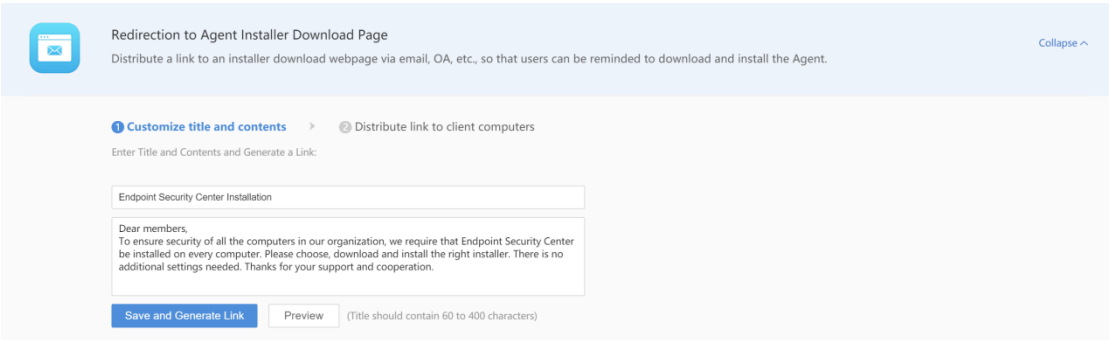
3.8.1 Agent Deployment



Agent Installation on Physical Machines: This is used to download the Agent to be installed on the endpoint, including that for Windows and Linux client computers. Installation steps are also provided here, as shown below:

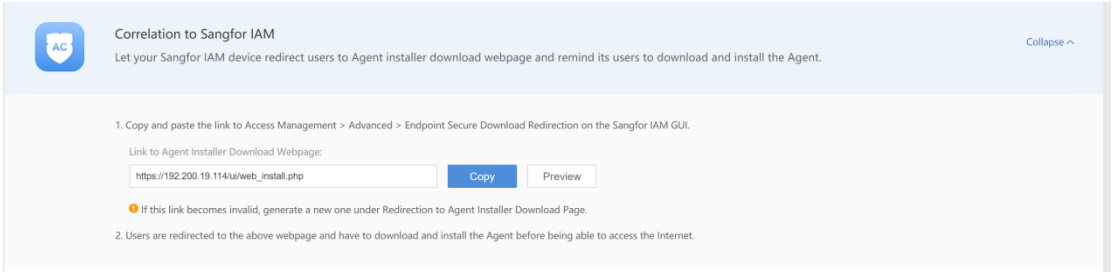


Redirection to Agent Installer Download Page: Distribute the link address of the package download webpage to the users through email, OA and the like, as shown in the following figure:



Correlation to Sangfor IAM: The endpoint is redirected to the webpage of the deployment

notification through the Endpoint Secure correlated to IAM. The notification will display until the endpoint downloads and installs the Agent. This method needs to be used with **Redirection to Agent Installer Download Page**, as shown below:

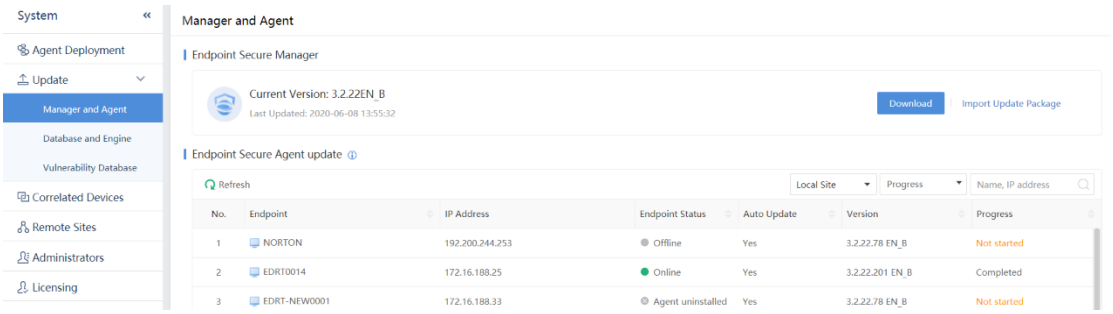


Agent Installation on Virtual Machines: Create a new VM in the virtualization management Endpoint Secure server and install Agent on the virtual machine and then convert the VM into a template to deploy more virtual machines. You may optionally install the Agent on the existing template VM, then perform update operation on the template to install the Agent on virtual machines deployed from that VM template, as shown in the following figure:

3.8.2 Update

This section includes update of **Manager and Agent, Database and Engine** and **Vulnerability Database**.

3.8.2.1 Manager and Agent



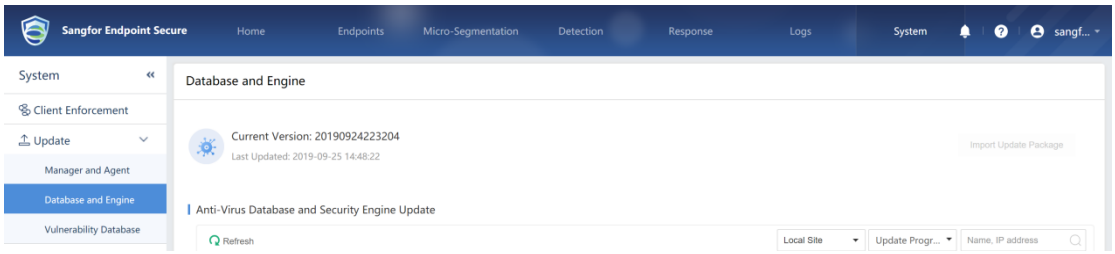
Sangfor Endpoint Secure Manager: It displays the current version of the manager.

Download and import the upgrade package from the official BBS. The upgrade does not require restarting server.

Agent Update: When the Agent on endpoint detects that the manager has been upgraded, it will be upgraded automatically. The current version of the endpoint agent and the upgrade status show here.

3.8.2.2 Database and Engine

If the manager can access to the Internet and once the manager detected that there is update of anti-virus database in the cloud, it will automatically update the database.

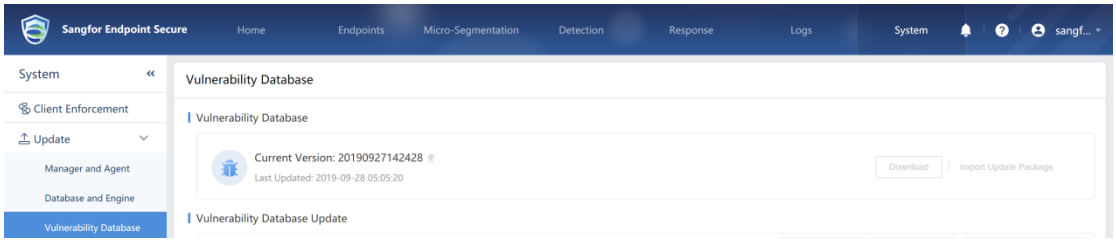


Database and Engine If the Endpoint Secure Manager cannot access the Internet (for example, in the isolated network scenario), download the offline anti-virus database from the official BBS, and then import the anti-virus database in this page after decompression update the anti-virus database.

Anti-Virus Database and Security Engine Update When the Agent on endpoints detects that the manager's anti-virus database has been upgraded and if its update server is the manager, the anti-virus database of the agent is automatically updated. The current anti-virus database version and the upgrade status of the Agent show here.

3.8.2.3 Vulnerability Database

If the manager can access the Internet and the automatic update of the vulnerability database is enabled and when the manager detects that there is update of vulnerability database in the cloud, the database will be updated automatically.



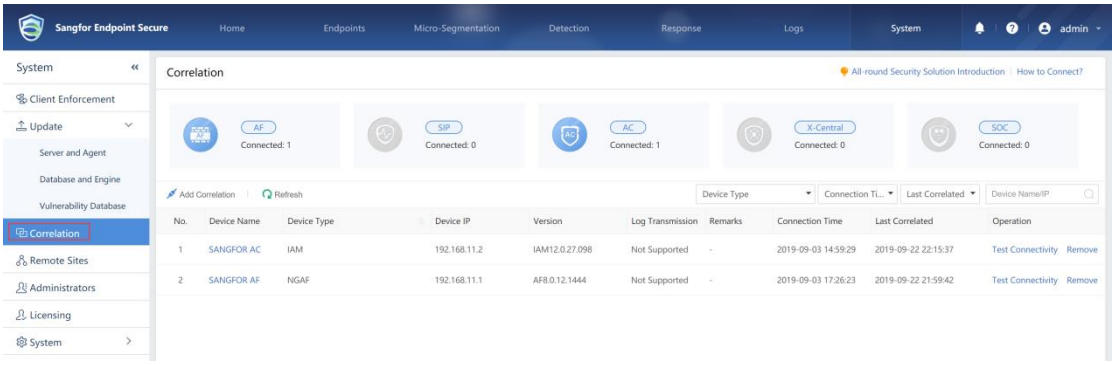
Vulnerability Database If the Endpoint Secure Manager cannot access the Internet (for example, in the isolated network scenario), download the offline vulnerability database from the official BBS, and then import the vulnerability database from this page after decompression to update the vulnerability database.

Vulnerability Database Update When Agent on endpoint detects that vulnerability database on the manager has been upgraded, vulnerability database on Agent will be updated automatically. The current vulnerability database version and the upgrade status of the endpoint agent show here.

3.8.3 Correlated Devices

Endpoint Secure Manager can be correlated to IAM, NGAF, Platform-X and Cyber Command to provide customers with a closed-loop solution from threat detection and threat removal. The following are what the Endpoint Secure can do when correlating to other security products.

System > Correlated Devices page displays correlation status between the Endpoint Secure and other products, as shown below:



3.8.3.1 Correlated to IAM

The correlation between the Endpoint Secure and the IAM can facilitate the deployment of the Endpoint Secure Agent and jointly detect and remove viruses. The following describes

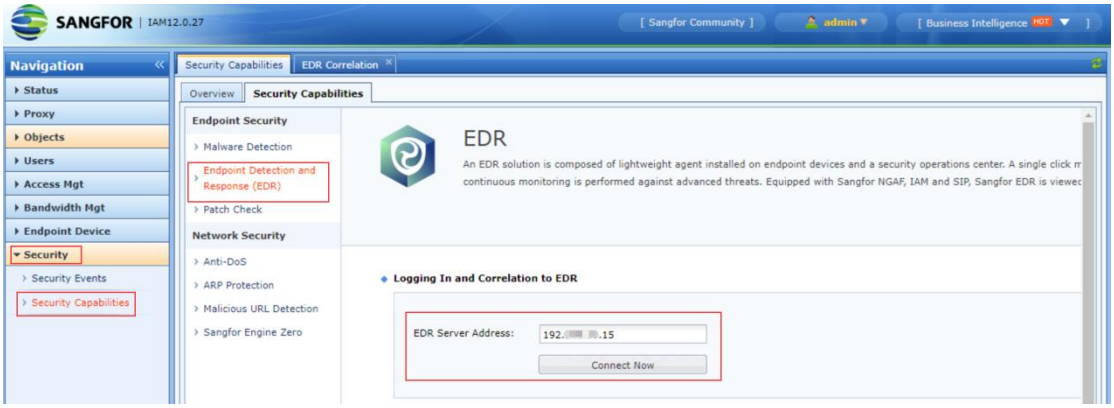
the requirements, settings and actions of correlation between Endpoint Secure and IAM:

➢ Requirements

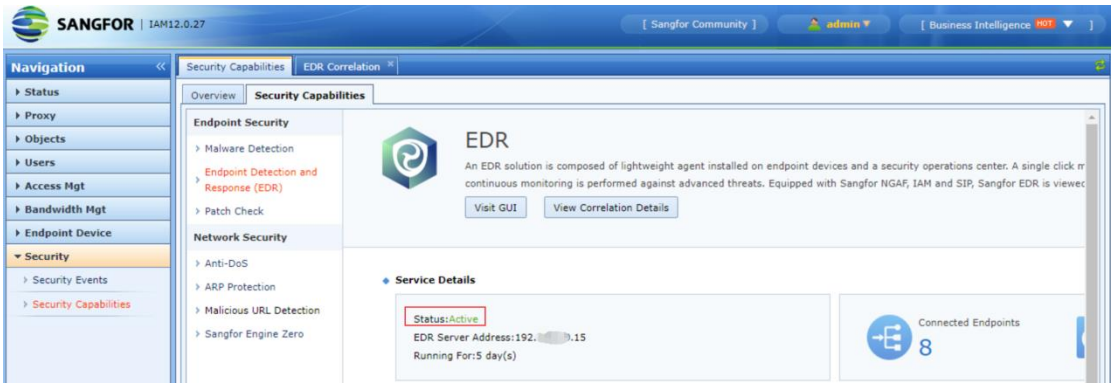
- The IAM is required to connect to the Endpoint Secure via TCP 443 port.
- The version of IAM must be 12.0.17 or later.

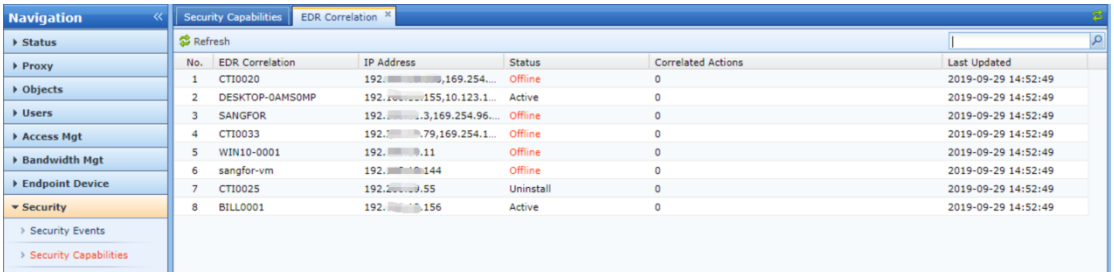
➢ Settings

- Correlate Endpoint Secure to IAM simply by entering IP address of Endpoint Secure Manager through **Security** > **Security Capabilities** > **Endpoint Secure** page on IAM manager.



- After the correlation is successful, the Endpoint Secure service status in the IAM device shows "Active". Click View Correlation Details to view the connectedi endpoints on the Endpoint Secure, as shown below:

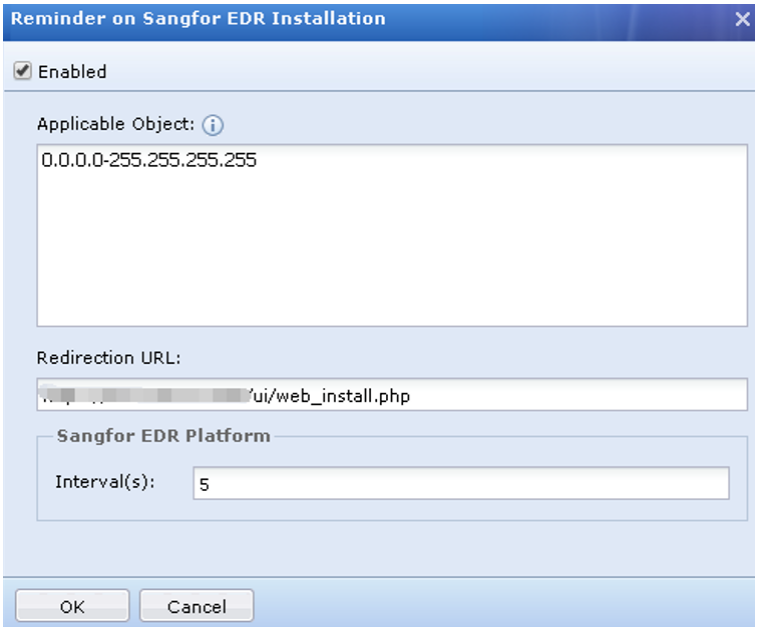




➢ Actions

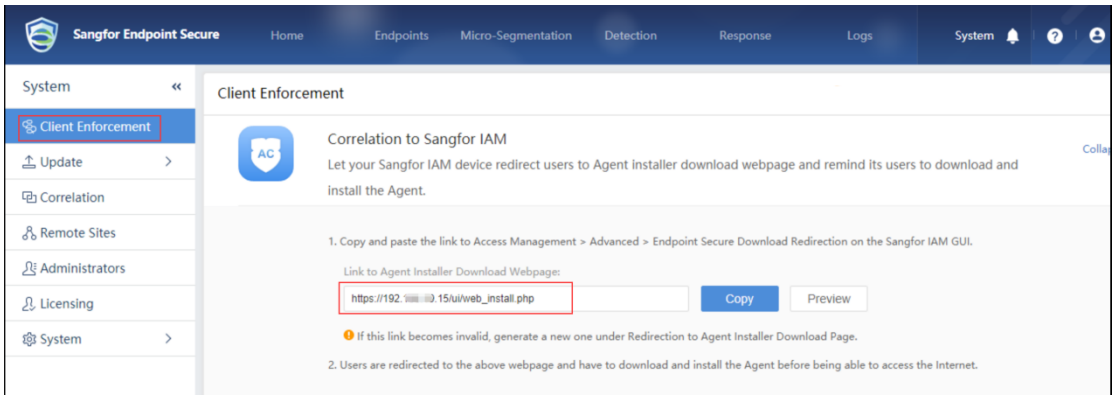
- Promote Endpoint Secure Agent

Go to **Security > Security Capabilities > Endpoint Secure**, click Reminder Options to configure the IP address range where the Agent is installed and redirect to the Agent download address, as shown below:

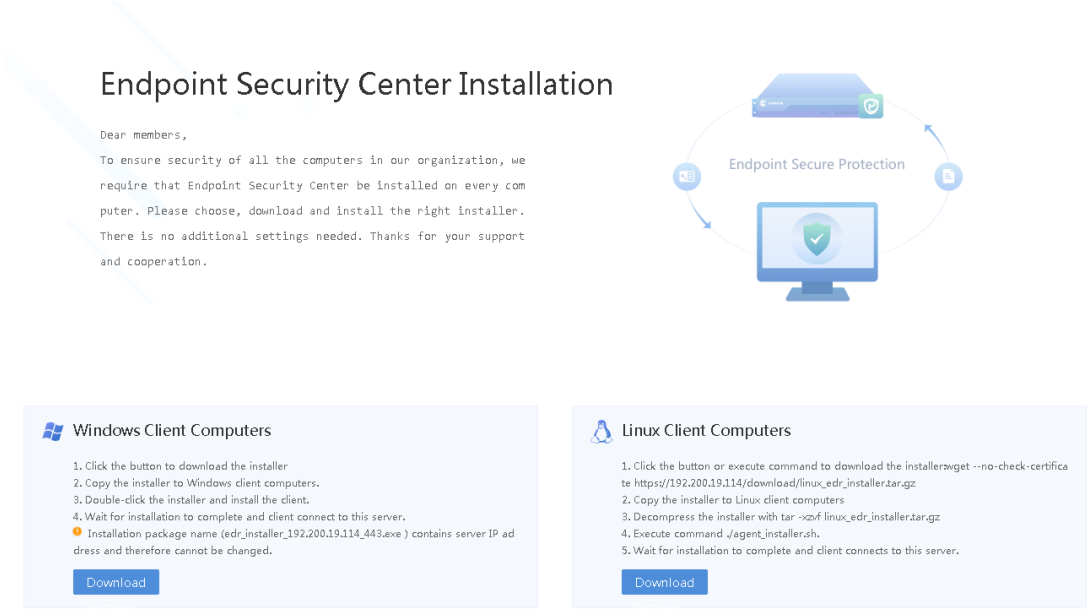


Applicable Object: Fill in the IP address range of computers in the intranet that needs to install the Agent.

Redirection URL: The endpoint is redirected to the download address of the Agent, fill in the URL in **System > Client Enforcement** page on the Endpoint Secure Manager, as shown below:

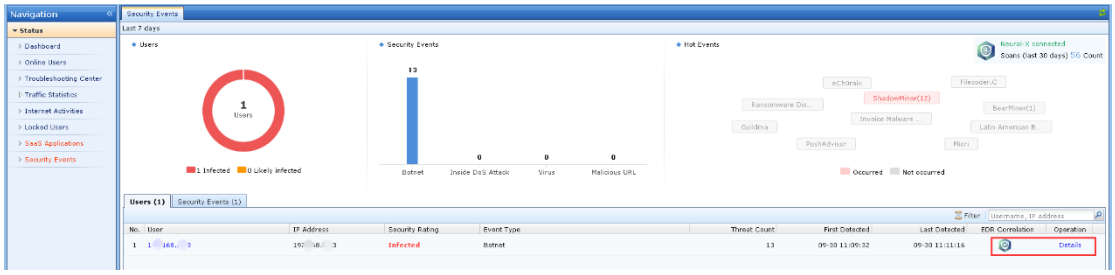


After the configuration completes, the user is redirected to the agent installation notification page when accessing the web page, as shown below. This page pops up periodically until the user installs the Agent.

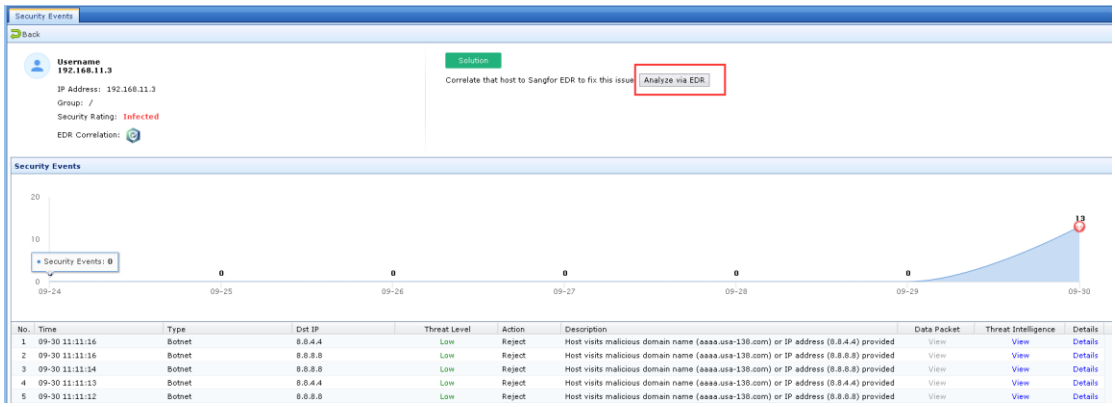


- Correlated Virus Scan and Removal

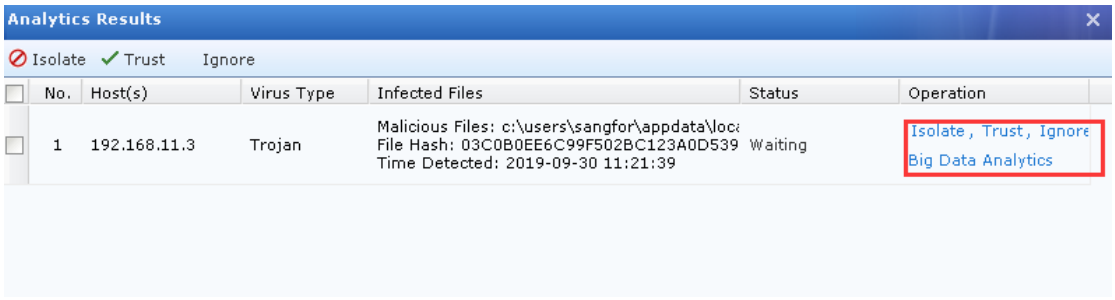
When IAM enables Bot Detection and identifies the risky endpoint, Endpoint Secure will scan for and remove the virus. Go to **Status > Security Events > Users** on IAM manager, as shown below:



Click **Details** to view the details, as shown below:



Click Analyze via Endpoint Secure to perform virus scan and removal on risky endpoint, and return the scanning result, as shown below. From the IAM manager, "Isolate", "Trust" or "Ignore" are supported to perform on detected suspicious files.



