Sangfor Endpoint Secure

User Manual

Product Version	3.5.5
Document Version	02
Released on	Jul. 30, 2021

Disclaimer

Products, services or features described in this document, whether wholly or in part, may be not within your purchase scope or usage scope. The products, services or features you purchase must be subject to the commercial contract and terms as agreed by you and Sangfor. Unless otherwise provided in the contract, Sangfor disclaims warranties of any kind, either express or implied, for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Unless otherwise agreed, this document is used for reference only, and all statements, information, and recommendations therein do not constitute any express or implied warranties.

Before You Start

About This Document

This document describes the architecture, features, installation, and O&M management of Endpoint Secure.

Product Version

The following table lists the product version involved in this document.

Product	Version
Endpoint Secure	3.5.5EN

If the configuration is updated in later versions, this document will be updated accordingly.

Intended Audience

This document is intended for:

- Network design engineers
- O&M personnel

Symbol Conventions

The symbols that may be found in this document are defined as follows.

English Icon	Description
	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
	Indicates a hazardous situation, which if not avoided, could result in minor or moderate injury.

NOTICE	Indicates a hazardous situation, which if not avoided, could result in settings failing to take effect, equipment damage, or data loss. NOTICE addresses practices not related to personal injury.
NOTE	Calls attention to important information, best practices, and tips. NOTE addresses information not related to personal injury or equipment damage.

Change History

Changes between document issues are cumulative. Therefore, the latest document issue contains all changes made in previous issues.

Issue	Date	Change Description
01	Jun.22, 2020	This is the first release.
02	Jul.30, 2021	Updated version from v3.2.22

Technical Support

User support email: tech.support@sangfor.com

Technical support hotline:

- Technical Service (Global): +60 1271 175 11 (7129)
- Technical Service (Thailand): +66 600024050
- Technical Service (Indonesia): +62 001 803 492 483 403 09 (Toll-free)
- Technical Service (Singapore): +65 800 852 803 4 (Toll-free)
- Technical Service (Hong Kong): +852 800 931 345 (Toll-free)
- Technical Service (Pakistan): +92 800 900 444 00 (Toll-free)

Inquiry of Sangfor Technologies' service provider and service validity period:

https://community.sangfor.com/plugin.php?id=service:query

Feedback

If you find any product information-related problem using our products, please contact us through the following means.

- https://community.sangfor.com
- Call the local office to provide feedback
- After-sales service hotline:
    - Technical Service (Global): +60 1271 175 11 (7129)
    - Technical Service (Thailand): +66 600024050
    - Technical Service (Indonesia): +62 001 803 492 483 403 09 (Toll-free)
    - Technical Service (Singapore): +65 800 852 803 4 (Toll-free)
    - Technical Service (Hong Kong): +852 800 931 345 (Toll-free)
    - Technical Service (Pakistan): +92 800 900 444 00 (Toll-free)