3.8.3.2 Correlated to NGAF

The correlation between Endpoint Secure and the NGAF can facilitate correlated virus scan and removal and botnet forensics. The following describes the requirements, settings and actions of correlation between Endpoint Secure and NGAF:

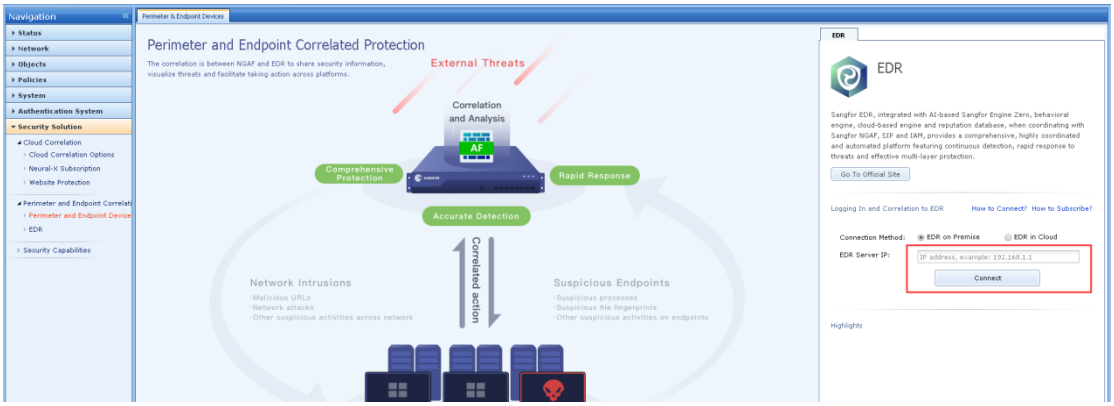
- Requirements

The following requirements must be met to enable virus removal and botnet proof:

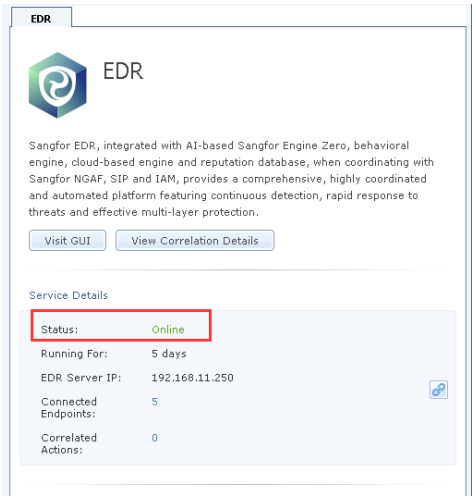
- The NGAF is required to be connected to the Endpoint Secure via TCP port 443
- The version of NGAF should be 8.0.12 or later.

- Settings

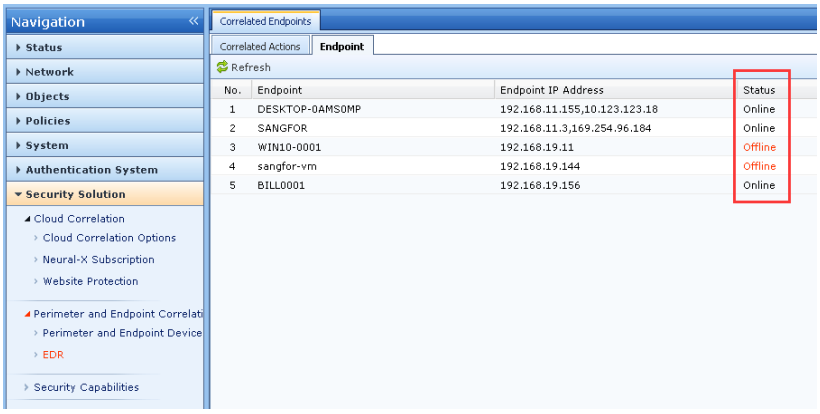
Correlate Endpoint Secure to IAM simply by entering IP address of Endpoint Secure Manager through **Security > Endpoint Protection > Endpoint Secure Correlation** page on NGAF manager, as shown below:



Once they are correlated, the status of Endpoint Secure in configuration page in NGAF is **Online**, as shown below:



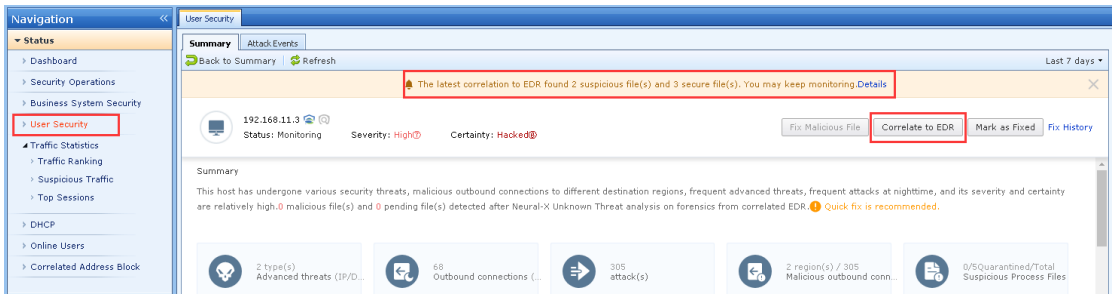
After they are correlated, log in to NGAF manager and go to **Security Solution > Endpoint Protection > Endpoint Secure Correlation to** view the connected endpoints and other details, as shown below:



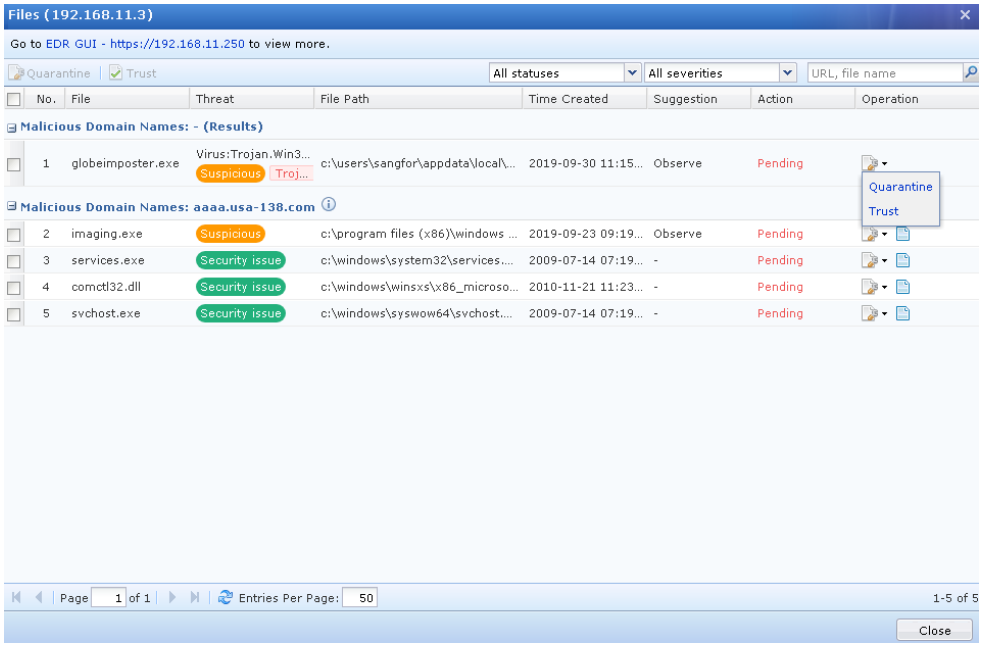
- Actions

- Correlated Virus Scan and Removal

When NGAF identifies a risky endpoint, it can perform virus scan and removal via the Endpoint Secure. Go to **Status > User Security** in NGAF manager, and remove the viruses on the found risky endpoints via Endpoint Secure, as shown below:

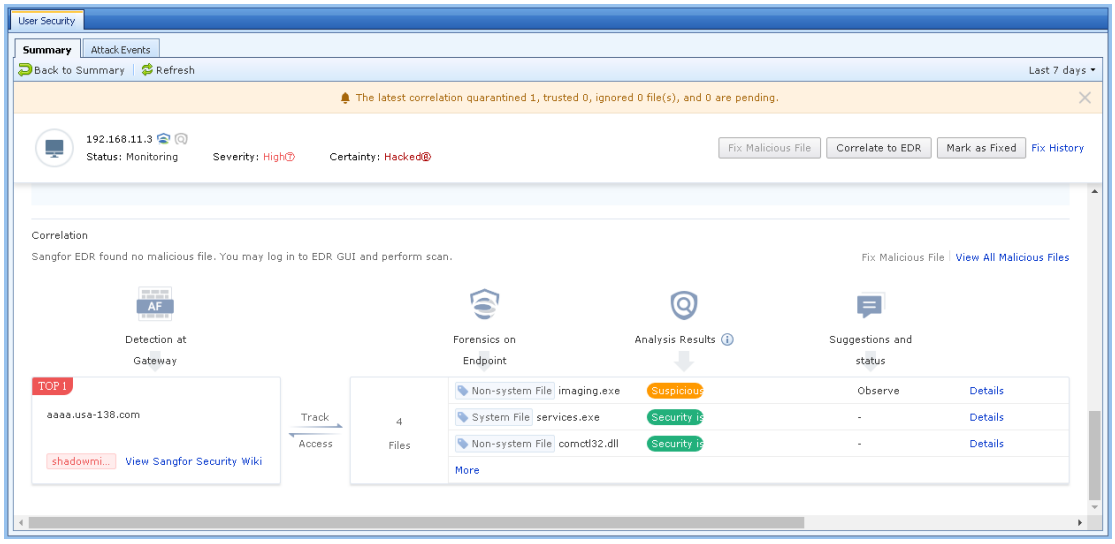


In NGAF manager, Quarantine or Trust the detected threat files via correlated Endpoint Secure, as shown below:

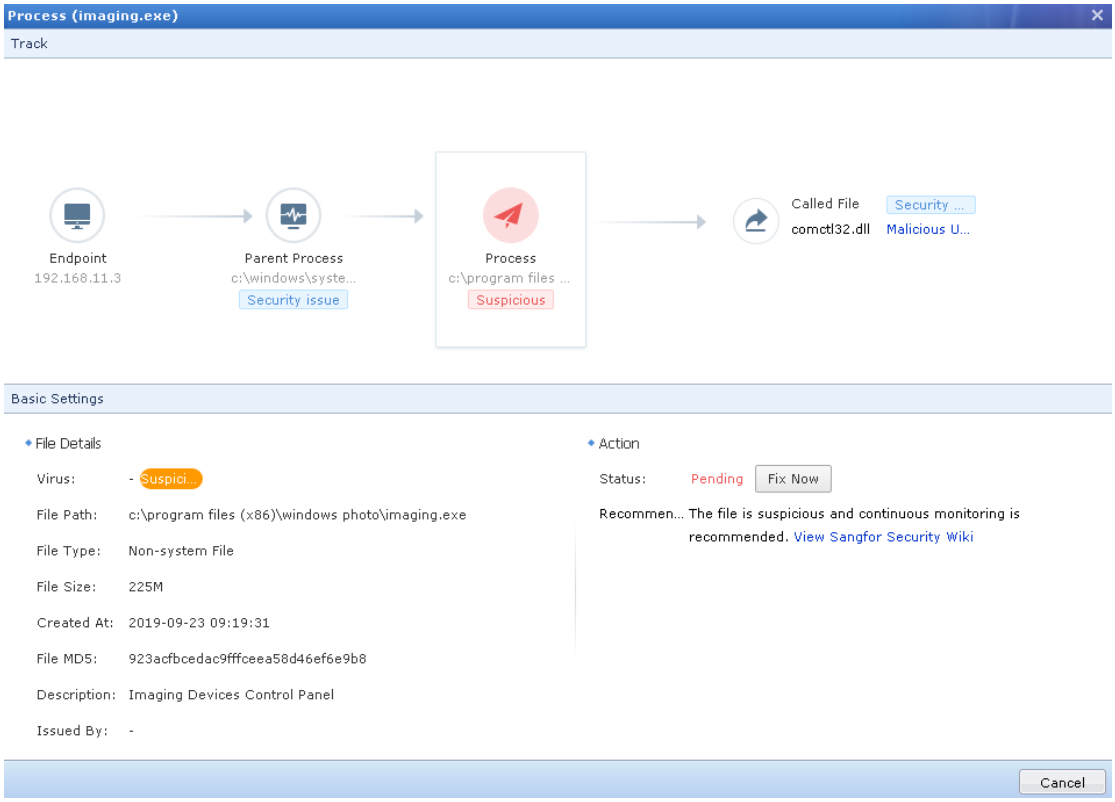


- Botnet Forensics

Endpoint Secure can record the domain accessed by endpoint and processes that access the domain. When the botnet attack is found on the NGAF, it will show forensics and seek the source via Endpoint Secure, which can help users find examples of specific processes that access the botnet domains and related files of the processes. Go to **Status > User Security** in NGAF manager and click the specific risky endpoint. As shown below, "Forensics on the Endpoint" is the proof for botnet domain obtained by NGAF and Endpoint Secure.

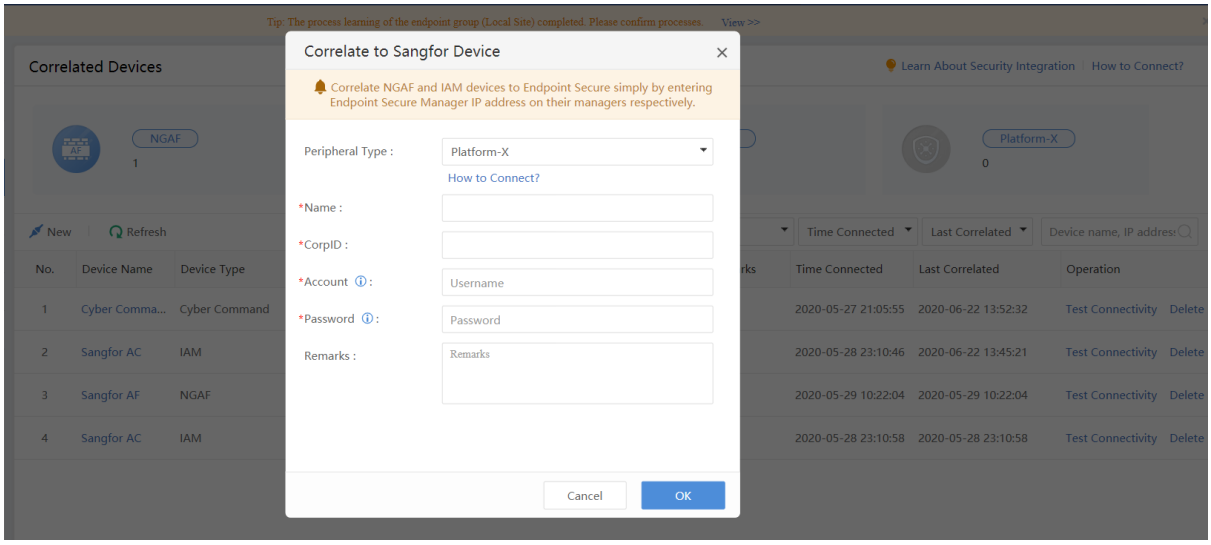


Click Details to view the tracing result of malicious domain access obtained by Endpoint Secure and fix threat files, as shown below:



3.8.3.3 Platform-X Correlation

Correlating Endpoint Secure to Platform-X can provide correlated threat fix and botnet forensics. Log in to Endpoint Secure Manager and go to **System** > **Correlated Devices**, and click New to correlate to a new device, as shown below:



Device Type: Select Platform-X.

Name: Enter an identifiable name for Platform-X.

CorpID: CorpID is required. Each user account that uses Platform-X has a unique CorpID.

Account: username is required and should be the same as the account created on Platform-X.

Password: password is required and should be the same as that set on Platform-X.

3.8.3.4 Cyber Command Correlation

By correlating to Cyber Command, infected files or victim endpoints can be detected on Cyber Command, and Endpoint Secure can perform virus scanning or isolate inbound and outbound traffic of victim endpoints, and also can report security logs on Endpoint Secure to Cyber Command for analysis. The correlation between Endpoint Secure and Cyber Command will be introduced in the following three aspects: correlation requirement, correlation configurations and correlation result.

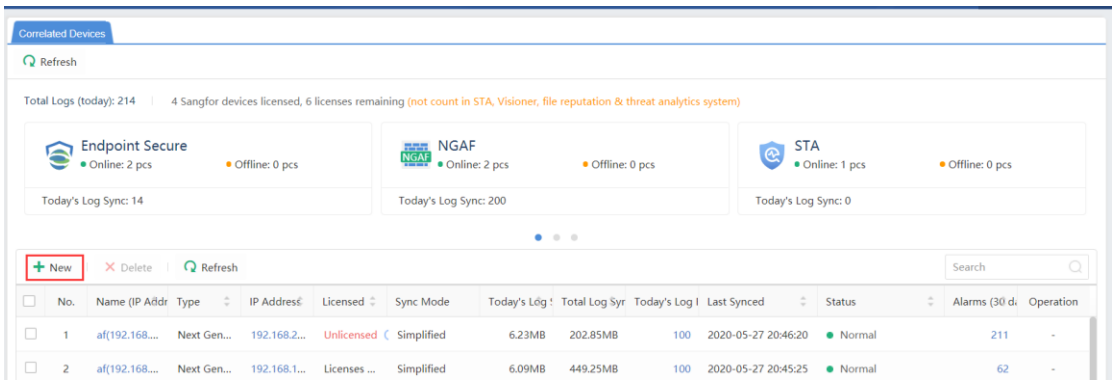
Correlation Requirement:

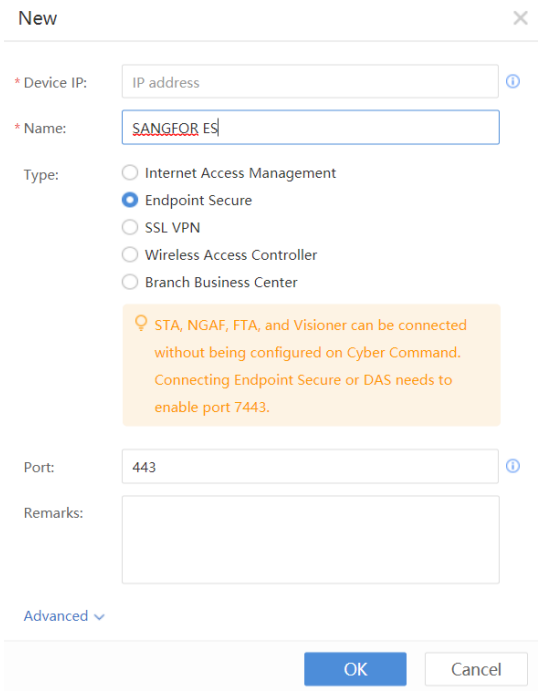
- Cyber Command version 3.0.23 and later versions.
- Endpoint Secure Manager can communicate with Cyber Command port TCP7441 (This port is used to receive logs).
- Cyber Command can communicate with the TCP443 port of Endpoint Secure Manager.

Correlation Configurations:

The correlation can be configured on either Endpoint Secure Manager or Cyber Command. To configure it on Cyber Command:

Go to **System** > **Correlated Devices** > **Correlated Devices**. Click New.





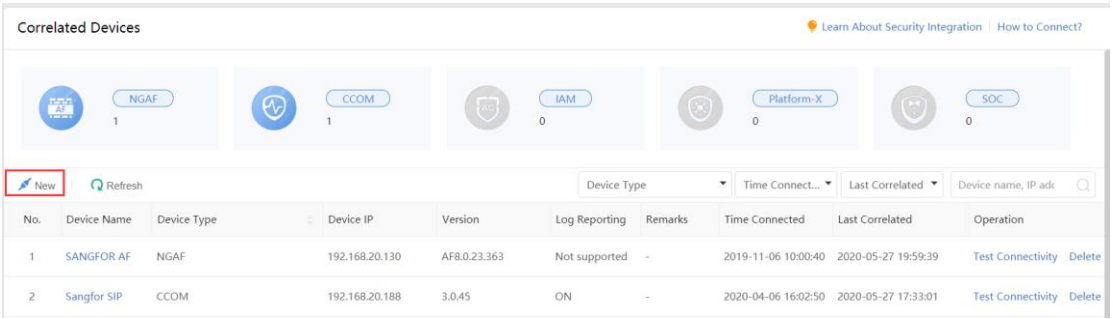
Device IP: Enter Endpoint Secure Manager IP address.

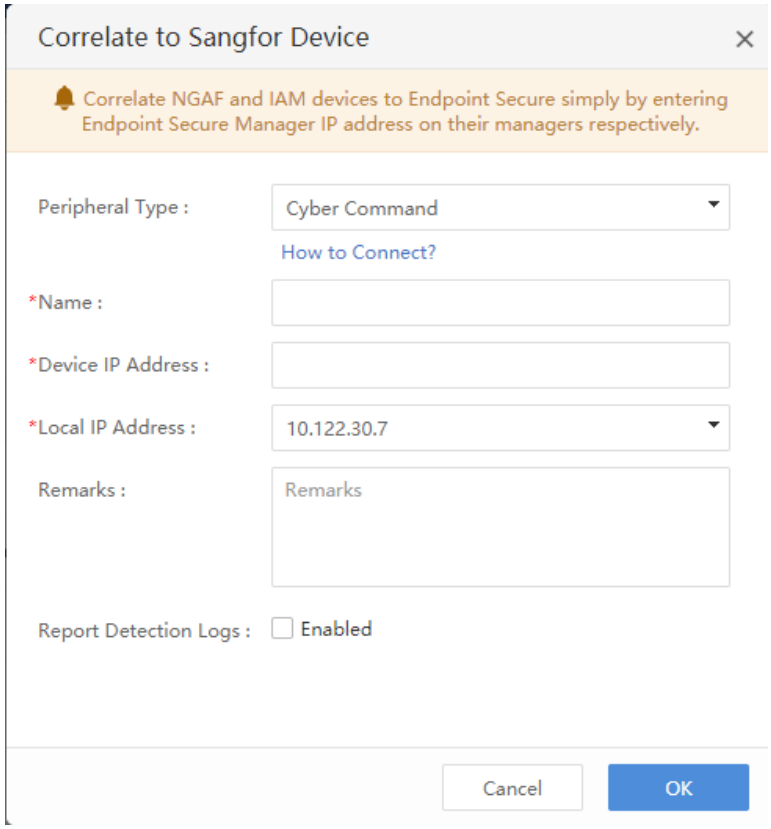
Name: Enter a name for the Endpoint Secure

Type: Select Endpoint Secure

To configure it on Endpoint Secure Manager:

Go to System > Correlated Devices. Click New.





Peripheral Type: Select Cyber Command.

Name: Enter a distinguishable name for Cyber Command.

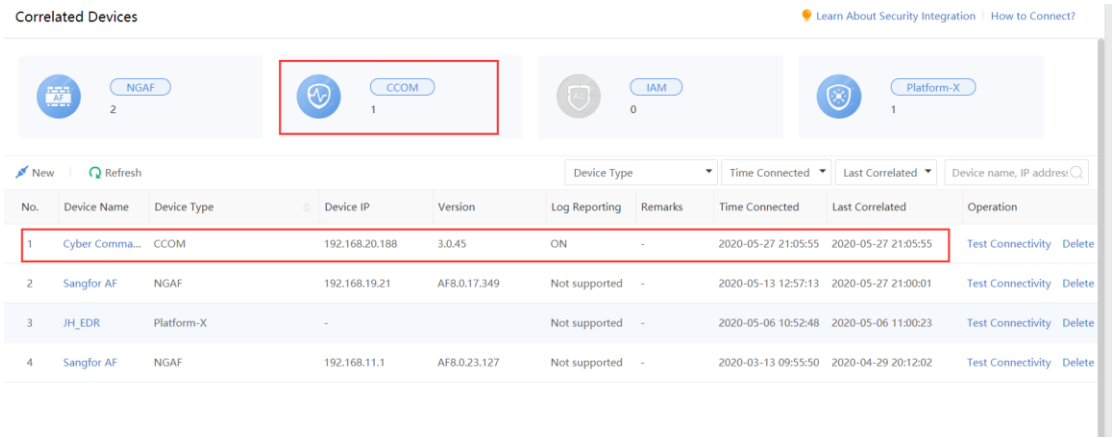
Device IP Address: Enter Cyber Command IP address.

Local IP Address: Select the IP address that can communicate with Cyber Command.

Report Detection Logs: Enable it to upload logs to Cyber Command for analysis.