Contents

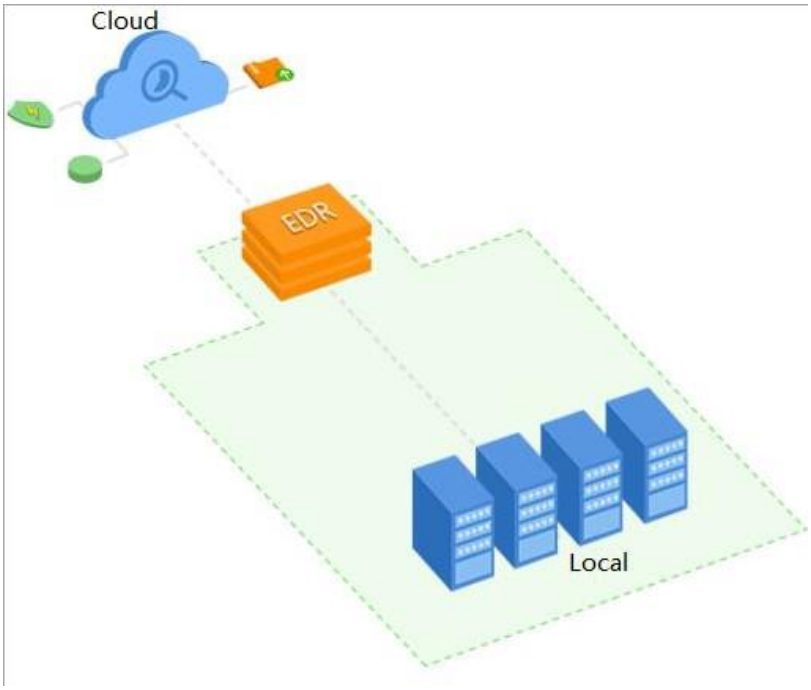
1 Product Overview

Endpoint Secure is an endpoint security solution provided by Sangfor. It consists of the cloud service center, lightweight endpoint security software Endpoint Secure Agent (Agent for short), and Endpoint Secure Manager (Manager for short). The Manager supports centralized endpoint management, virus scan and removal, compliance check, and centralized management of micro-segmentation and access control policies. The Agent supports the antivirus, intrusion prevention, firewall, data collection and reporting, and one-click threat fixing functions.

In addition, Endpoint Secure can integrate and coordinate with Internet Access Gateway (IAG), Cyber Command, Next Generation Application Firewall (Sangfor NGAF), and Platform-X, forming the new-generation security protection system.

1.1 Introduction

Endpoint Secure can be installed in the customer's local environment. The Manager functions in both the software and hardware modes. The Manager software is installed on a Linux server, and the Manager hardware, which is connected to the network core switch in bypass mode, centrally manages all Agents. The Agent is installed on each endpoint. The Manager coordinates with Security Butler through the public network and coordinates with the Agent on each endpoint through the intranet to provide accurate security information and solutions for local endpoint users. The communication data is encrypted. The following figure shows the installation layout.



1.2 Key Features

1.2.1 Network-wide Endpoint Inventory

Network-wide endpoint inventory includes that of business servers and user PCs. The inventory can contain the hardware, software, and asset management information of each endpoint. IT administrators can use this feature to obtain a full picture, analyze risk surfaces, and reduce attack surfaces of hosts on the entire network.

1.2.2 Endpoint Security Compliance Audit

Each organization has its own endpoint security compliance requirements, especially information security level protection (ISLP) compliance requirements and host security requirements. This feature is designed based on the ISLP host security requirements to audit compliance of the identity identification, access control, security audit, intrusion prevention, and malicious code prevention policies. Enterprises can use this feature to ensure that their systems in construction meet the host security requirements of ISLP.

1.2.3 Real-Time Protection from Ransomware

Ransomware is a type of malware that encrypts the victim's files and demands a ransom payment to decrypt them. It becomes more and more common, and victims appear every day. Endpoint Secure can identify different ransomware families accurately, recognize ransomware infection and encryption features after professional analysis, scan and remove the latest ransomware to prevent infection.

1.2.4 System Vulnerability Detection and Rectification

Attackers may exploit system vulnerabilities of different risk levels that fail to be identified or rectified on time to access the customer's intranet, which may cause severe service impact and loss. Endpoint Secure can help administrators identify and rectify endpoint system vulnerabilities on the intranet to enhance system security.

1.2.5 Proactive Detection of Intrusion Attacks

Endpoint hosts may be intruded and then infected with ransomware or crypto mining. Most attackers crack weak passwords using brute force methods to intrude on endpoint hosts. Endpoint Secure can proactively detect brute force cracks, block the IP addresses that initiate attacks, and proactively detect web backdoor files to prevent web security attacks.

2 Installation

Endpoint Secure is an endpoint security solution that consists of the cloud service center, Manager, and Agent. This chapter describes how to install the Endpoint Secure, including preparation, Manager installation, product activation, and Agent installation and uninstallation.

2.1 Preparation

2.1.1 Manager Installation Environment

The Manager functions in both the software and hardware modes. The Manager software can be installed in a physical or virtual environment. The following table describes the hardware resource requirements for installation in both environments. The Manager hardware is connected to the network core switch in bypass mode.