Correlation Status:

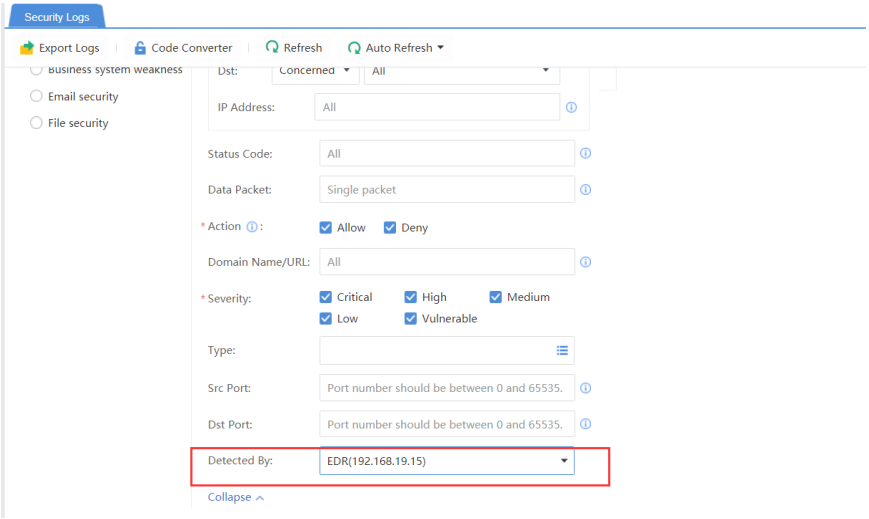
If Endpoint Secure is correlated to Cyber Command, the status in System > Correlated Devices on Cyber Command will display online.



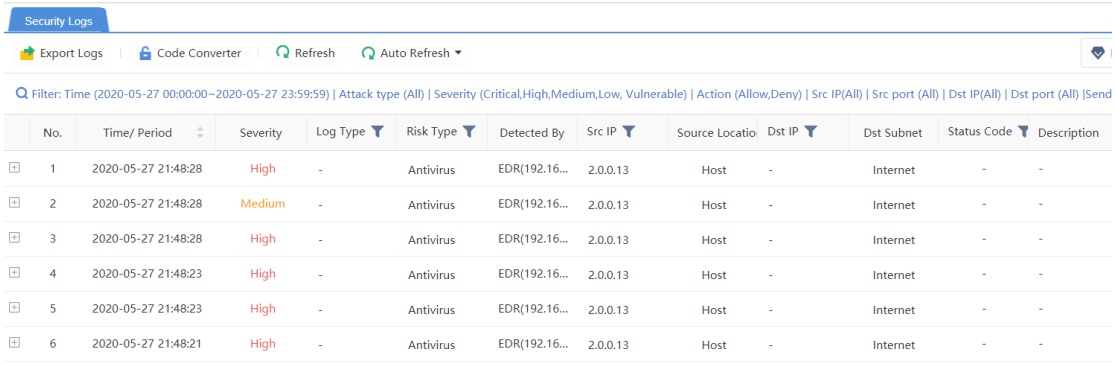
To check correlation status, click Test Connectivity in System > Correlated Devices on Endpoint Secure Manager.

Correlation Result:

Endpoint Secure Manager uploads logs to Cyber Command: On Cyber Command, go to **Analytics** > Security **Logs.** Click Detected By dropdownlist to select the Endpoint Secure Manager you configure on Cyber Command, as shown below:

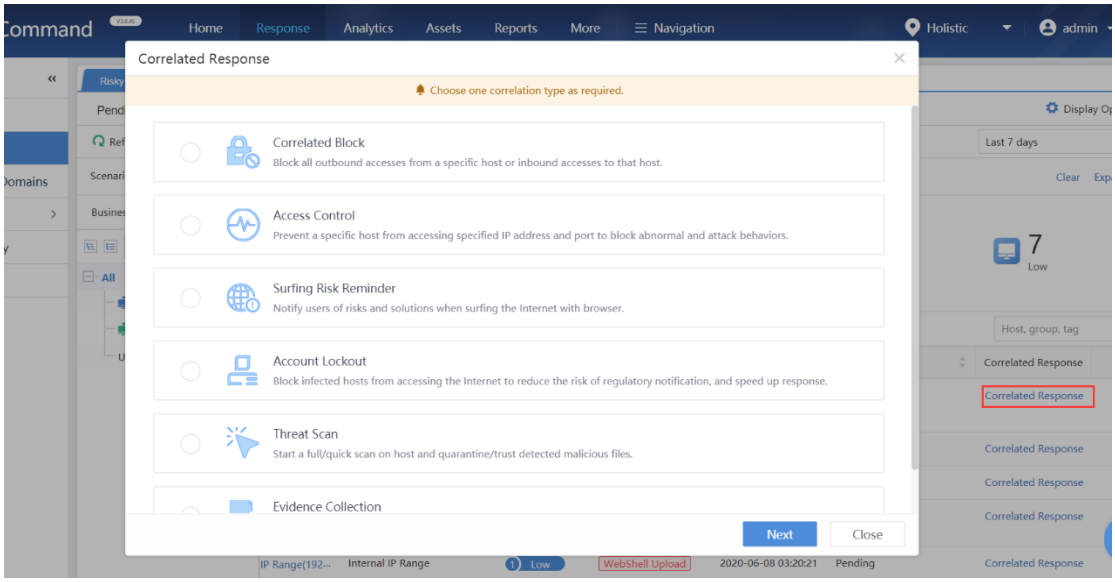


Click on Go then it will show all logs uploaded from Endpoint Secure Manager.



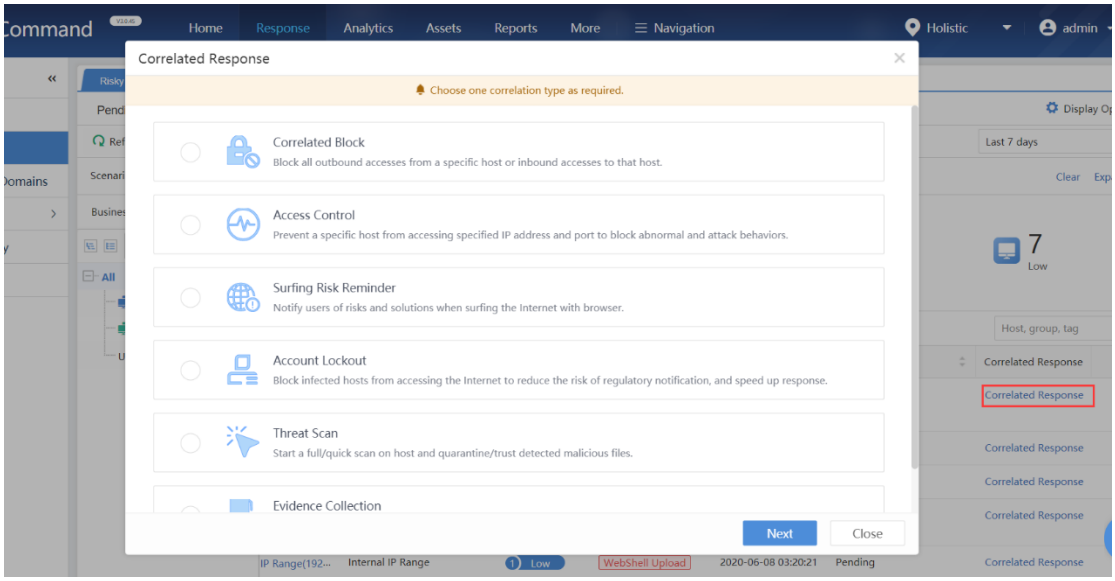
Correlation with Endpoint Secure to do virus scanning

When Cyber Command discovers a risky endpoint, it can correlate to Endpoint Secure to perform virus scanning. Go to Response > Risky Hosts to conduct virus scan on risky hosts with installed Endpoint Secure Agent installed. After the Agent finished the virus scan, administrator can fix the risky hosts on Cyber Command, Isolate, Trust, or Ignore, as shown below:



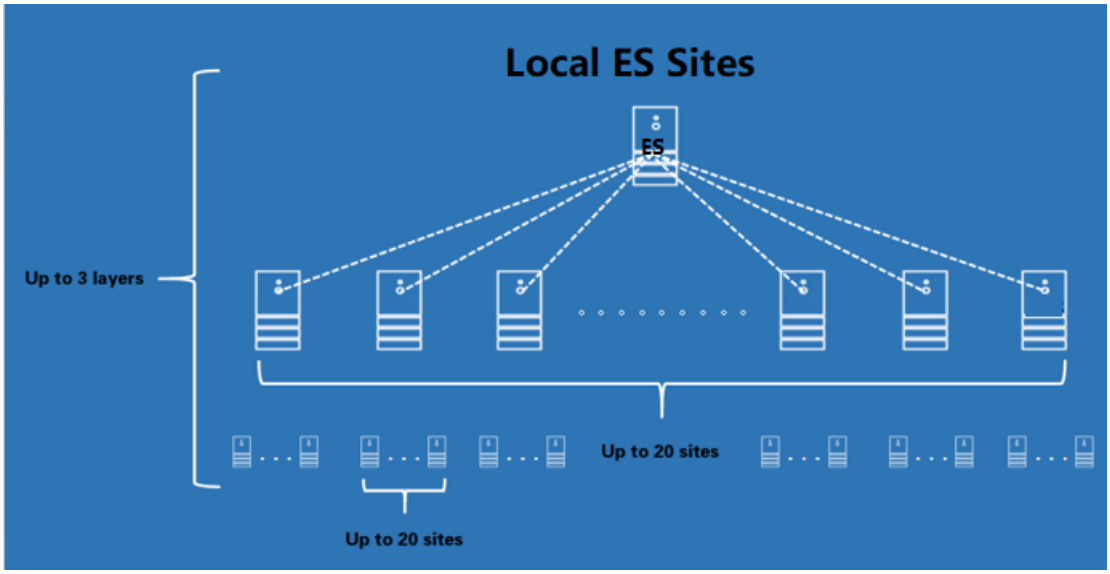
Risky Host Isolation:

When a risky host is discovered by Cyber Command, it can correlate with Endpoint Secure to isolate the risky host. Go to Response > Risky Hosts to isolate the host, block, outbound and /or inbound traffic, as shown below.

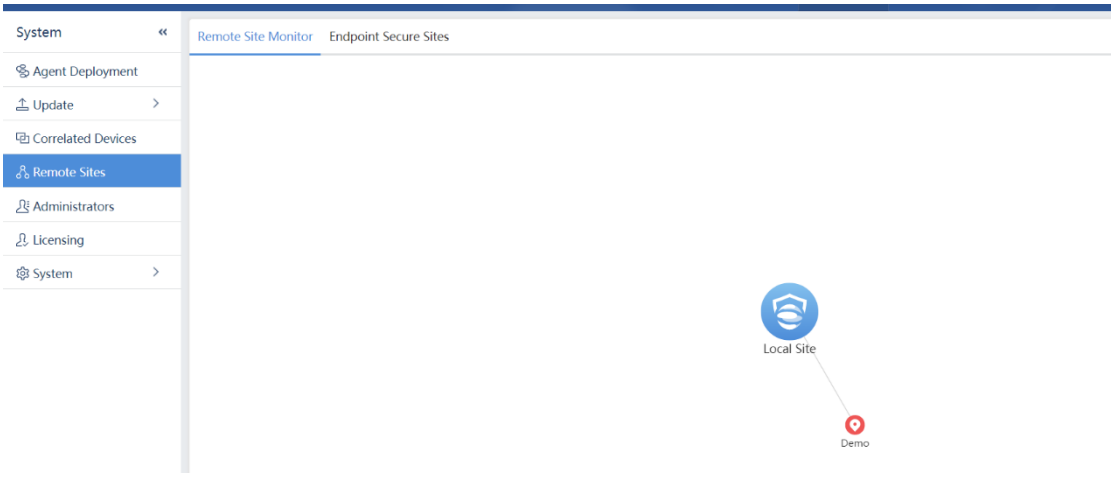


3.8.4 Remote Sites

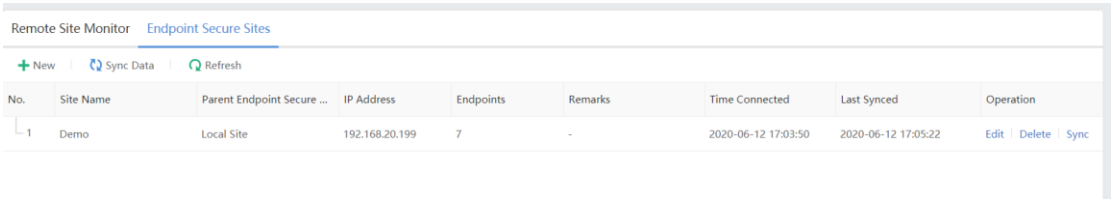
Remote sites are Endpoint Secure servers residing in remote offices that can be correlated with the local Endpoint Secure server. Up to 20 Endpoint Secure servers can be correlated with an Endpoint Secure server, as shown in the following figure:



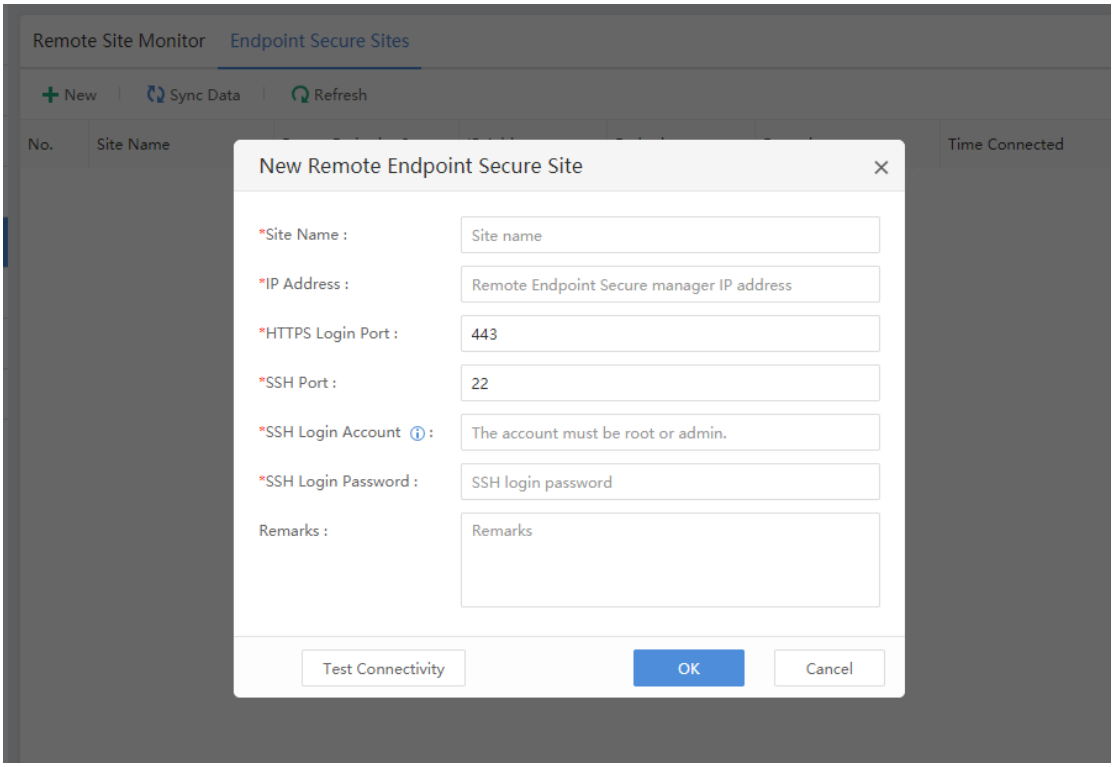
Go to **System** > **Remote Sites** to view the remote sites, as shown below:



To add a new remote site Endpoint Secure server, go to Endpoint Secure Sites



Click **Add Remote Endpoint Secure Site**.



Site Name: The name of the remote Endpoint Secure server.

IP Address: The IP address of the remote Endpoint Secure server.

HTTPS Login Port: It is port 443 by default. It is used to log in to the remote Endpoint Secure server and can be modified based on specific conditions.

SSH Port: It is port 22 by default. It can be modified based on specific conditions.

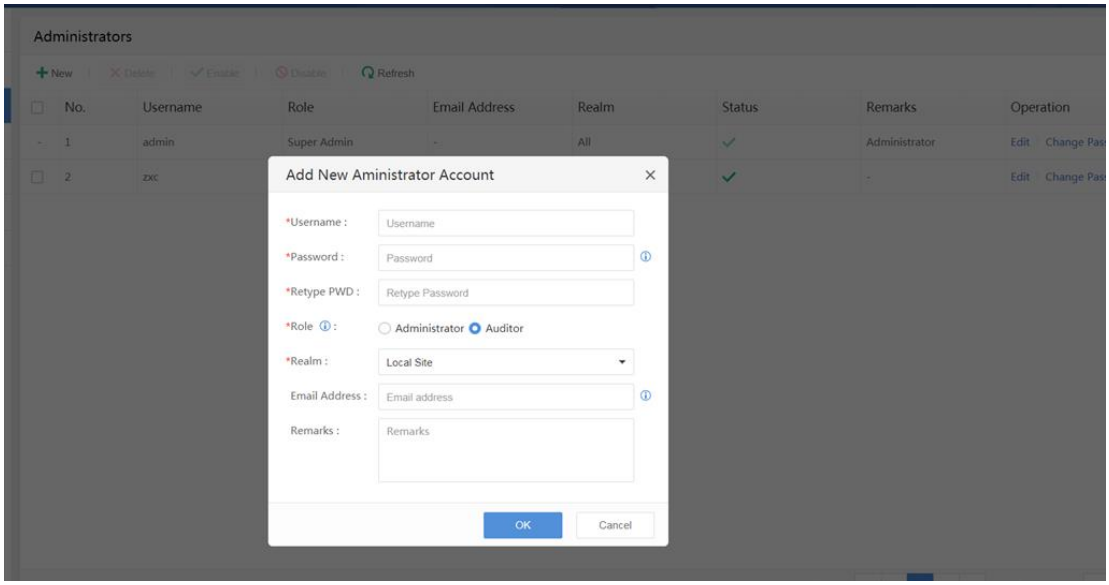
SSH Login Account: The account used to log in to the remote Endpoint Secure server. It supports password-free login by using root account.

SSH Login Password: The password of SSH account, supports password-free login.

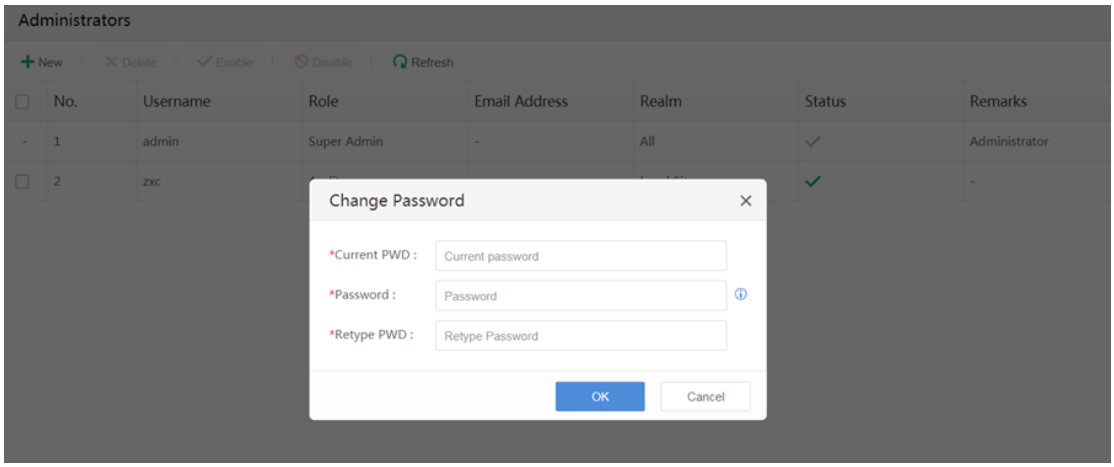
After completing configuration and the connection test succeeds, click **OK** to submit.

3.8.5 Administrators

Add one or more new administrator account, set role of the account to "Administrator" or "Auditor", then set administrative realm for the account. Each administrator can only manage or audit the endpoints in their administrative realm.

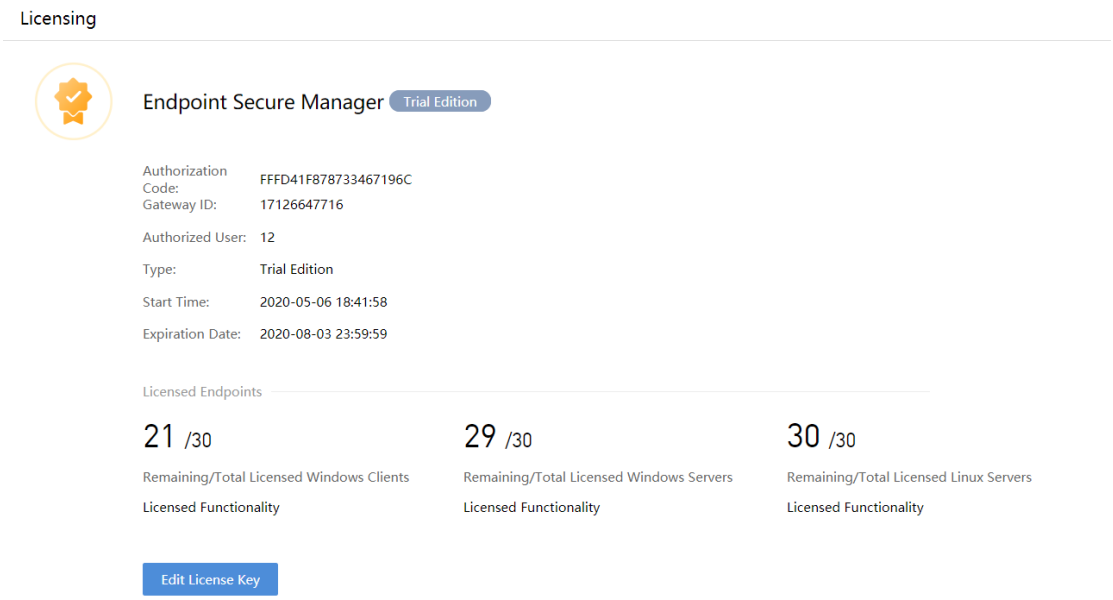


The password of the newly created account can be modified.