Endpoint Quantity	CPU	Memory	Hard Disk
1-300	2 cores	2G	240G
300-1000	2 cores	4G	1T
1000-2000	4 cores	8G	1T
2000-10000	8 cores	16G	1T

Table 1: Hardware resource requirements

2.1.2 Agent Installation Environment

The Agent is compatible with multiple versions of the Windows and Linux operating systems. The following table lists the supported operating systems and versions.

Operating System	Version
Windows	Windows XP, Windows 7, Windows 8, Windows 8.1, and Windows 10 (32-/64-bit)
Windows Server	Windows Server 2003 SP2 Windows Server 2008/2008 R2 Windows Server 2012/2012 R2 Windows Server 2016/2019
Linux	CentOS 5.7 x86/6/7 Ubuntu 10.04/11.04/12.04/13.04/14.04/16.04/18.04/20.04 Debian 6/7

	RHEL 5/6/7 SUSE 11/12/15 Oracle Linux
Mac	Mac10.13 Mac10.14 Mac10.15 Mac11.0

Table 2: Supported operating systems and versions

2.1.3 Network Connectivity Requirements

Communication between the Agent and Manager and between the Manager and cloud server must allow the Endpoint Secure functions to run properly. The following table describes the allowed ports and server addresses.

Source Device	**Destination Device**	**Protocol/Port**	**Port Function**
Agent	Manager	TCP 443	Access ES MGR management platform
		TCP 4430	Agent download and database update
		TCP 8083	Service port
		TCP 54120	Agent enable/disable by the Manager in emergency scenarios
		ICMP	Connectivity detection
Source Device	**Destination Device**	**Server Addresses Connected Through the Public Network**	
Manager	Cloud server	Patches	https://upd.sangfor.com.cn
		Licensing	https://auth.sangfor.com
		Cloud-Based Engine	https://analysis.sangfor.com

		Terms of Use and Privacy Policy	https://clt.sangfor.com
		Patches, signature, and antivirus database	http://download.sangfor.com.cn

Table 3: Network connectivity requirements

2.1.4 Trusted File Whitelisting

To prevent false error reports during virus scan and removal, you need to collect and whitelist trusted files in advance. Whitelisted files include customer-developed virus-free service software or files that have been whitelisted for other antivirus products. After the Manager is installed and activated, log in to the Manager, choose **Endpoints** > **Security Protection** > **Trusted Files**, and add files to the whitelist. Whitelisted files are skipped during virus scan and removal.

2.2 Manager Installation

The Manager functions in both the software and hardware modes. The following describes how to install the Manager software and hardware.

2.2.1 Manager Software Installation

The Manager software can be installed in either of the following modes:

1. OVA image mode is used in virtualization scenarios, such as when VMware or HCI is used.
2. ISO image mode: is used in virtualization scenarios or scenarios where physical servers are used.

2.2.1.1 Installation Package Downloading

To download related component packages, visit https://community.sangfor.com and choose **Self-Service** > **Software Download** > **Endpoint**.

NOTE

Download the OVA template of the ES3.5.5EN official version for installation in OVA image mode.

Download the ISO template of the ES3.5.5EN official version for installation in ISO image mode.

Download the installation and update package of the ES3.5.5EN official version for update.