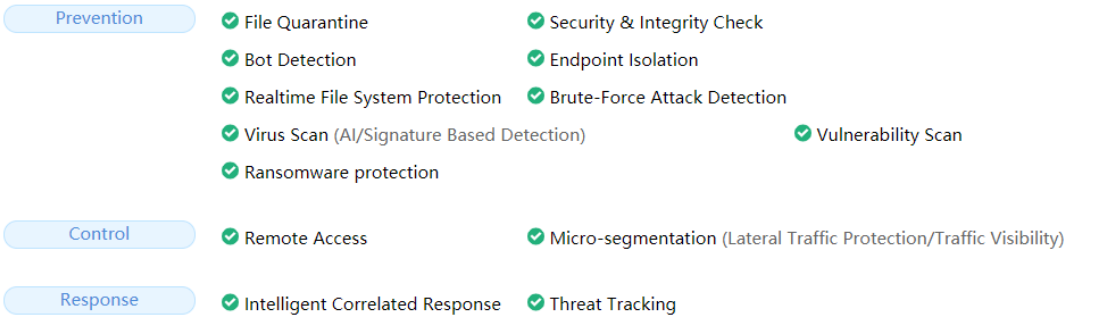


3.8.6 Licensing

The licensing on Endpoint Secure Manager is classified as Windows PCs, Windows servers and Linux servers. You can view the licensing details and expiration time here, as shown below:



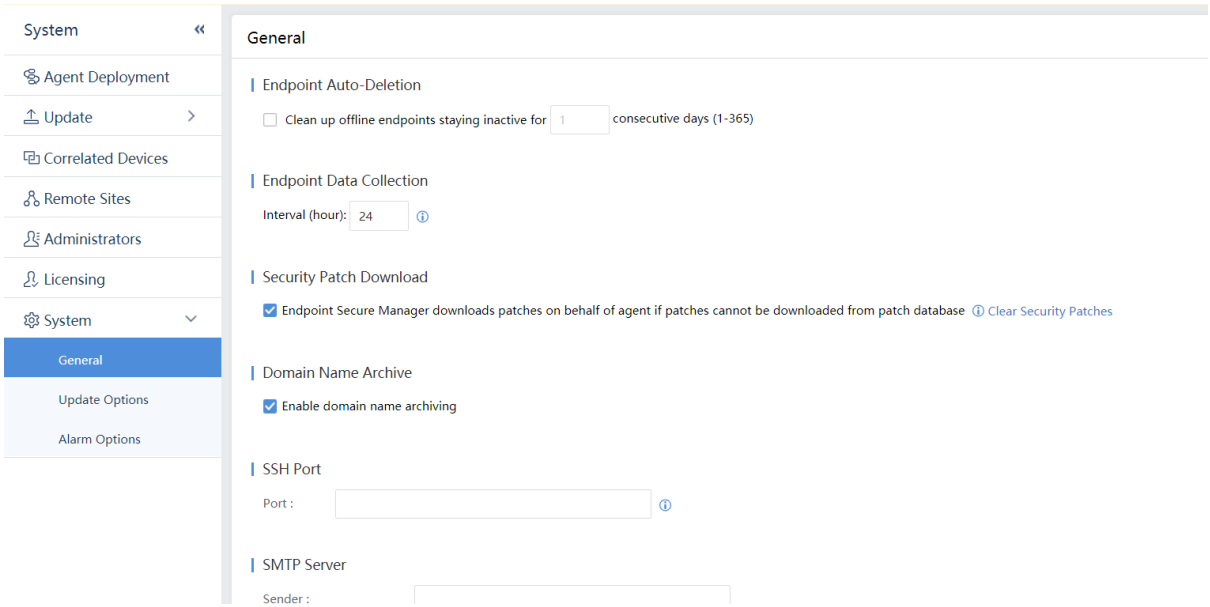
The complete licensed modules are shown as below:



3.8.7 System

3.8.7.1 General

You can set SSH port, SMTP server, and decide whether join the Sangfor Cloud Security Program in System > General page.



Endpoint Auto-Deletion: Automatically delete offline endpoints to release more authorizations.

Security Patch Download: For endpoints that cannot access Internet or download vulnerability patch, the vulnerability patches can be downloaded on endpoints through the manager to patch vulnerabilities.

SSH Port: To modify the port of the Endpoint Secure Manager. The default port is 22.

SMTP server: To configure SMTP server for sending the subscribed reports and alarm emails.

Sender: Configure the name of sender that sends alarm emails or subscribed reports.

SMTP Server Port: Configure the port of SMTP server. If the server is required to perform the encrypted sending, check **SSL.**

Sender Address and **Password** configure the email address and password to send emails.

Send Test Email: Click the button to verify whether the SMTP server configuration is successful. If the configuration is successful, you will receive the test email.

Sangfor Cloud Security Program: After joining the Sangfor Cloud Security Program, the Endpoint Secure will automatically upload any suspicious files to the Cloud Security Center for analysis so as to provide a more powerful and comprehensive security service, provided that the Endpoint Secure be able to access https://clt.sangfor.com.cn.

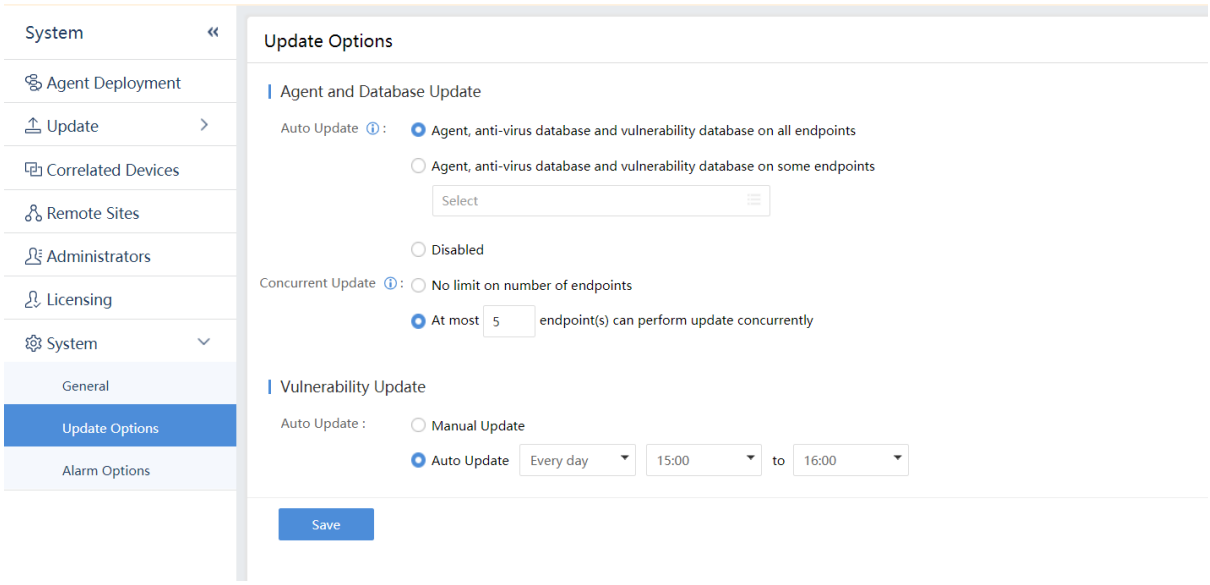
3.8.7.2 Update Options

You may update Endpoint Secure server and antivirus databases and vulnerability databases,

all together or separately, all or some concurrently. .

Update All or Some: To update Agent and database on one or some client computers, you can avoid upgrade failure that may occur on large number of client computers. If trial update is successful, perform all other client computers and servers at a time then.

Update All or Some Concurrently: To avoid network congestion caused by a large number of endpoint that perform update concurrently, you can set the maximum endpoints supported to reduce the impact of update on the network bandwidth.



Agent Database Update: To set the upgrade mode and the number of endpoints performing concurrent upgrade.

Auto Update: Choose a way to perform update, update all or select some endpoints.

Concurrent Update: It allows you to set the maximum number of endpoints that can be updated concurrently, reducing the impacts of update on the network bandwidth.

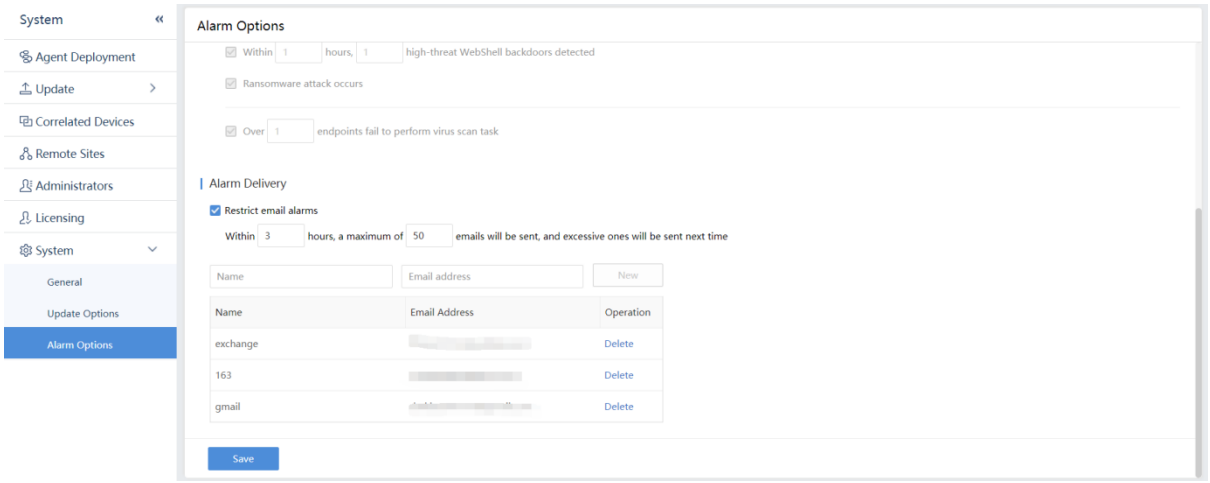
Vulnerability Update: To set the time for auto update of vulnerability database on manager. When enabled, the manager automatically updates the vulnerability database within the specified time range.

3.8.7.3 Alarm Options

On Endpoint Secure Manager, the email alarm can give alarms on the usage of CPU, memory, and disk on endpoints, and whether the network-wide threats reach defined

threshold. When the threshold is reached, an alarm email is sent to notify the administrator and let the administrator know the Endpoint Secure running status and the security of the entire network.

To use the email alarm, you need to configure SMTP server first. For the SMTP server settings, refer to Section 3.8.6.1.



Alarm-triggering Event: On Endpoint Secure Manager, configure the CPU, memory, disk alarm thresholds on endpoints, and network-wide threat alarm conditions. It is recommended to keep the default configuration and administrator can modify it based on actual conditions.

Alarm Delivery: It configures the recipient name and email address for alarm email. You can configure multiple recipients and multiple email addresses. Generally, it is configured as the administrator's email address.

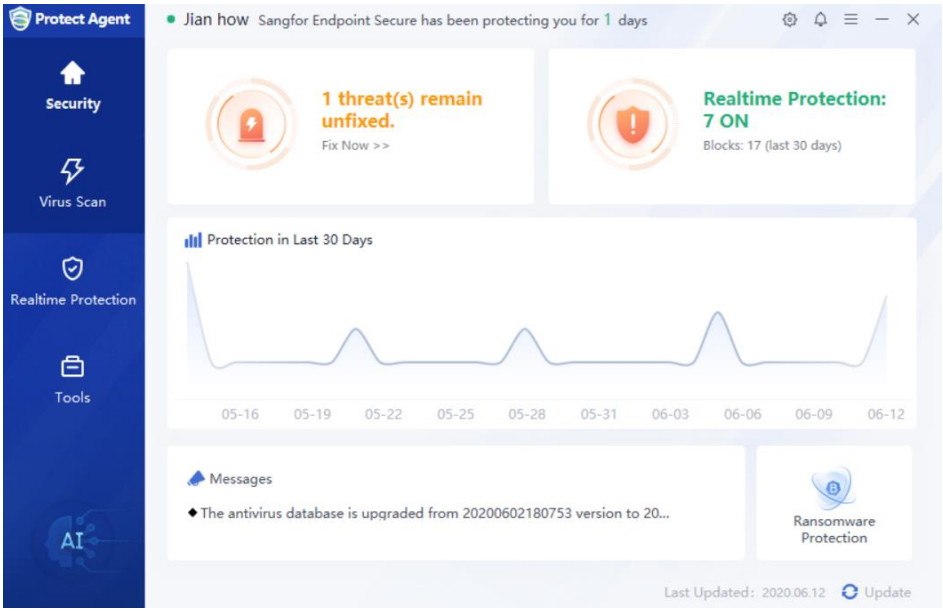
When an alarm event is triggered, an email will be sent to the configured email address.

Chapter 4 Installing Agent on Client Computer

This section is intended to facilitate the end users to perform virus scan on the client computers.

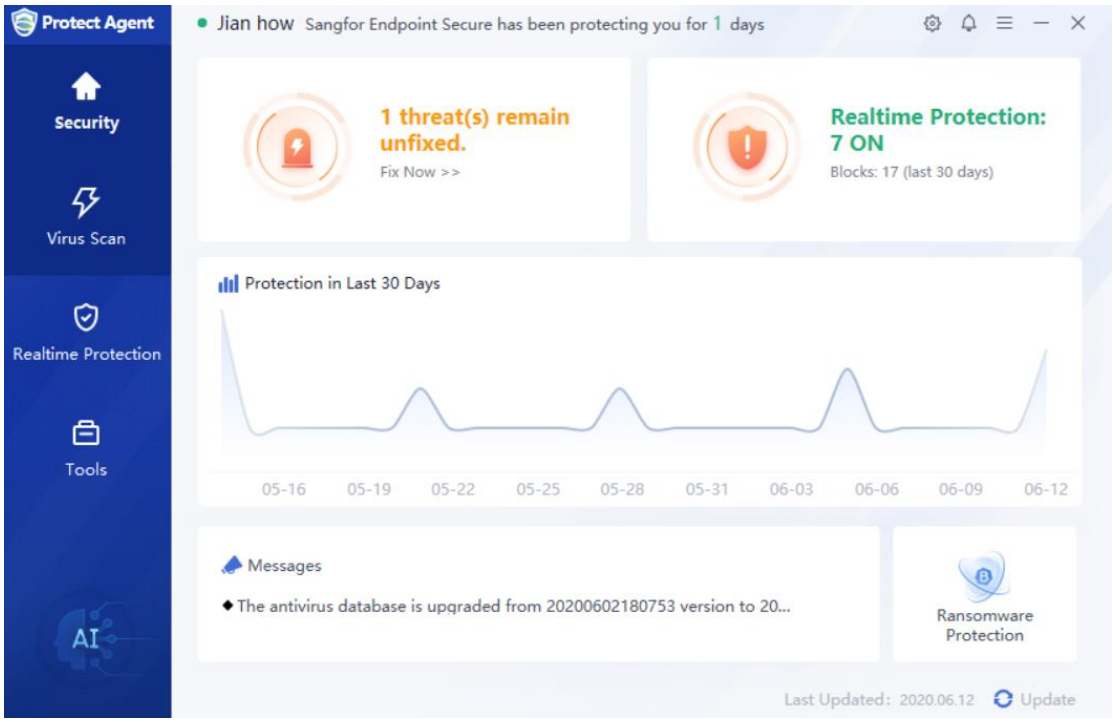
4.1 Installing Agent on Windows Clients

After Endpoint Secure Protect Agent is installed on Windows client, you will see the following page.



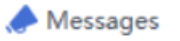
It can scan and remove the ransom virus, mining virus and Trojan on computers.

4.2 Protect Agent UI

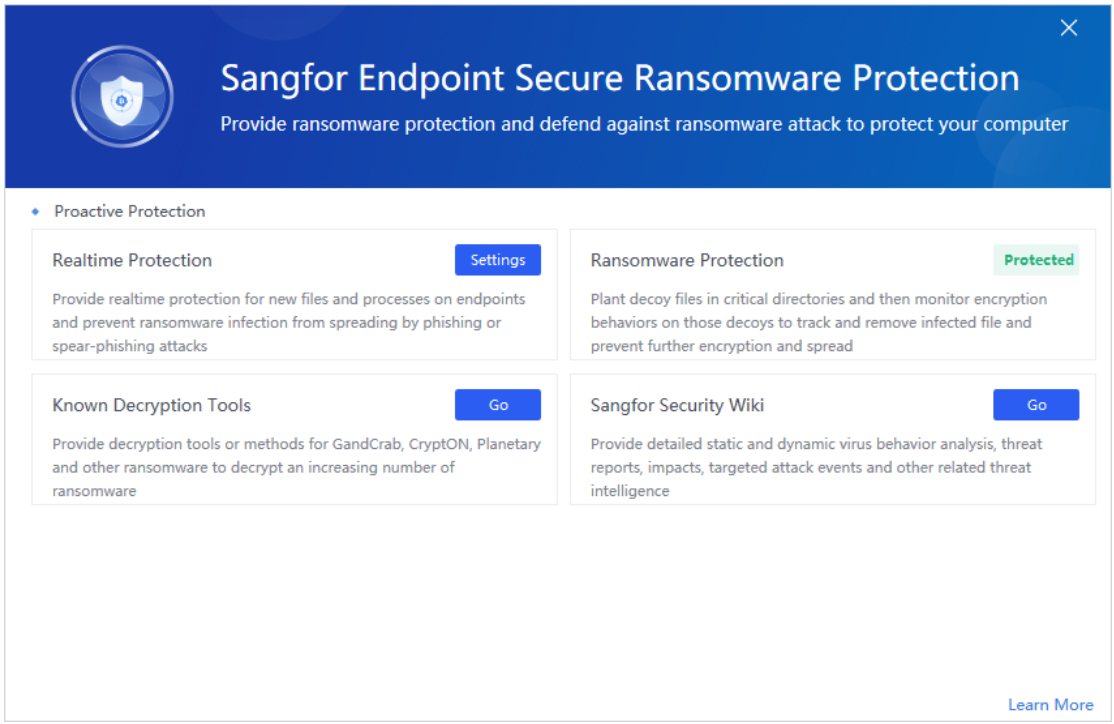


The top of the UI displays how long this endpoint has been protected and the status of the connection between endpoint the Manager. In the upper left corner, the green icon indicates that they are connected normally, and the gray icon indicates that the endpoint is disconnected from the Manager.

The Security section provides a quick entry point for virus detection, real-time protection, and protection trend over the past 30 days.

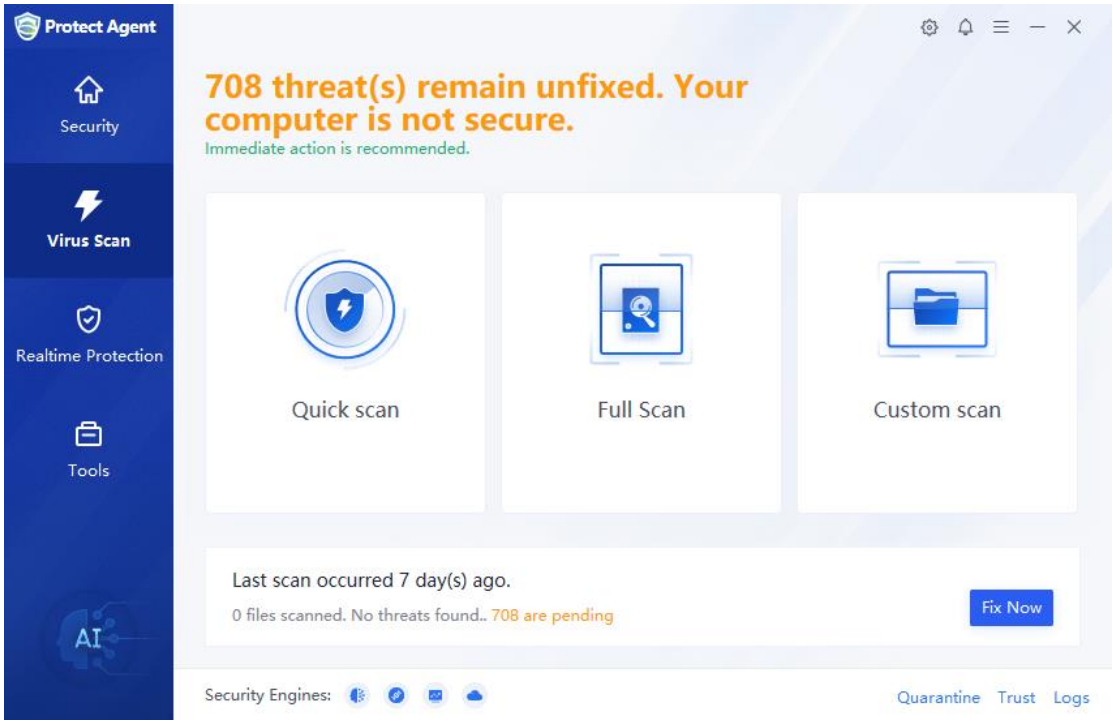
The  section lists recently received messages, such as virus database version updates, software version updates, and notifications issued by administrators.

Click at the lower right corner of the Security to enter the following page which shows capabilities of Endpoint Secure Protect Agent protection against ransomware, as shown below.


Sangfor Endpoint Secure Ransomware Protection
Provide ransomware protection and defend against ransomware attack to protect your computer
Proactive Protection
Realtime Protection
Settings
Provide realtime protection for new files and processes on endpoints and prevent ransomware infection from spreading by phishing or spear-phishing attacks
Ransomware Protection
Protected
Plant decoy files in critical directories and then monitor encryption behaviors on those decoys to track and remove infected file and prevent further encryption and spread
Known Decryption Tools
Go
Provide decryption tools or methods for GandCrab, CryptON, Planetary and other ransomware to decrypt an increasing number of ransomware
Sangfor Security Wiki
Go
Provide detailed static and dynamic virus behavior analysis, threat reports, impacts, targeted attack events and other related threat intelligence
Learn More

4.3 Virus Scan

The Virus Scan page provides scan feature for endpoints with three scan mode: full scan, custom scan, and offers Logs entry for users to view logs.



Quick Scan: scan critical directories on Windows system, such as /windows and /windows/system32 directories, /windows/system32/drivers directories and their subdirectories.

Full Scan: Scan all directories on Windows system.

Custom Scan: Scan specified files or directories.

The anti-virus engine can be viewed in the lower left corner of the Virus Scan page. The blue icon indicates that the engine is turned on, and the gray indicates that the engine is turned off. Hove the mouse over the engine icon, and you will see detailed engine description.

—— Name: Sangfor Engine Zero

This is an AI-based engine effective at detecting unknown ransomware and threats, and capable of perpetual self-learning and rapid updating.

——Name: Gene Analytic Engine

This is a traditional antivirus engine effective at detecting viruses based on family.

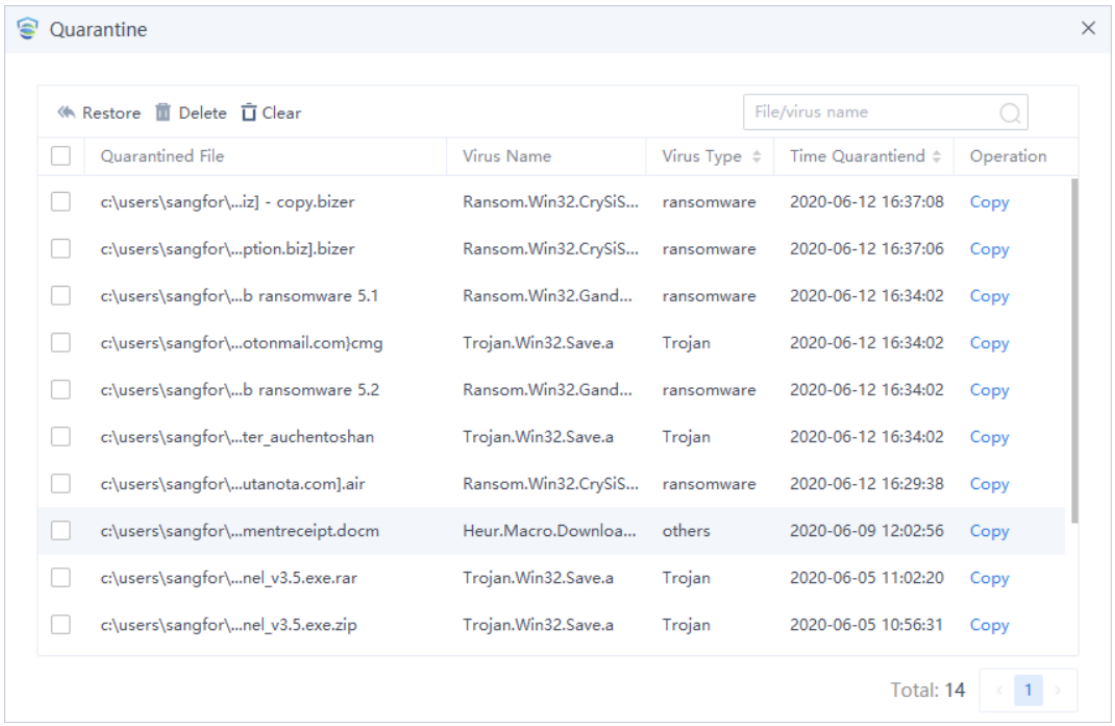
——Name: Behavior Analytic Engine

This engine is effective at detecting unknown virus variants by running them in virtual environments

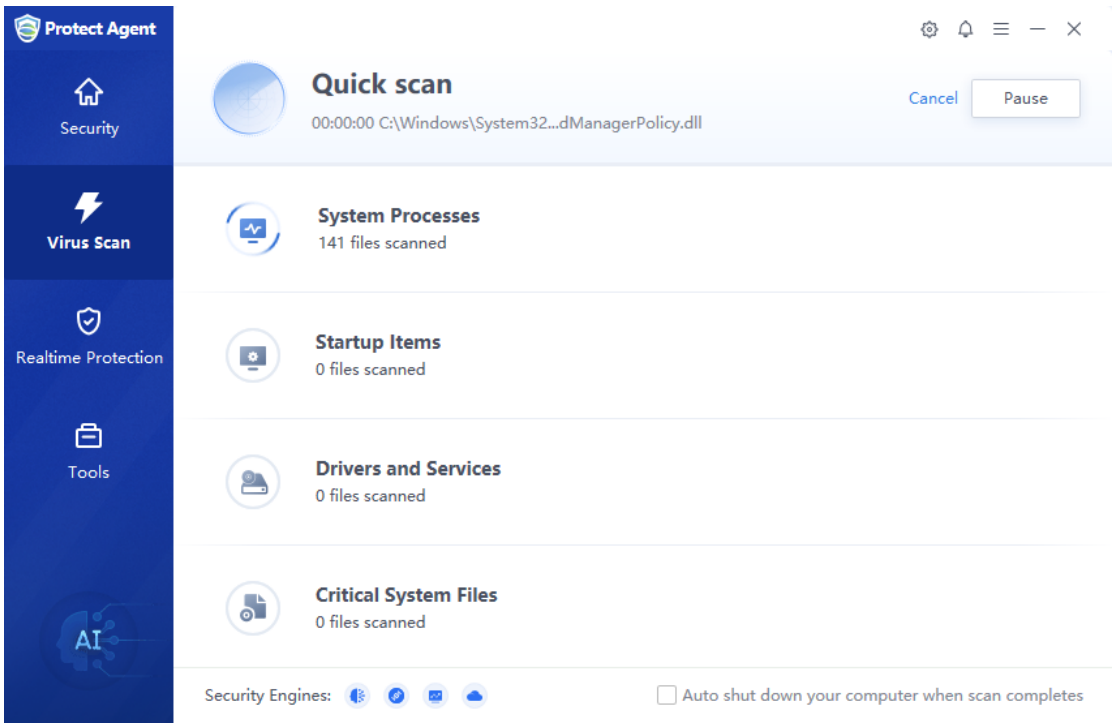
——Name: Cloud Based Engine

This engine integrates multiple cloud-based detection engines and antivirus databases.