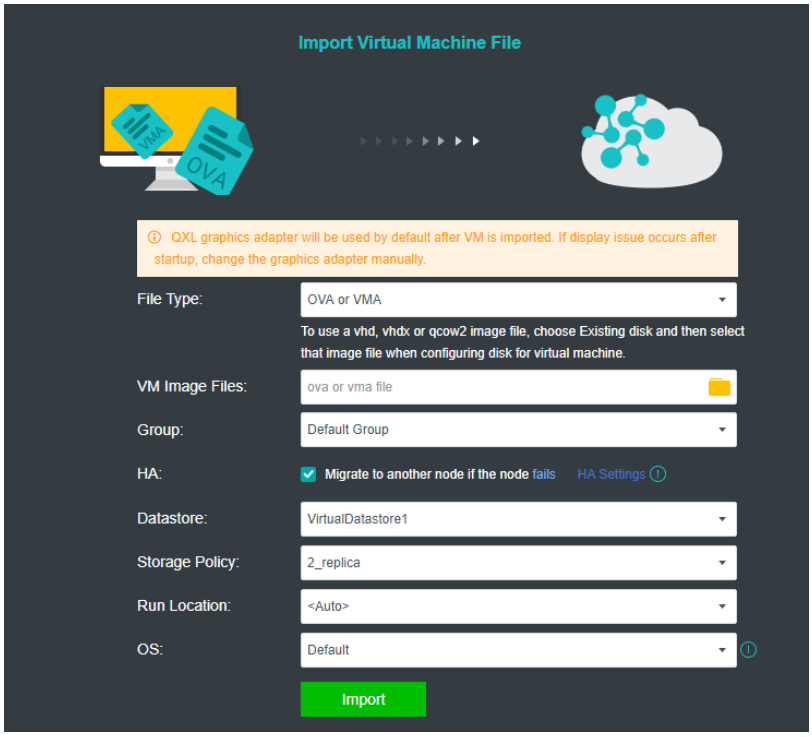
2.2.1.2 Installation in OVA Image Mode

NOTE

The following describes how to install the Manager software in OVA image mode on the HCI. Refer to the following procedure for installation on other virtualization platforms.

Step 1. Import the OVA template.

Import the OVA template from the local environment, as shown in the following figure.



Step 2. Configure the network.

NOTE

You can configure the network on the web portal in the 3.2.22EN or a later version (full installation).

1. Log in to the Manager.

Configure the PC IP address in the same network segment as the management port of the Manager. Open the browser, enter the default Manager address **https://10.251.251.251** in the address box, and press **Enter**. Log in to the Manager. The default user name and password are **admin** and **admin**, respectively.

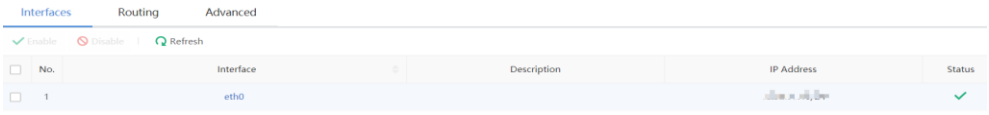
NOTE

The default IP address of the Manager management port is 10.251.251.251/24.

Internet Explorer 11 or later, Firefox, and Google Chrome are supported.

2. Configure the Manager IP address.

Choose **System** > **System** > **Network**, click the **Interfaces** tab, and set **IP Address**, as shown in the following figure.

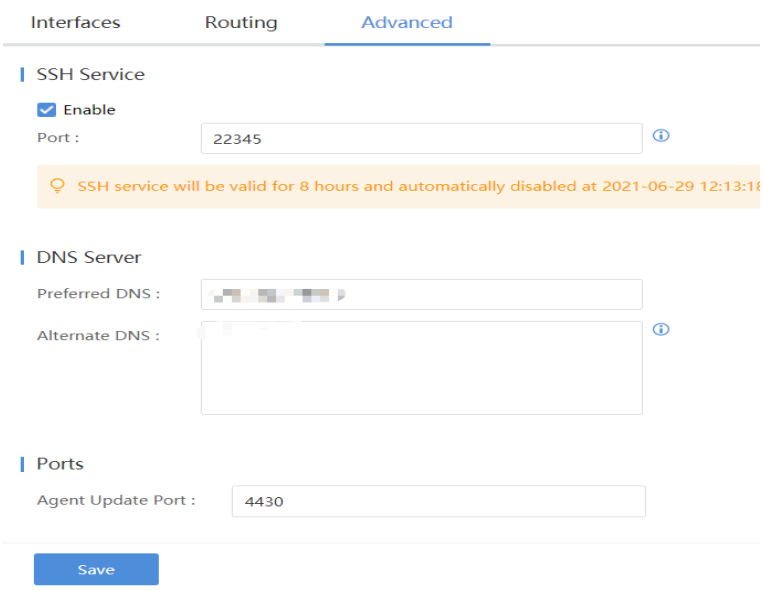


3. Configure DNS addresses.

Choose **System** > **System** > **Network**, click the **Advanced** tab, and set **Preferred DNS** and **Alternate DNS**, as shown in the following figure.

NOTE

The DNS addresses must be configured because domain names need to be parsed when the Manager updates the antivirus database.

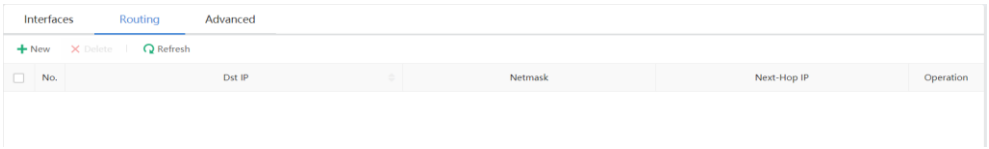


4. Configure routes.

Choose **System** > **System** > **Network**, click the **Routing** tab, and configure routes, as shown in the following figure.

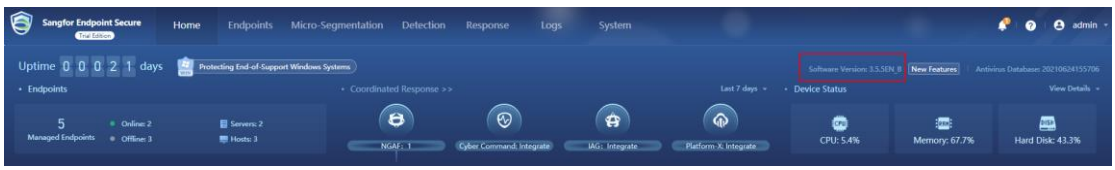
NOTE

Routes must be configured for the Manager to connect to and communicate with endpoints.



Step 3. Verify that the Manager installation is successful.

Log in to the Manager (default address: https://10.251.251.251, default user name and password: **admin** and **admin**) and check whether the version number on the home page is correct, as shown in the following figure. If the version number is correct, the installation is successful.



2.2.1.3 Installation in ISO Image Mode

Step 1. Prepare for the installation.

Use UltraISO to burn the ISO template to an empty USB flash drive or DVD.

NOTE

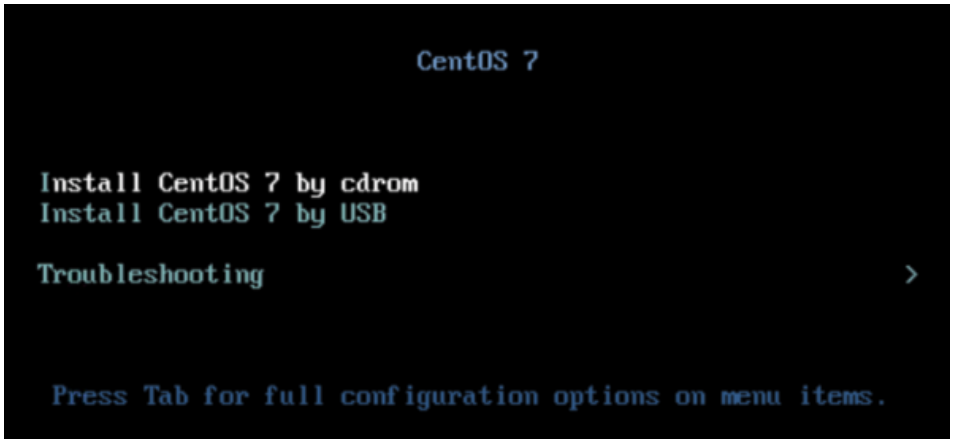
Before burning the ISO template to the USB flash drive, ensure that data in the USB flash drive has been backed up so that data lost during burning can be restored.