In the lower right corner of the virus scan page, you can click Quarantine Trust Logs to view the files in the Quarantine and Trust, and view logs. on the Quarantine page, you can restore, completely delete, or clear quarantined files with one click, as shown below:

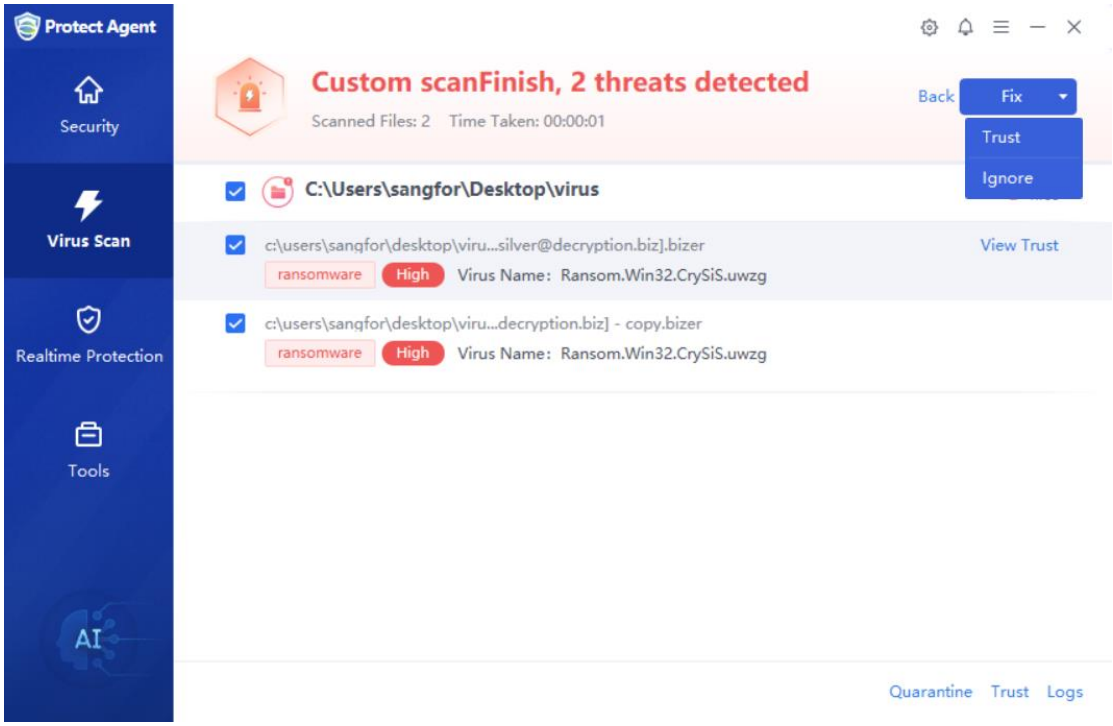


Click to start quick scan to scan the key directories on the system, as shown below.



Select at bottom right corner of the scan page. It is suitable for the scenario that virus scan is turned on before off hours and endpoints needs to be shut down after scan completes.

The discovered threat files can be fixed by clicking Trust or Ignore. You can also Click View to see details, as shown below.

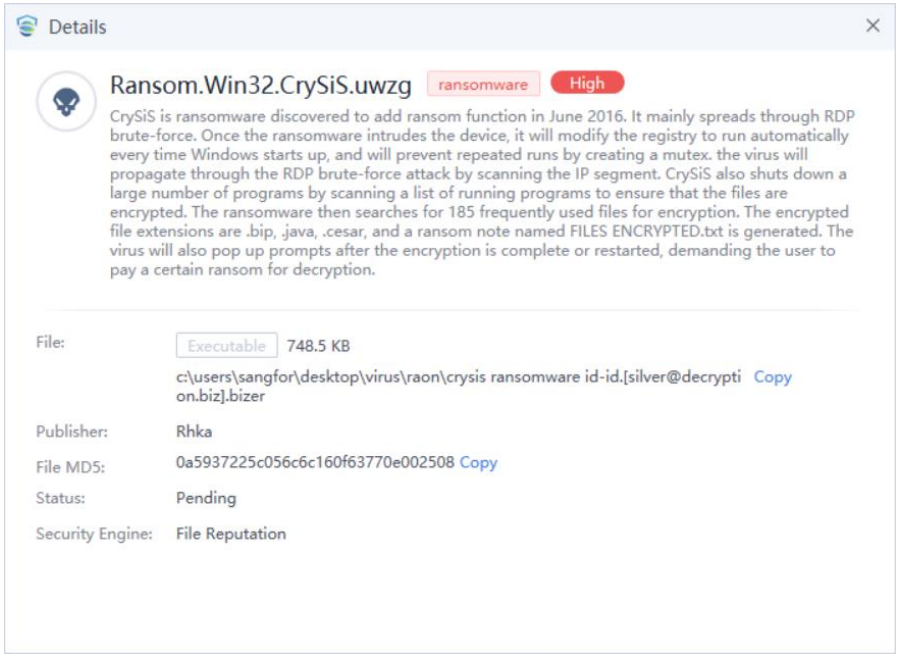


Fix: Fix the virus files found. For a macro virus or an infectious virus file, try to repair it first. The quarantined files can be viewed in the "Quarantine".

Trust: If the discovered threat file is considered secure, you may click Trust. Trusted files can be viewed in the "Trust".

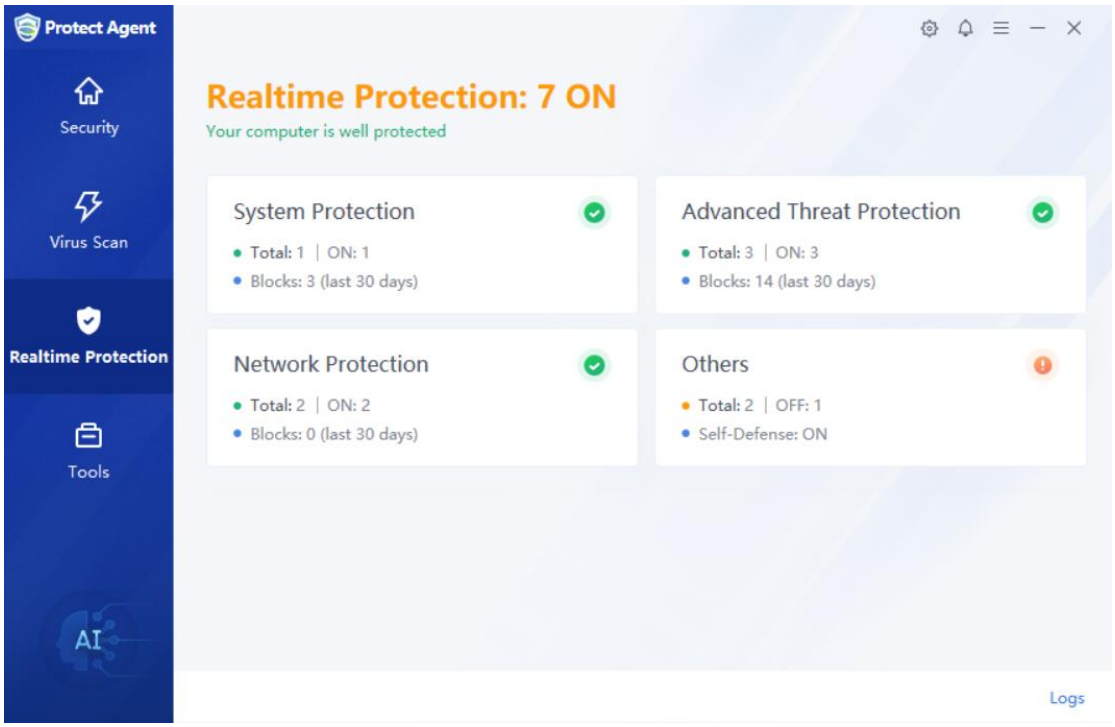
Ignore: Ignore threat files.

View: Click it to view the detailed information of a threat file, as shown below.

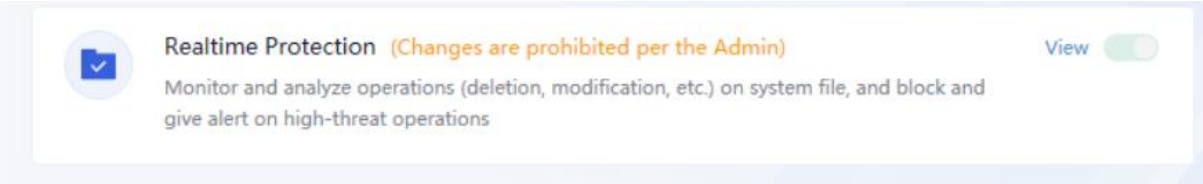


4.4 Realtime Protection

Real-time protection includes system protection, advanced threat protection, network protection and other protection. The Realtime Protection page shows status of each protection feature, as shown below:

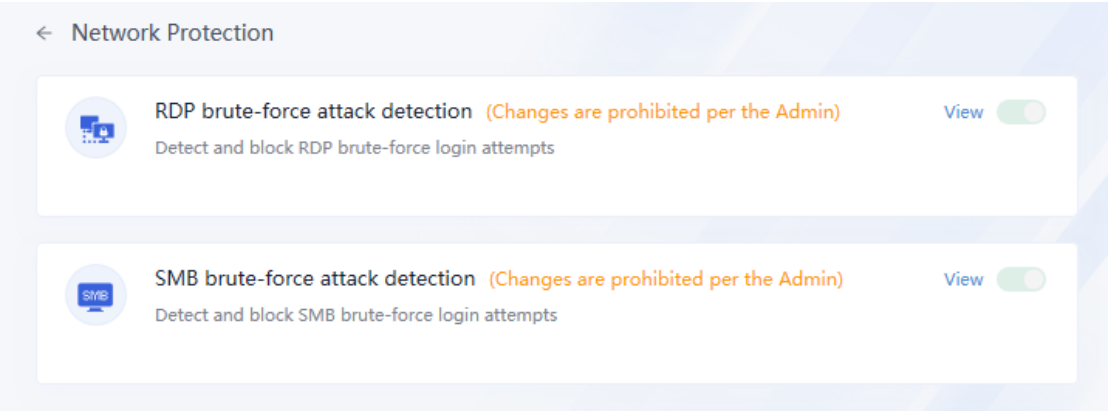


Click on System Protection to view details. System protection includes Realtime file protection. Endpoint Secure Manager administrator can configure to allow or not allow end users to change Agent settings. If the administrator does not allow the end users to modify the configuration, the message “Changes are prohibited per the Admin” will appear, as shown below.

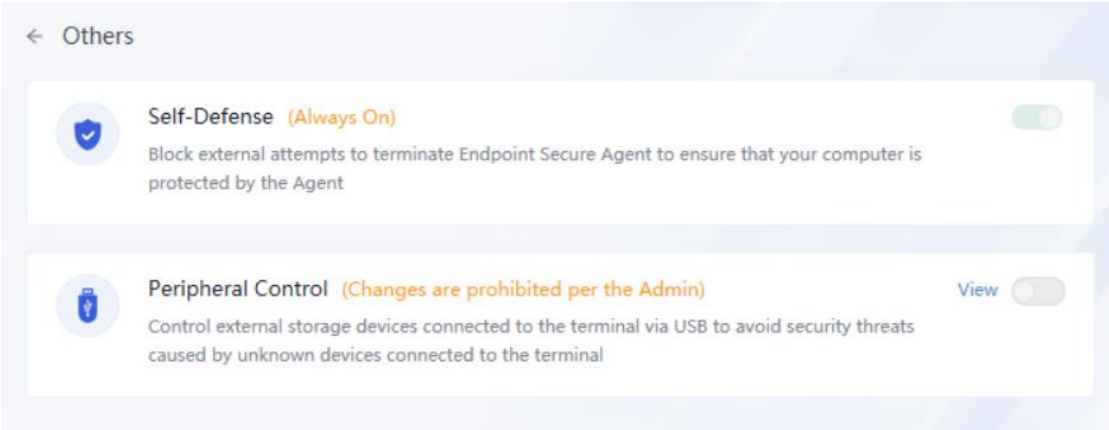


Click on Advanced Threat Protection to enter the following page., which provides Ransomware Protection, Fileless Attack Protection, and Stubborn Malware Protection, as shown below:

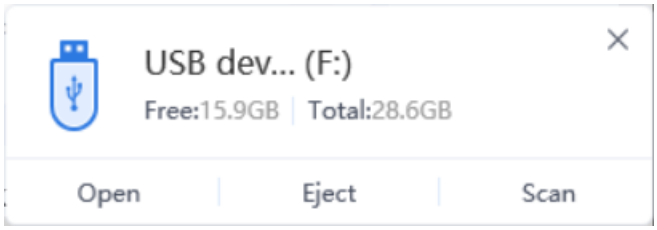
Click on Network Protection to view details. Network Protection includes RDP brute-force attack protection and SMB brute-force attack protection, as shown below:



Click on Others to view other protection details, including Self-Defense and Peripheral Control, as shown below.

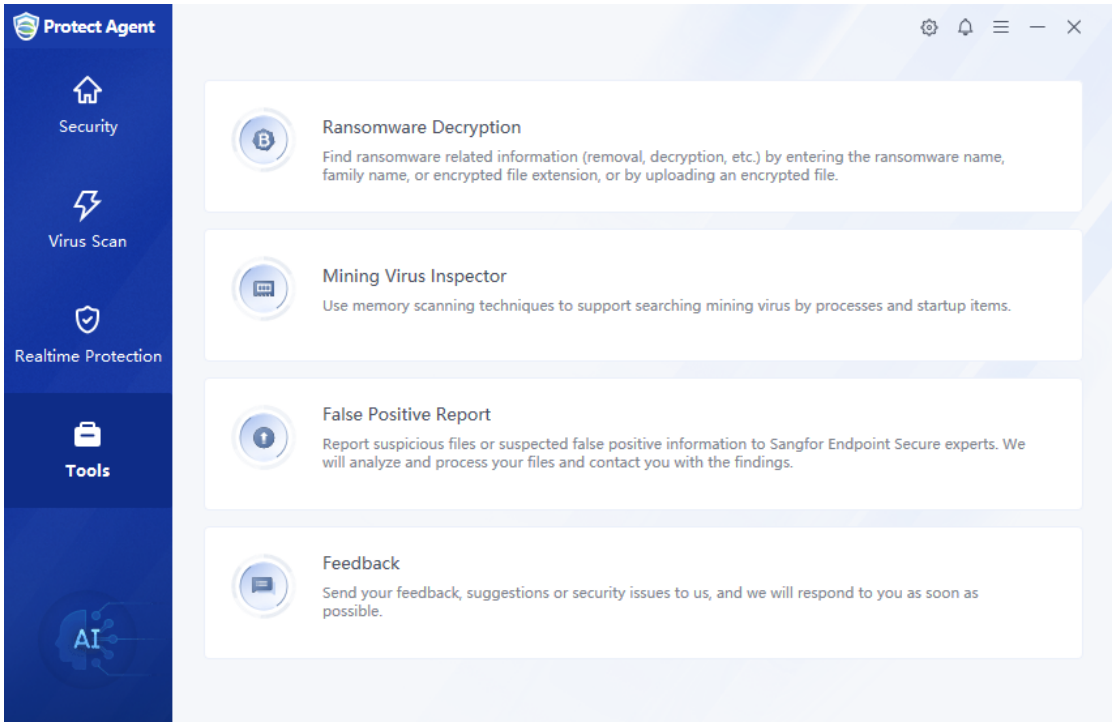


Peripheral Control is enabled by default. When a USB device is inserted into the endpoint, a message will pop up in the lower right corner, as shown below. You can open, eject the USB device, or perform virus scan on it.



4.5 Tools

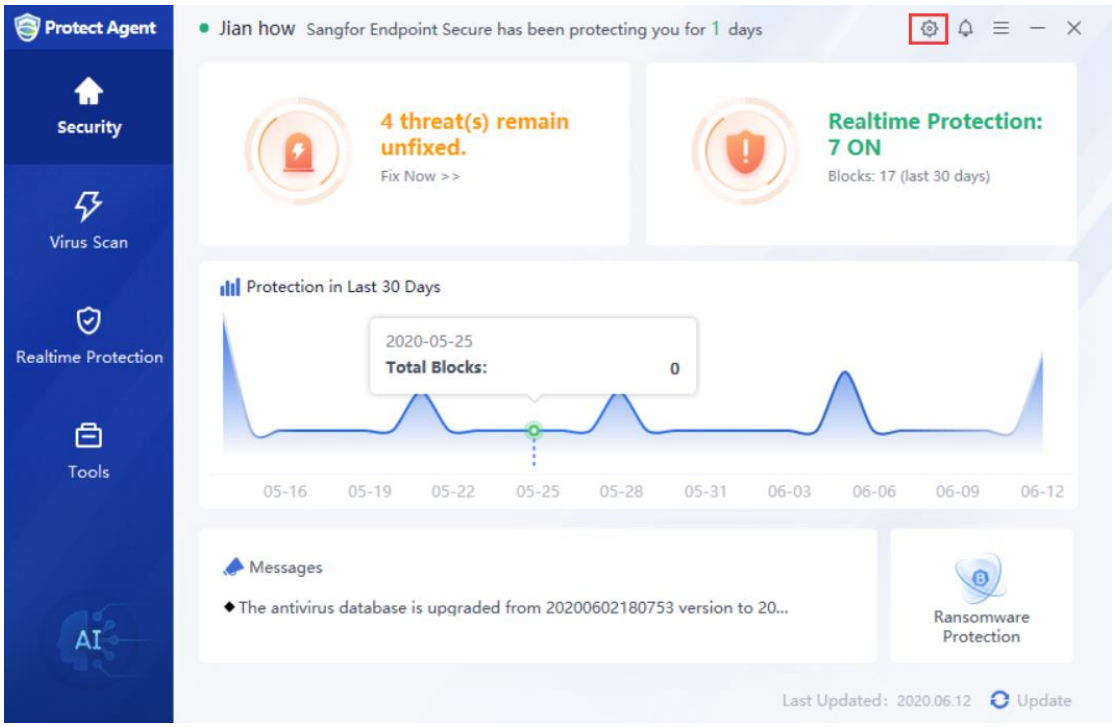
System tools include Ransomware Decryption, Mining Virus Inspector, False Positive Report, and Feedback.

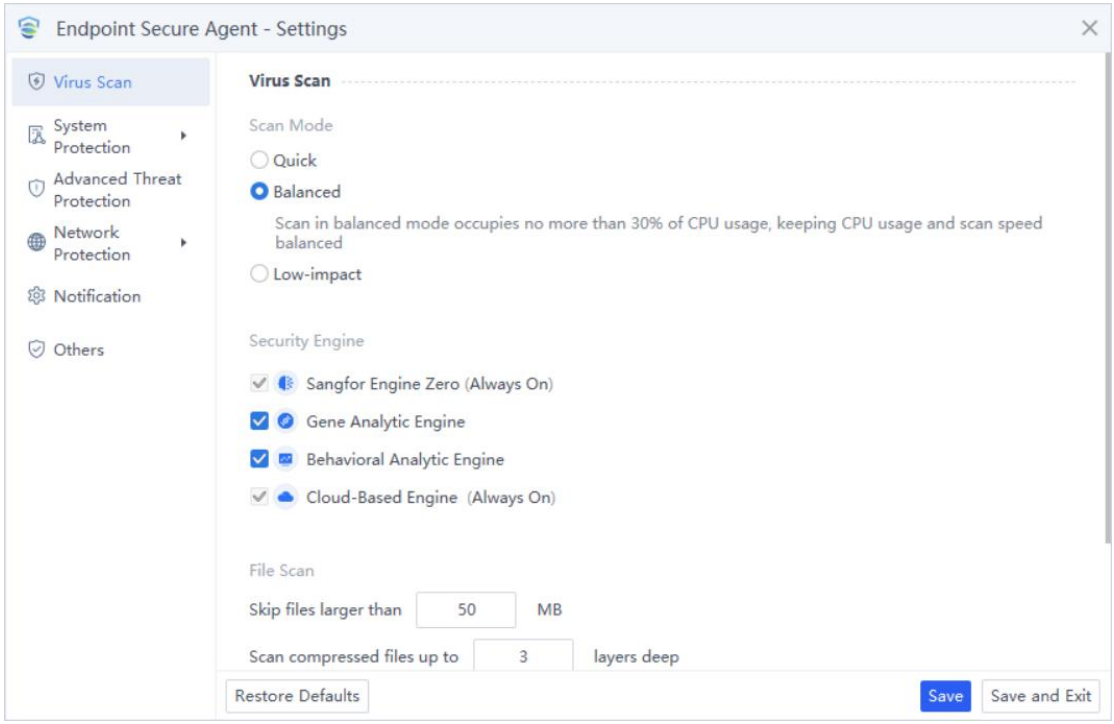


Ransomware Decryption: When a server is encrypted by ransomware, you use ransomware decryption tool to query the ransomware information and check whether there is decryption by providing characteristics of the ransomware, such as the encrypted file suffix and ransomware information.

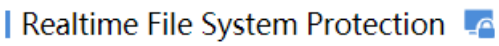
4.6 Settings

Click on the icon  in the upper right corner of the client to enter the Setting, as shown below:

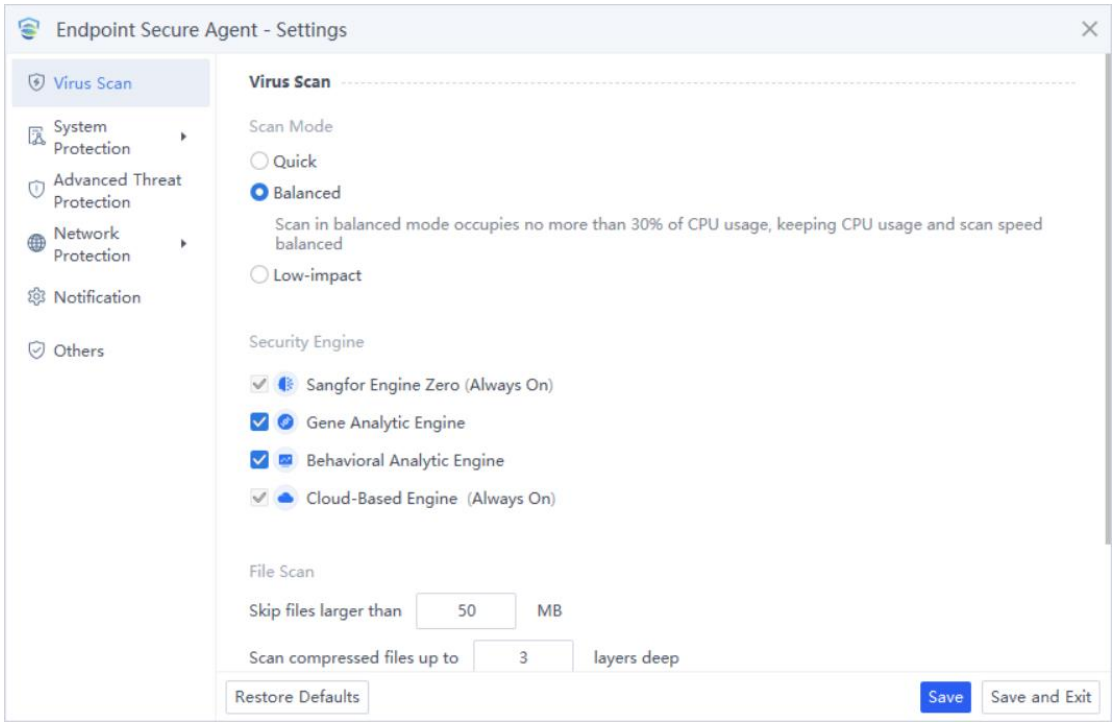




On the above page, there are the following tabs: Virus Scan, System Protection, Advanced Threat Protection, Network Protection, Notifications, and Others. Each function has the same configuration items on the Manager except the notification settings, and the administrator

can reclaim the configuration permissions of the Agent. There is a lock icon on the right side of each function in Endpoints > Security Protection on the Manger. For example, on the Manager, 

this indicates end users are not allowed to change this function settings on endpoints. When the lock icon is grayed, this means end users can change the settings on endpoints.



Virus Scan: This includes CPU Usage, Security Engine, File Scan and Action.

For CPU Usage, you can choose High, Balanced, or Low.

High: This consumes the most CPU resources but scan speed is faster.

Balanced: This consumes no more than 30% CPU resources, balancing CPU usage and scan speed.

Low: This consumes no more than 10% CPU resources,but scan speed is slow.

Security Engine Refer to chapter 4.3 for introduction.

File Scan Define the size of the scanned file and the maximum compression level of the scanned file (the maximum is 10).

Action Set the action on discovered threat files. It has the following options: Standard, Enhanced and No Action- Report Only.

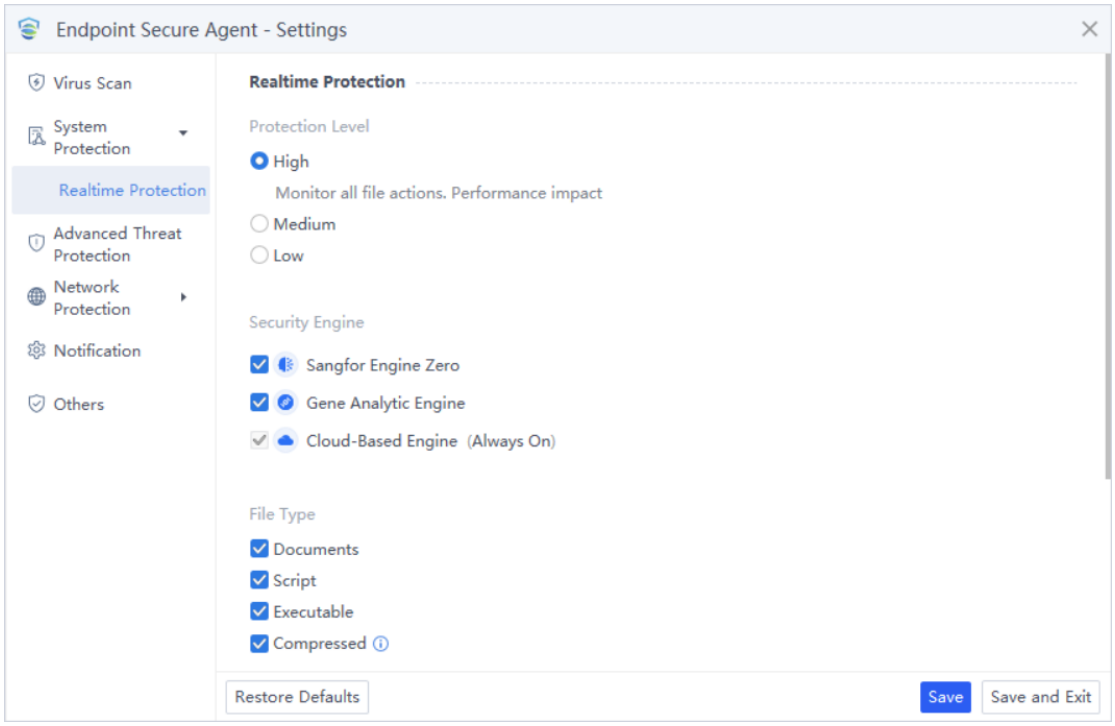
Standard: Automatically fix or quarantine malicious files based on default virus detection s ettings. You can also deal with infected files manually, and manually recover files from Qua rantine. Sangfor Endpoint Secure continuously updates to enhance protection against evolv ing threats.

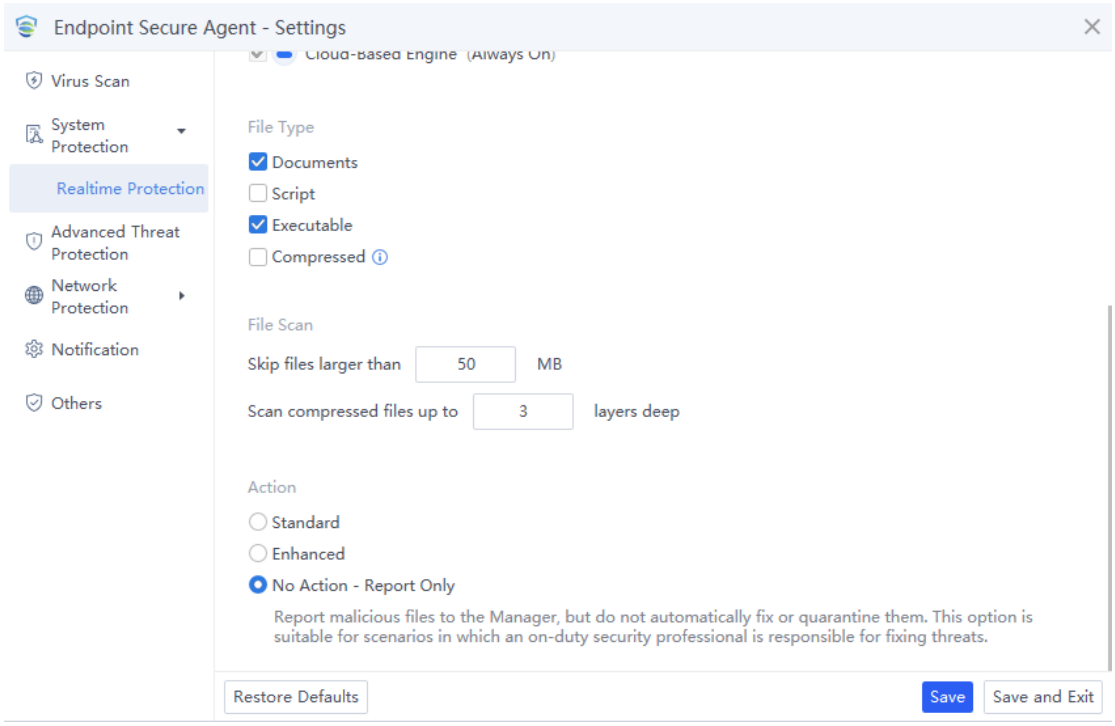
Enhanced: Fix or quarantine all malicious files automatically. You can manually restore fil es from Quarantine. This option is suitable for Enhanced Protection scenarios.

No Action-Report Only: Report malicious files to the Manager, but do not automatically fix or quarantine them. This option is suitable for scenarios in which an on-duty security professional is responsible for fixing threats.

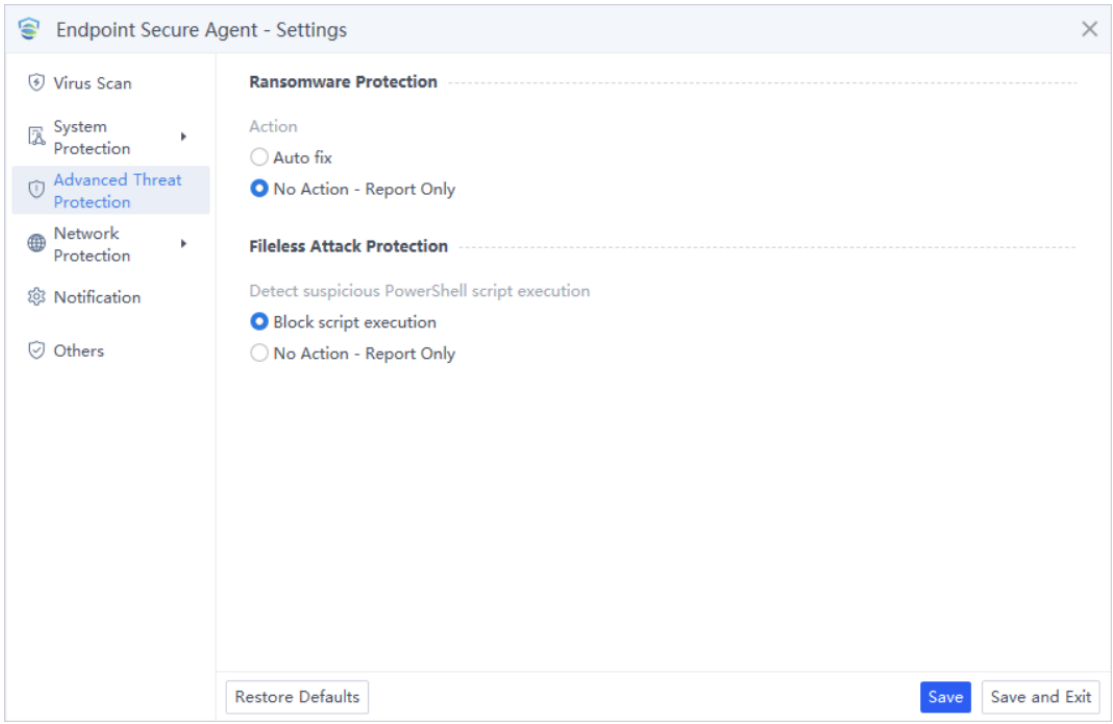
Click **Save** to save the current page configuration and then users can continue to go to other tabs under Settings for configuration.

Click **Save and Exit** to save the current page configuration and exit the Settings window.

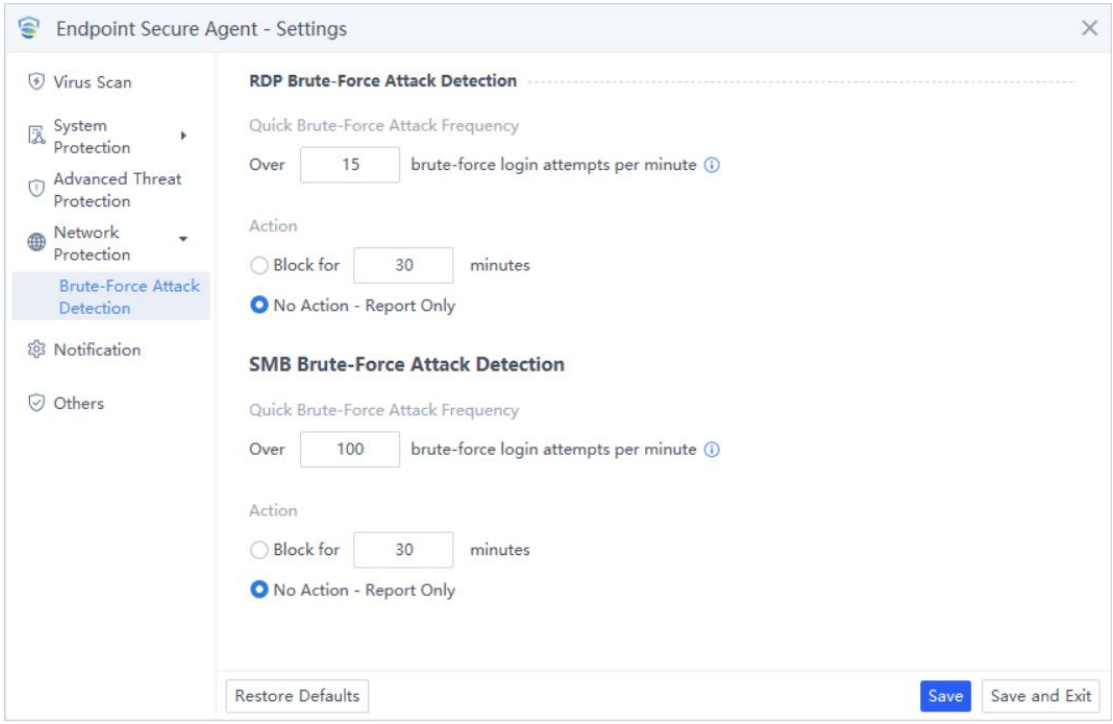




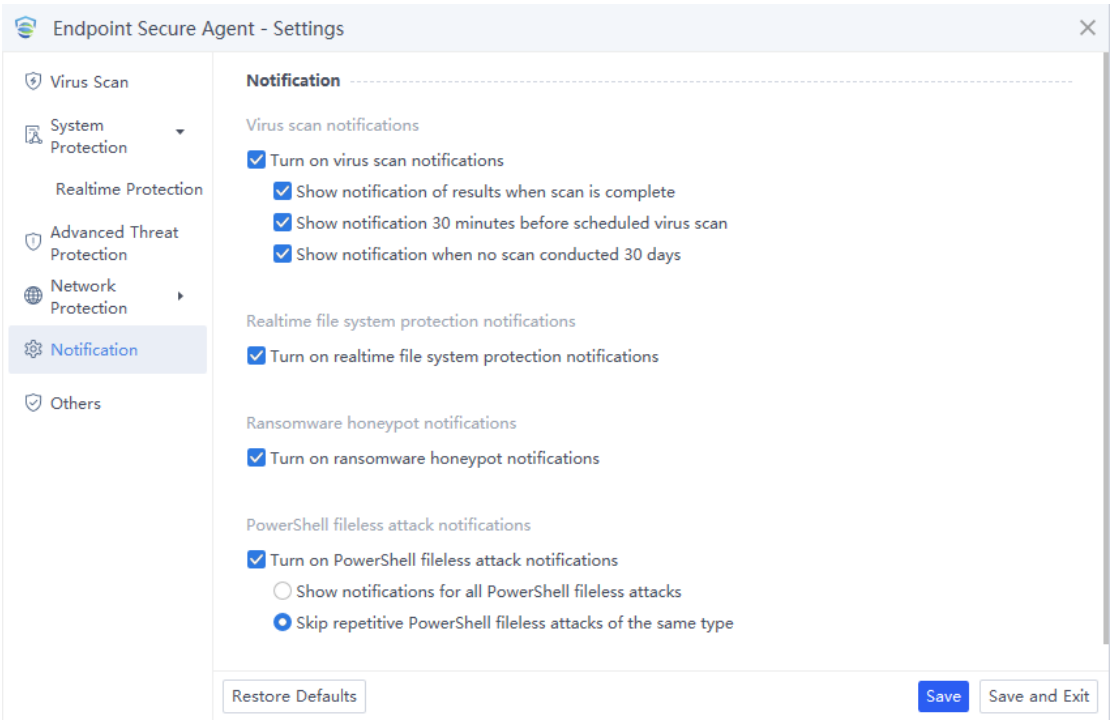
System Protection: The system protection sets the protection level, security engine, file type, scanned file, and action of real-time protection. The settings are consistent with the realtime protection settings on the Manager. For details, please refer to the "3.3.3.3 Realtime Protection" chapter.



Advanced Threat Protection: Advanced threat protection settings include Ransomware Protection and Fileless Attack Protection. The settings of the two functions are consistent with that of the corresponding feature on the Manager. For details, refer to the "3.3.3.3 Realtime Protection" chapter.



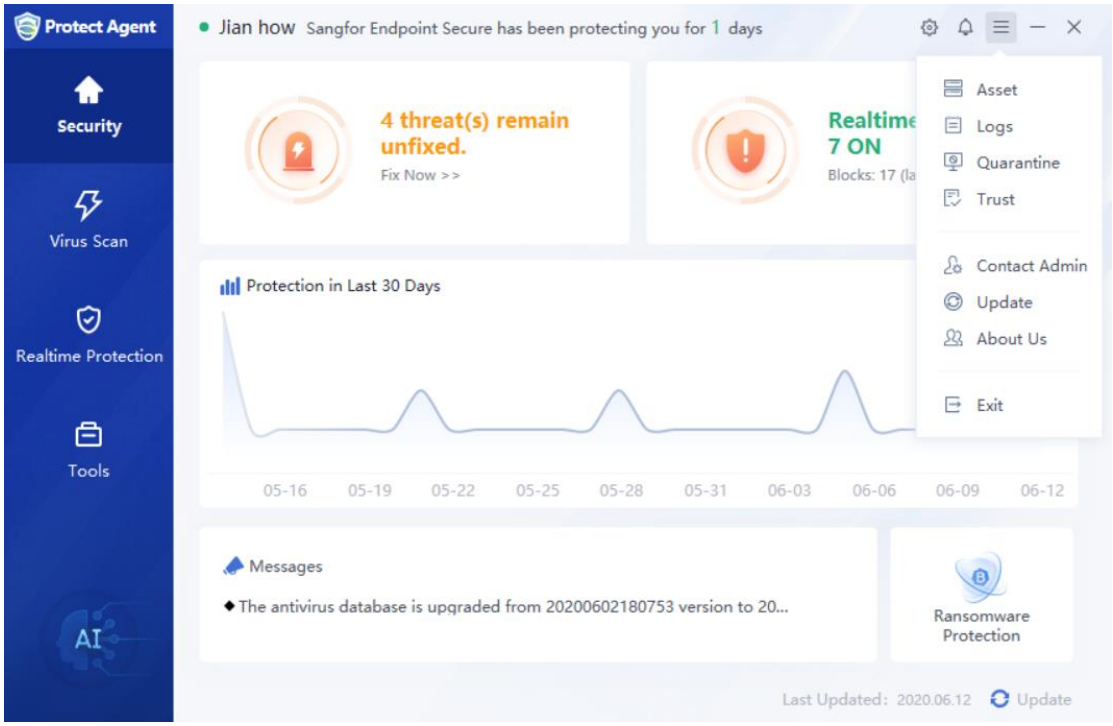
Network Protection: Network protection settings include RDP brute force detection and SMB brute force detection settings. The setting of each parameter is consistent with the setting method of brute force crack detection on the management platform. For details, please refer to the "3.3.3.3 Real-time Protection" chapter.

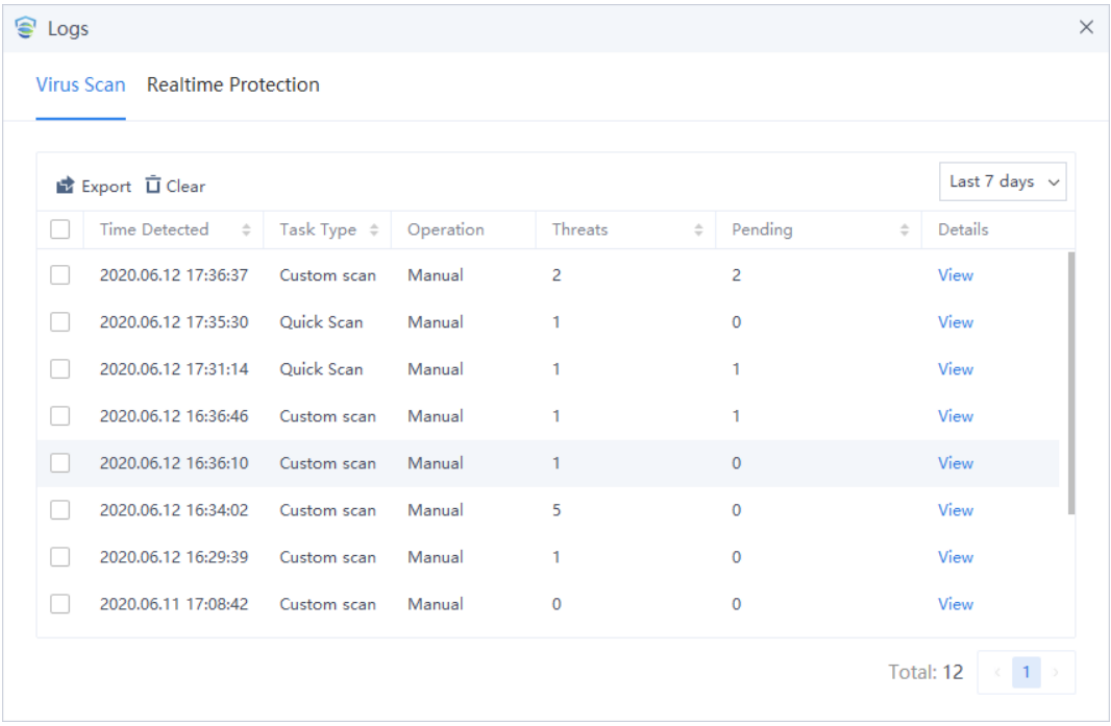


Notification: This tab notification settings include virus scan notification settings, realtime protection notification settings, ransomware honeypot notification settings and PowerShell fileless attack protection notification settings. Users can configure whether to allow notifications according to actual needs.

4.7 Logs

Click the icon  in the upper right corner of the Agent page to view logs, as shown below.





Security logs include virus scan logs and realtime protection logs.

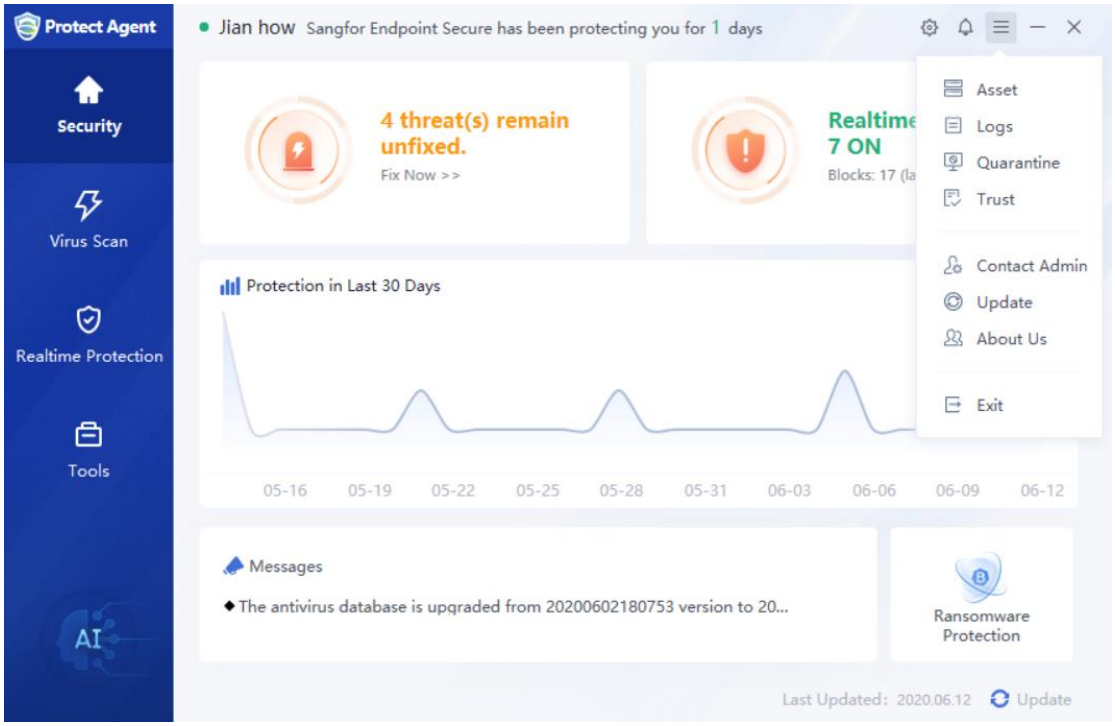
Reatime protection log is a security log generated when a threat file is detected after realtime file protection is enabled.

The virus scan log refers to the records of operationsthat trigger virus scan. Click View to view the details of the virus scan, as shown below.

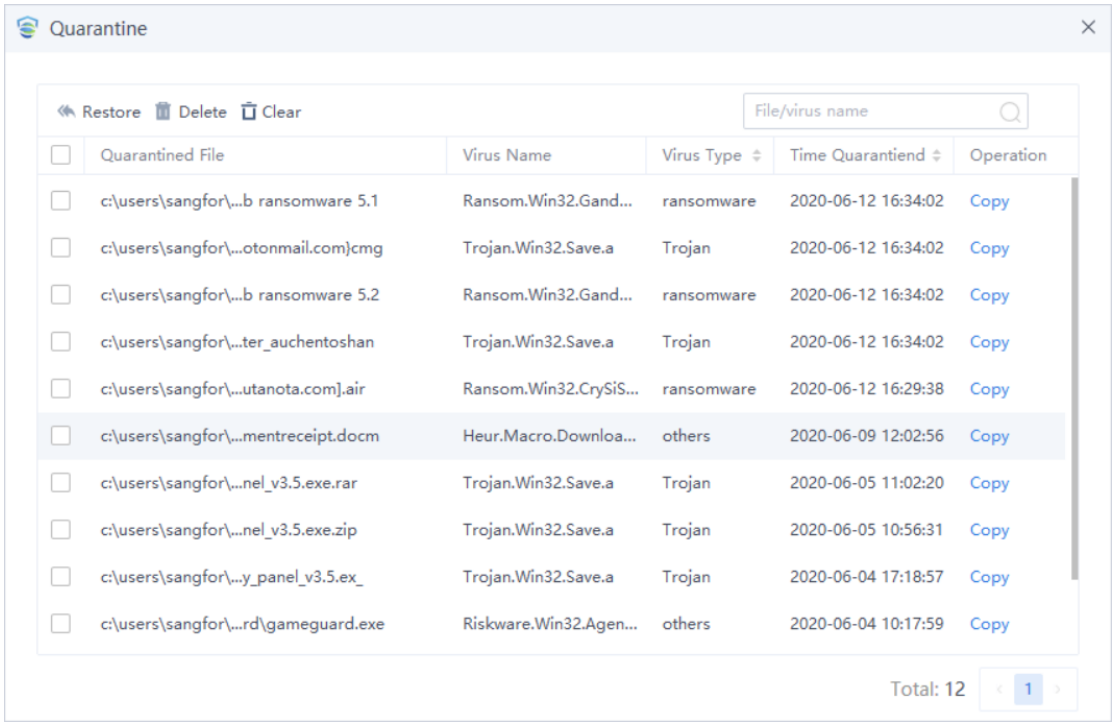
4.8 Quarantine/Trust

When Endpoint Secure detects a threat file, it will quarantine it and move the file to the Quarantine. The file or process that has been misreported can be added to the Trust, and the files in the Trust will be skipped from virus scan and file Realtime monitoring.

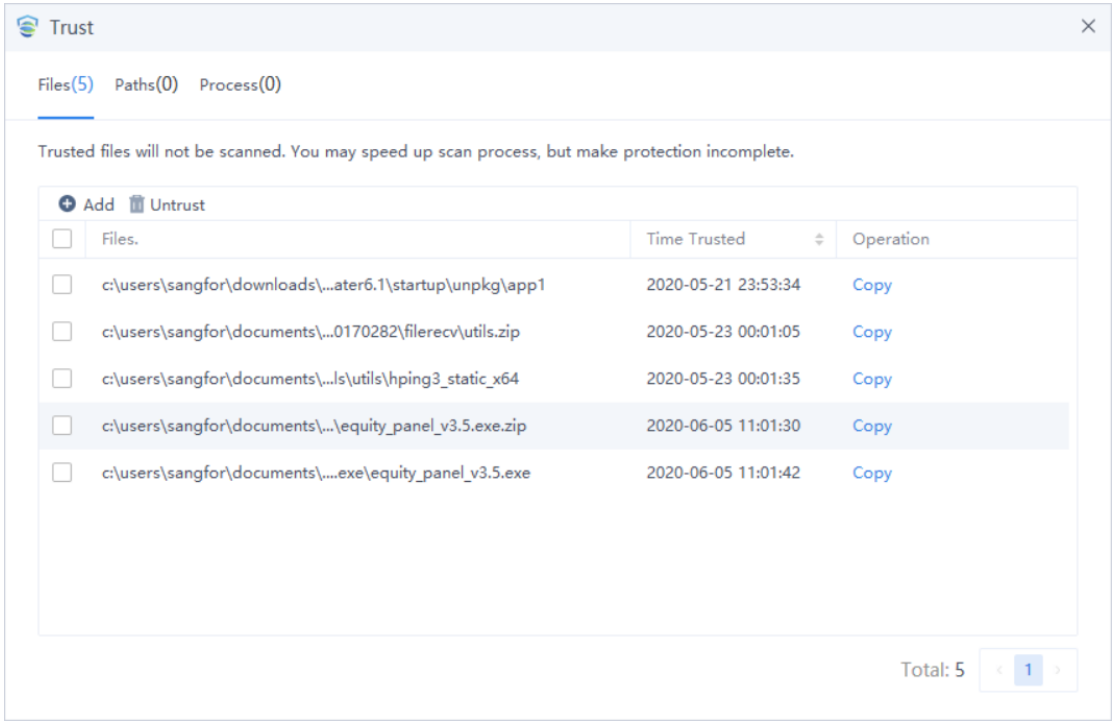
Click the icon ☰ in the upper right corner to view the page, as shown below.



Click Quarantine to enter the following page. The files in the Quarantine can be restored, completely deleted, or cleared with one click, as shown below.

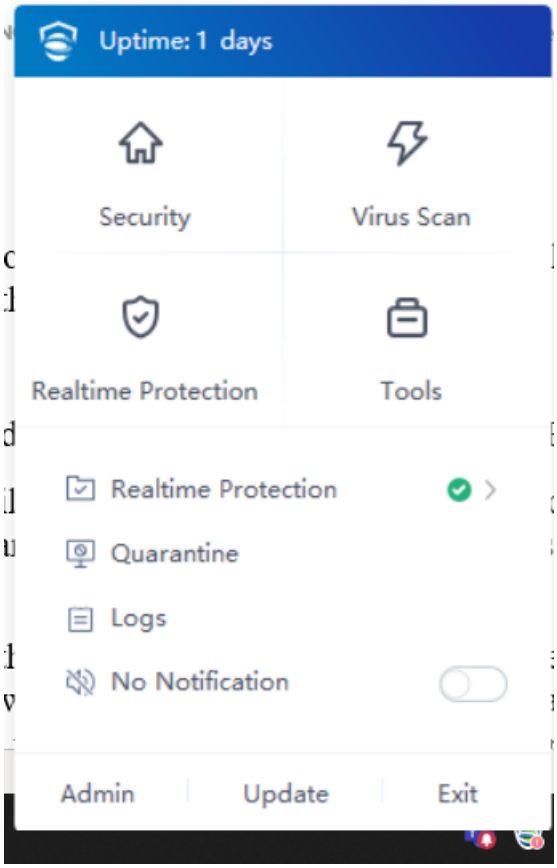


The Trust page lists all the trusted files, paths, and processes., You can trust any files, directories, and processes, as shown in the following figure.



4.9 Agent Tray

You can perform some operations quickly through Endpoint Secure Protect Agent tray in the lower right corner of the system. Right-click on the Agent icon and you will see the following page, as shown below:

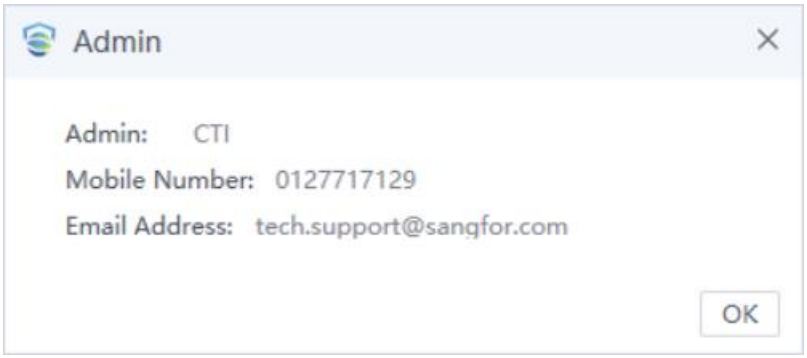


Uptime: Shows how long Endpoint Secure Protect Agent has protected the endpoints.

The Security, Virus Scan, Realtime Protection, Tools, Quarantine, and Logs are all quick entries to the functions provided.

No Notification: When it is enabled, the Endpoint Secure Protect Agent detects a threat file and will not prompt a notification. This function can be individually configured by the customer or by the Manager administrator.

Admin: Click to view administrator information. When needing assistance in using Endpoint Secure Protect Agent, the user can get contact with the administrator quickly.



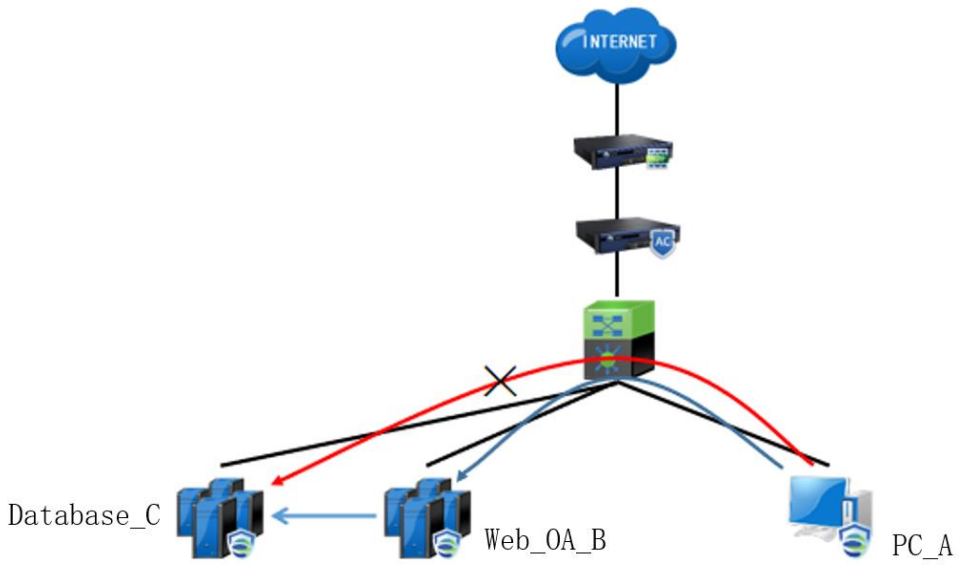
The administrator information can be set on the Manager. For details, please refer to the "3.3.3.1 Basic Policy" chapter.

Chapter 5 Appendix

5.1 Appendix 1: Micro-Segmentation Scenario

5.1.1 Scenario 1

In a daily office scenario, a working endpoint has access to OA web server, the web server can access the database, and the working endpoint has no access to the database server.



Description:

PC (endpoint A, with or without the Agent), Web server (endpoint B) and database server (endpoint C, with the Agent installed and can communicate with MGR)

Network connection among endpoints A, B, and C (you can use the ping command to verify)

Expected Results:

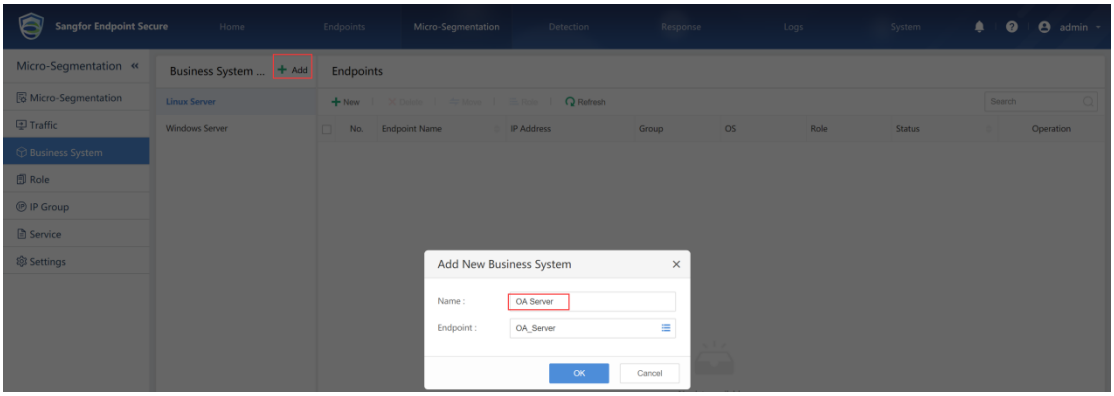
The PC (endpoint A) can access port 80 of WEB_OA _B and cannot access other ports.

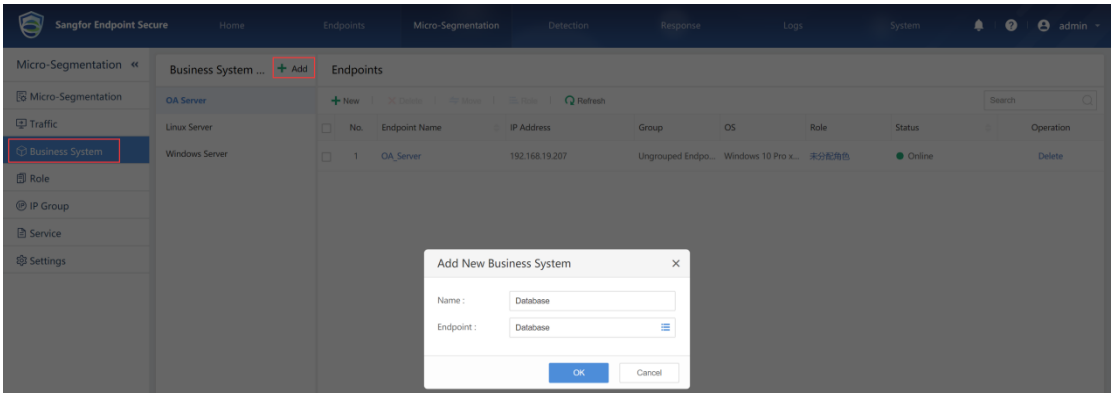
The PC (endpoint A) cannot access database Database_C (endpoint C).

WEB_OA_B can access port 3306 of database Database_C and cannot access other ports.

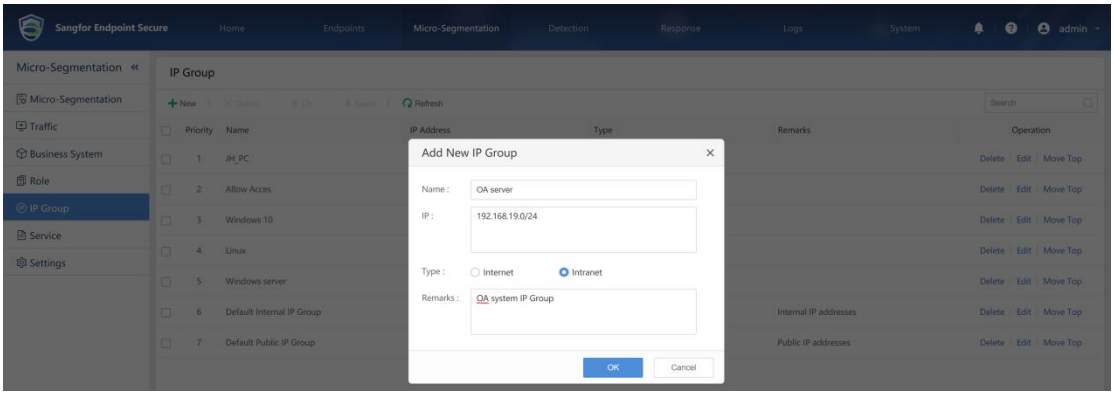
Configuration Steps:

- Log in to the Endpoint Secure Manager, go to **Micro-Segmentation > Business Systems**, click Add to create a new business system, and add the web OA server to the OA server group. Add the database server to the database server system.

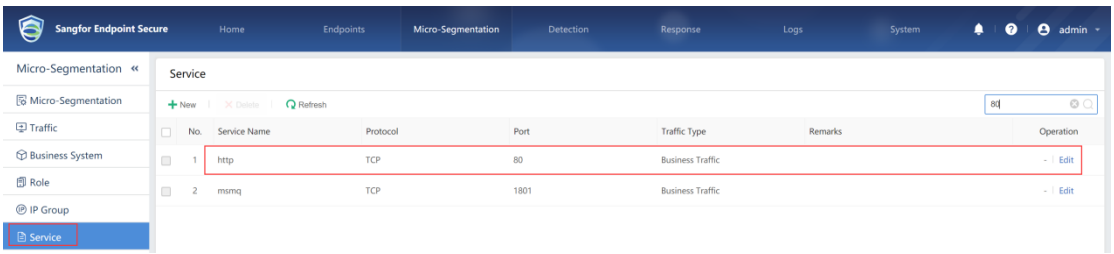




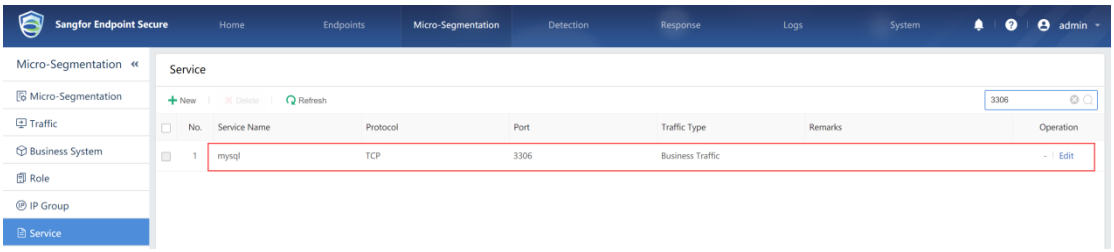
- Go to **Micro-Segmentation** > **IP Groups,** and configure the IP range that can access the web server in the office endpoint. The name is OA system. Note that this IP range should include the IP address of endpoint A. Select Intranet.



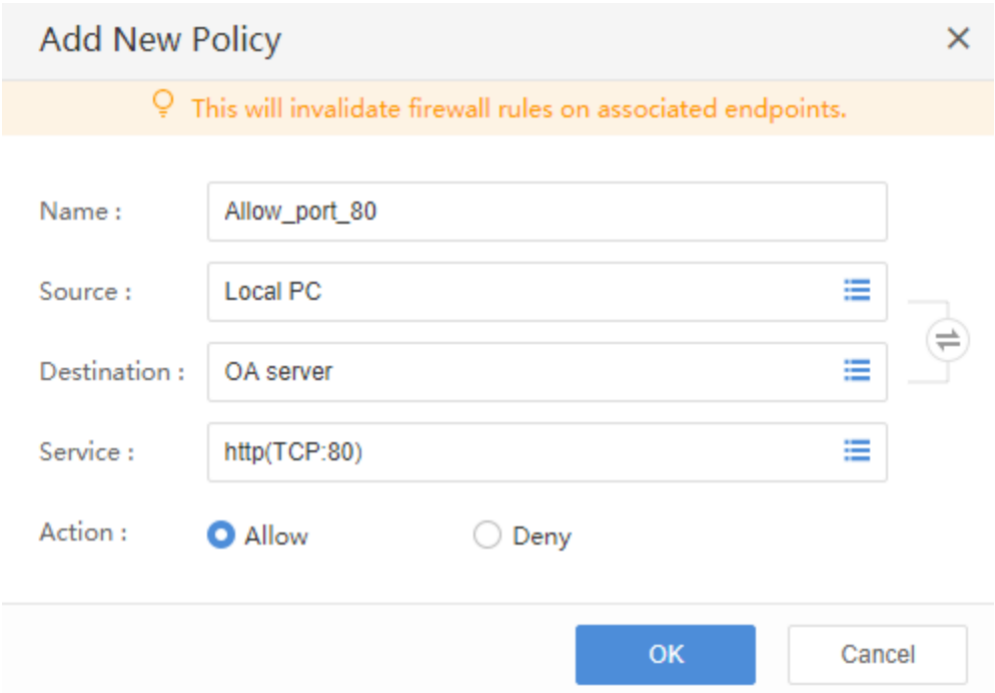
- Go to **Micro-Segmentation** > **Services** to see that port 80 of the web server is a built-in service.



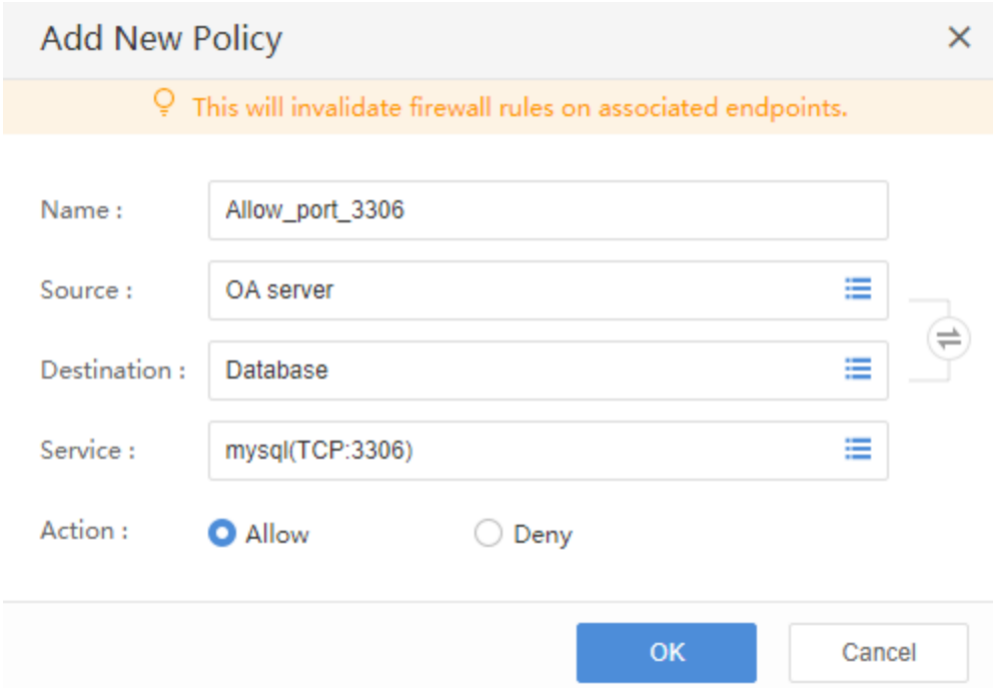
- The mysql database uses the 3306 port as a test built-in port.



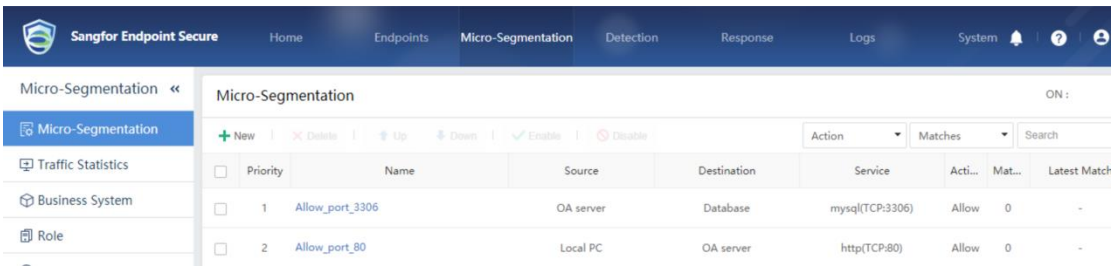
- Configure **Micro-segmentation policy** to use the above configuration items. The office endpoint has access to the OA's web server.



- The OA server has access to port 3306 of the database server.



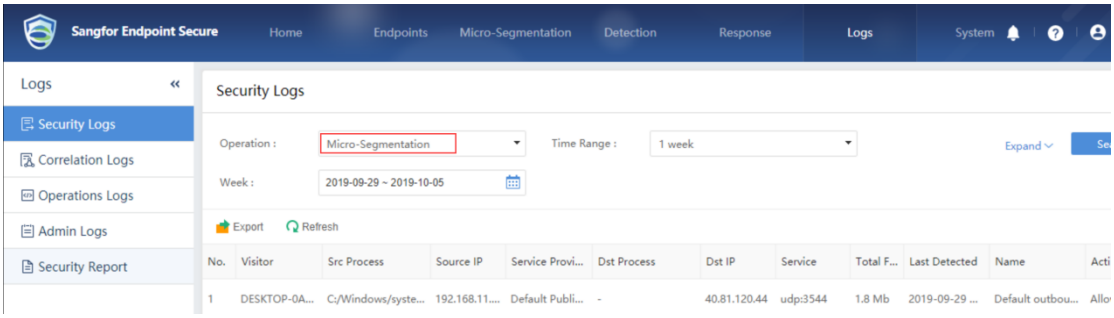
- View the policy distribution to endpoints.



Policy-matching priority: newly-added allow policy > newly-added deny policy > default policy

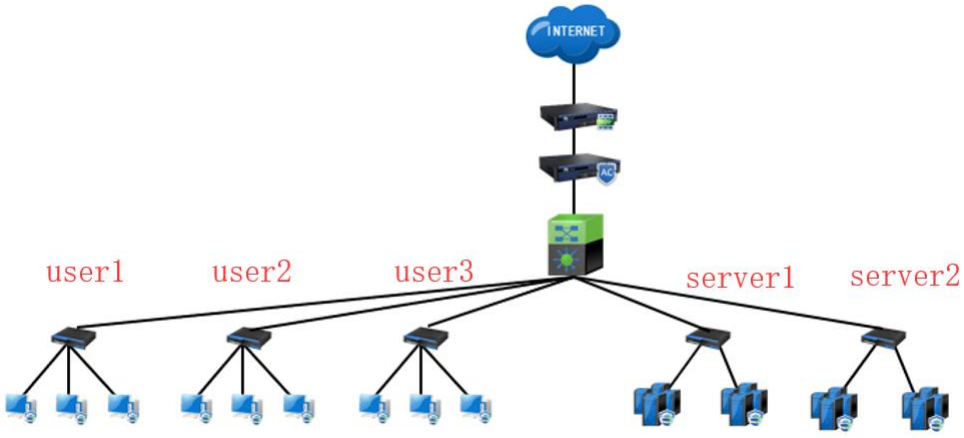
- Check the access status of the PC (Endpoint A) to Port 80 of Web server (Endpoint B), and try to access the Webpage of endpoint B (you can also open the command line on the PC (endpoint A), use the telnet command, for example, enter telnet 172.16.xxx.xxx 80).
- Check the access status of the PC (endpoint A) to the other ports (any port) of Web server (endpoint B).
- Check the access status of Web server (endpoint B) to port 3306 of database server (endpoint C). (Windows-> Linux, Windows-> Windows: You can also use the telnet command on the Windows server, enter telnet 172.16.xxx.xxx (IP address of endpoint B) 3306. Linux-> Linux: In the case that both are Linux servers, endpoint C first uses the nc command nc -l 3306 to listen to the port. Endpoint B uses the nc command ***nc IP address port.*** Then endpoint B can enter the information on the command line page and press Enter to see if endpoint C receives it.
- Check the access status of the PC (endpoint A) to 3306 port of the database server (endpoint C).

- Go to **Logs** > **Security Logs**. Select Micro-Segmentation in Log Type to view the micro-segmentation log.



5.1.2 Scenario 2

When ransomware spreads, the shared ports and the remote desktop ports of all endpoints can be blocked by micro-segmentation, preventing the ransomware from spreading.



Description:

When there is a ransomware in the user zone, the ransomware will spread via Port 135, 136, 137, 139, 445 and 3389. When it is not possible to remove it immediately, you can use micro-segmentation to block the ports of all the endpoints (PCs, servers). Confirm which servers need to use Port 3389 to perform remote login or use the sharing function in advance. If necessary, you can configure allowing policy to allow the specific endpoints to access.

Expected Results:

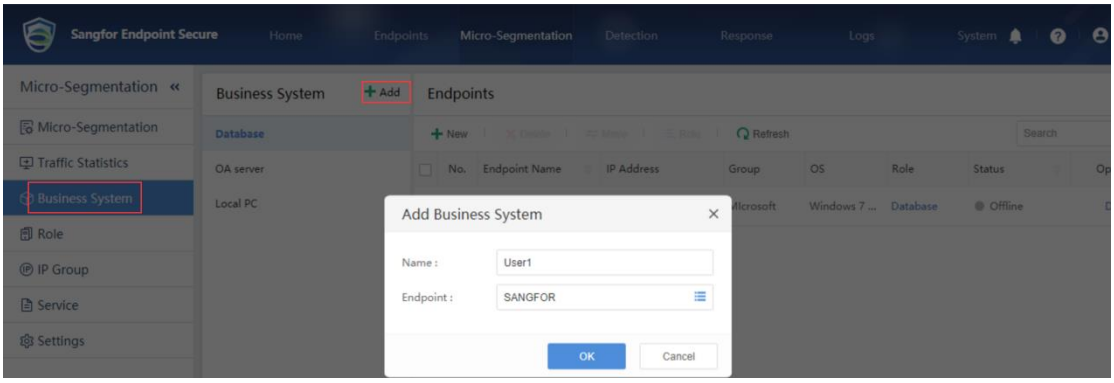
1. All the endpoints cannot access each other's sharing service port or remote desktop port.

2. Only a few endpoints that need to use the shared services can access the sharing service port or remote desktop port.

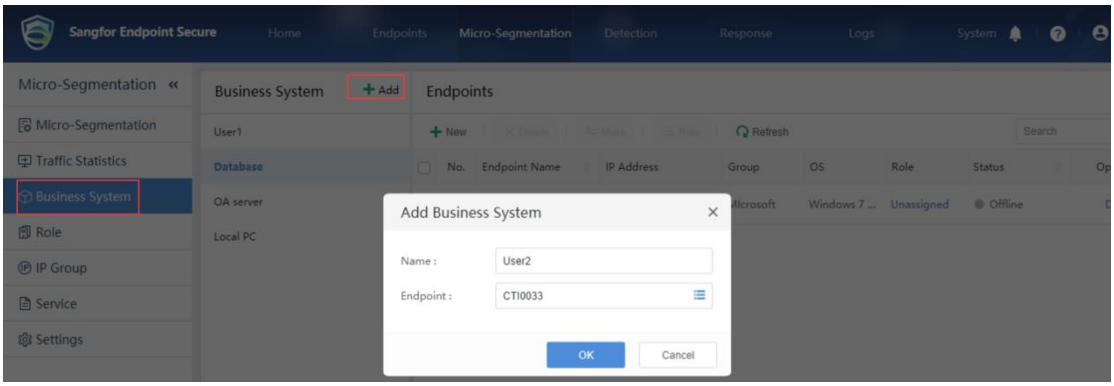
Configuration Steps:

- Assign all the endpoints to the corresponding business system zones. As shown in the above figure, there are three user zones and two server zones.

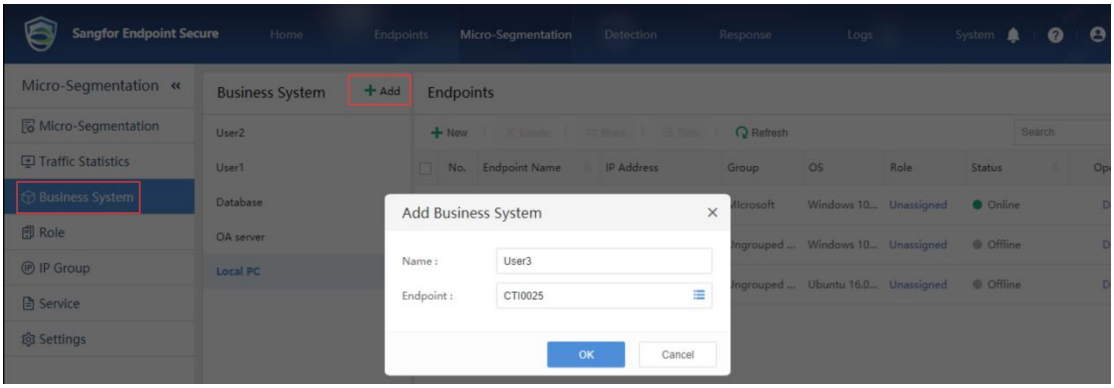
  User zone 1



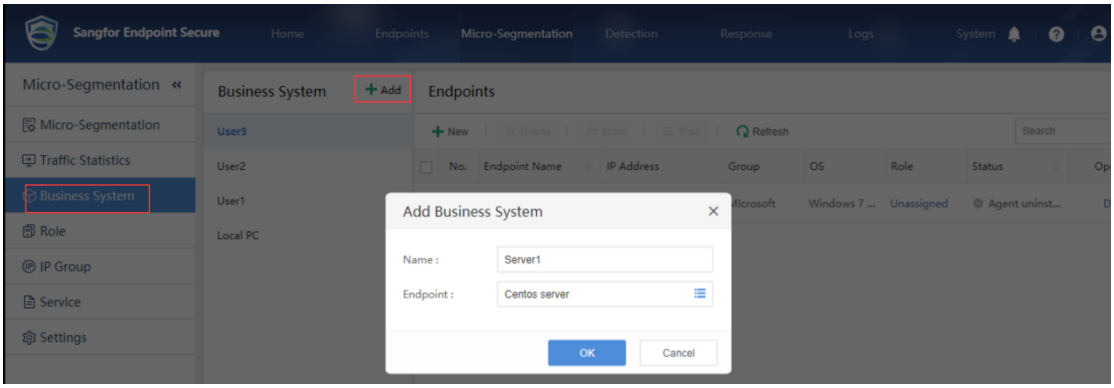
  User zone 2



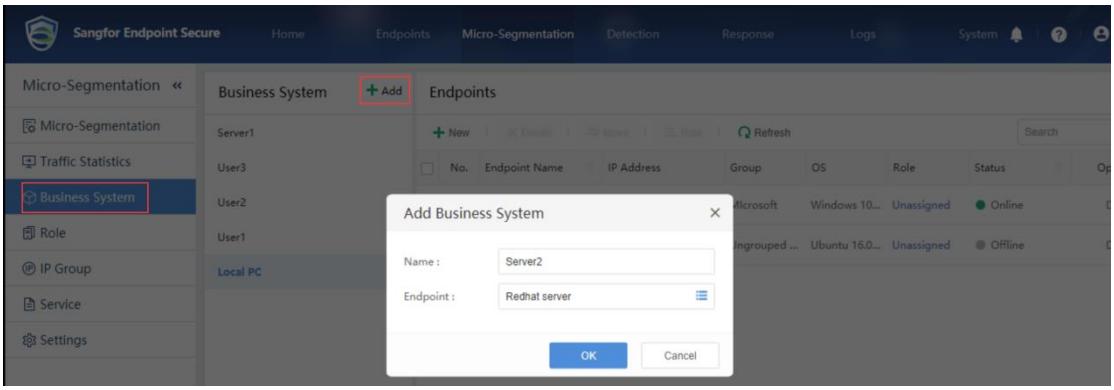
  User zone 3



  Server zone 1

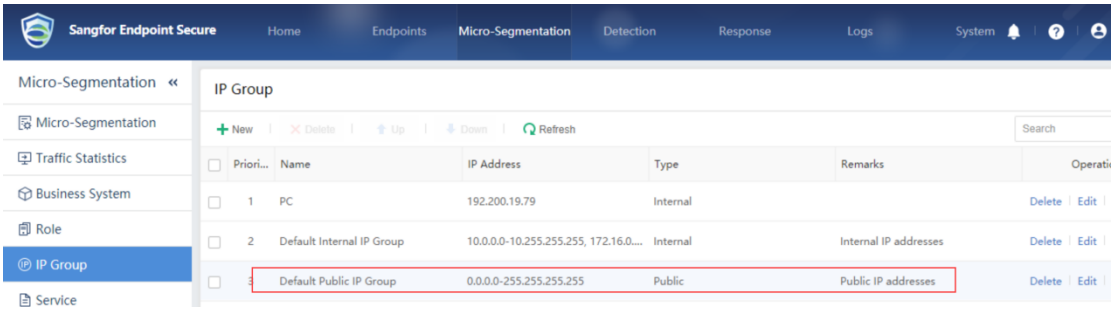


Server zone 2

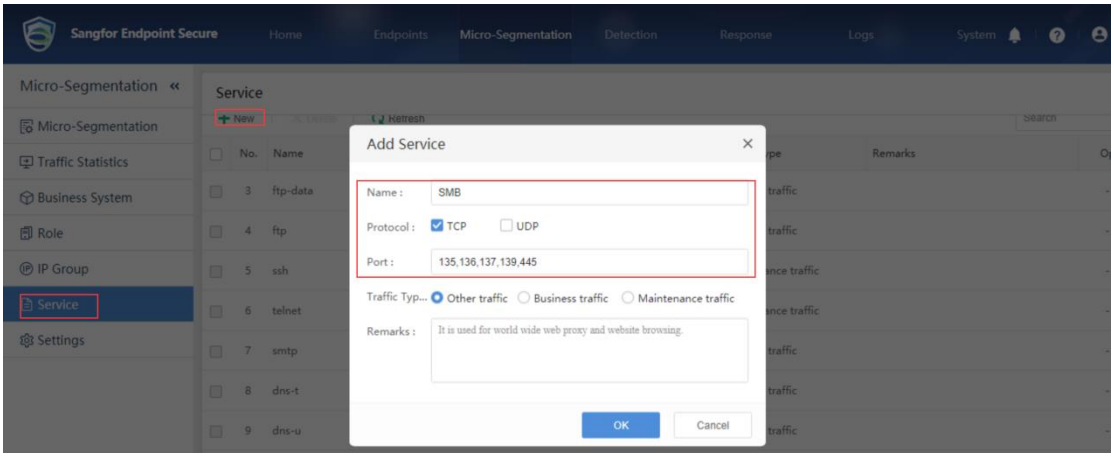


Complete the configuration of a new business system.

- The built-in Default Public IP Group is 0.0.0.0 - 255.255.255.255. This IP group can be called to prevent all IPs on the intranet from accessing each other's shared port.

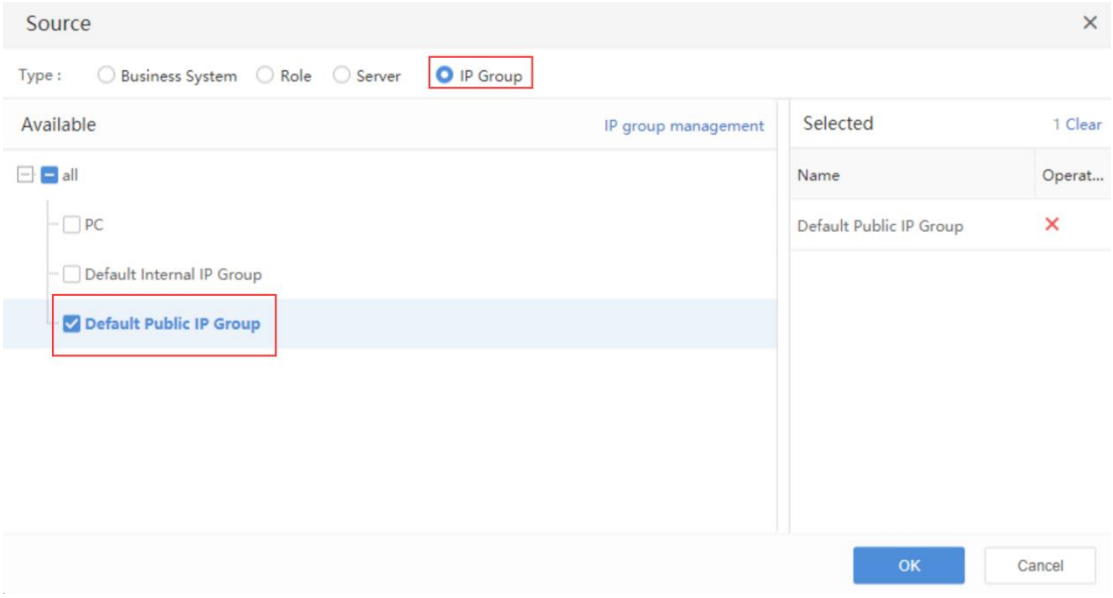


- Define services, including the shared ports to be disabled. Includes TCP (135, 136, 137, 139, 445) ports. Call the remote login ports on the Endpoint Secure Manager.

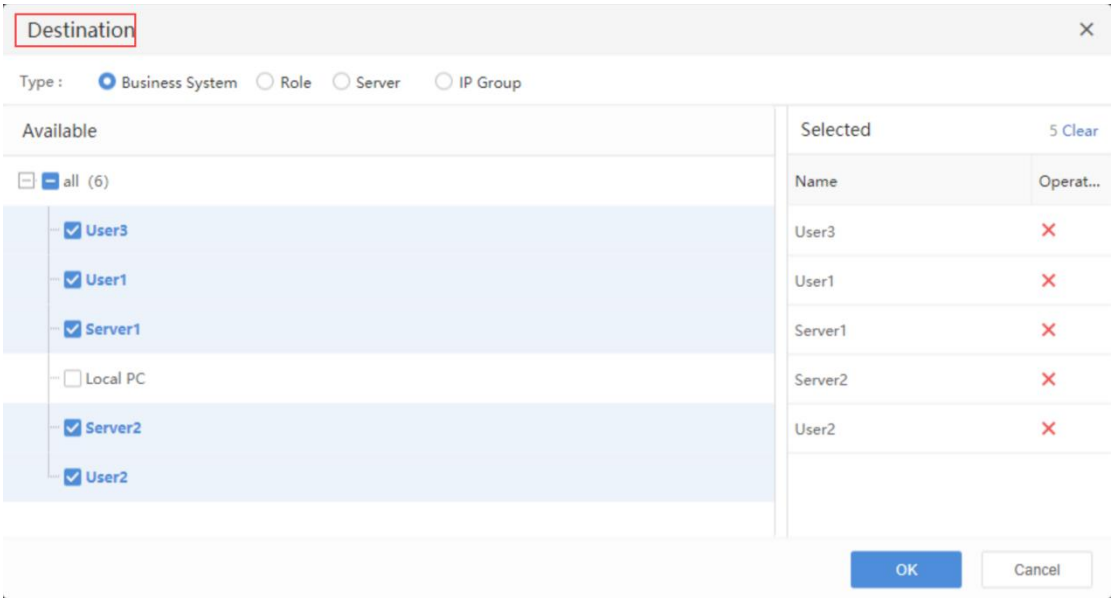


- Configure a micro-segmentation policy to deny any shared port access between all the endpoints (PCs, servers) and access from all the Internet IPs to intranet endpoints via shared port.

Select the default public IP group in the IP group as the source.

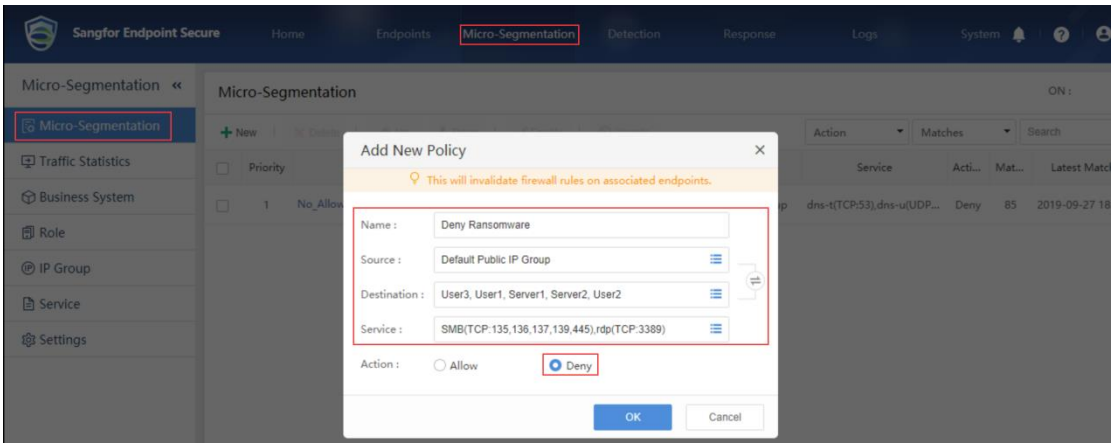


Select 5 business systems as the destinations.



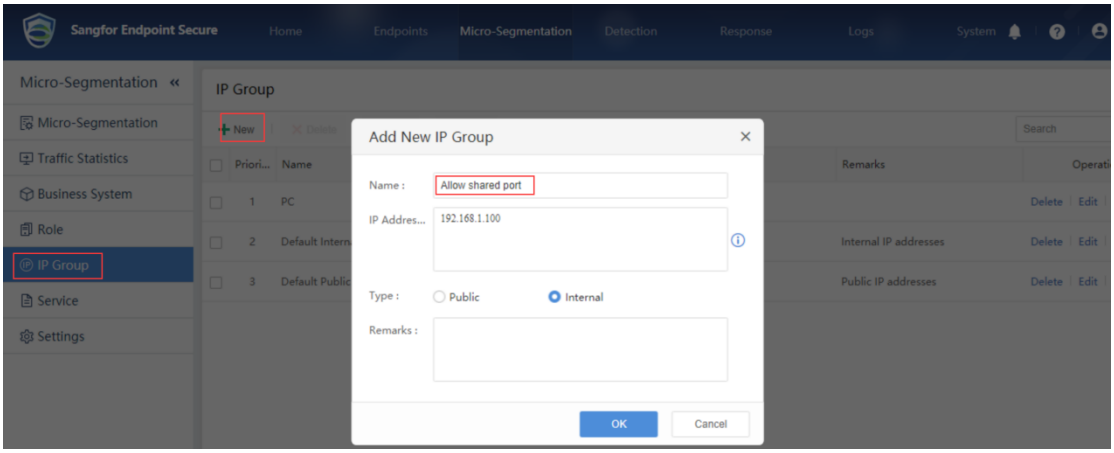
Select customized SMB and built-in rdp as services.

The policy is configured as follows:

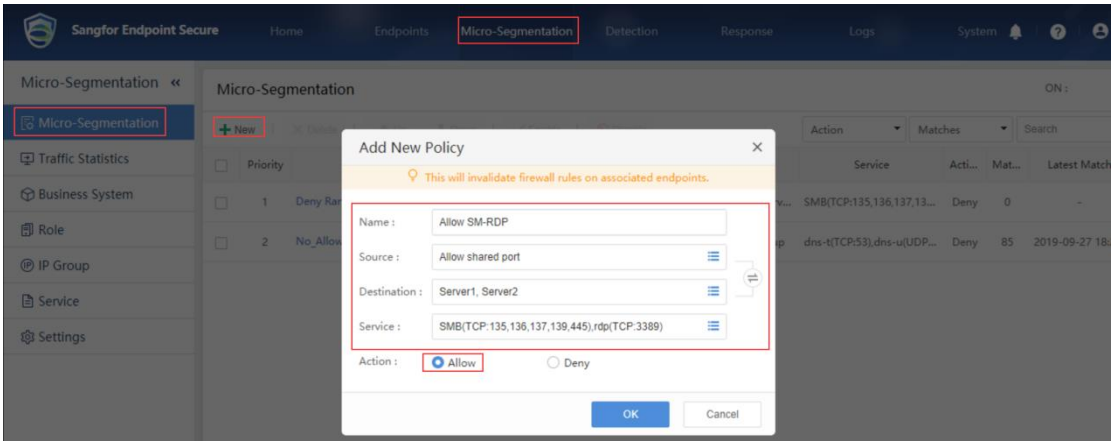


- When a endpoint needs to access the server's shared port or requires remote desktop, you need to configure the policy to allow it.

Add the endpoints that will initiate the access to the IP group.



- Then configure an Allowing Policy for the access from the PC to the server. Select the IP group as the source and select the server as the destination.



The configuration for this scenario is completed.

SANGFOR