Before burning the ISO template to the USB flash drive, calculate the MD5 value of the VMP ISO file used for burning.

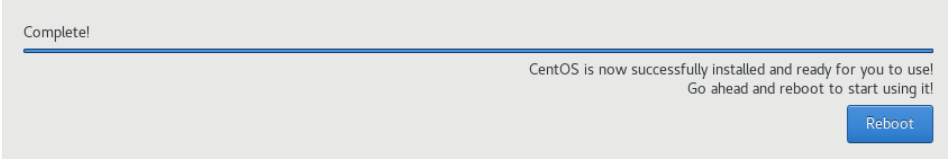
When burning the ISO template to the USB flash drive, select the correct USB flash drive.

Step 2. Install the Manager.

1. Set the server to first boot from the CD ROM or USB flash drive, as shown in the following figure.



2. Select **Install CentOS 7 by USB** and press **Enter**. The Manager is automatically installed, and no manual operation is required. Wait until the page shown in the following figure is displayed indicating that the installation is complete.



3. Click **Reboot** to restart the server.

Step 3. Configure the network.

For details, see "Configure the network" in 2.2.1.2.

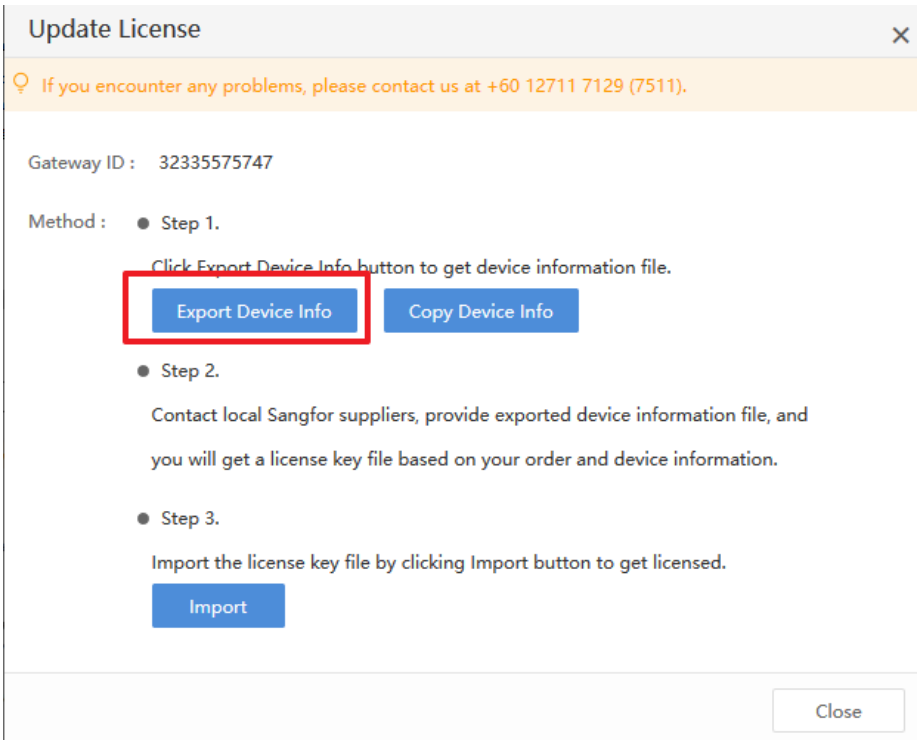
Step 4. Verify that the Manager installation is successful.

Log in to the Manager (default address: https://10.251.251.251, default user name and password: **admin** and **admin**) and check whether the version number on the home page is correct, as shown in the following figure. If the version number is correct, the installation is successful.

2.3 Product Activation

After the Manager is installed, you must activate the Manager before installing the Agent and using the Endpoint Secure Manager. For Endpoint Secure 3.2.17 and later versions, the Manager is licensed on the Platform-X in centralized mode. Perform the following operations to activate the Manager as a customer:

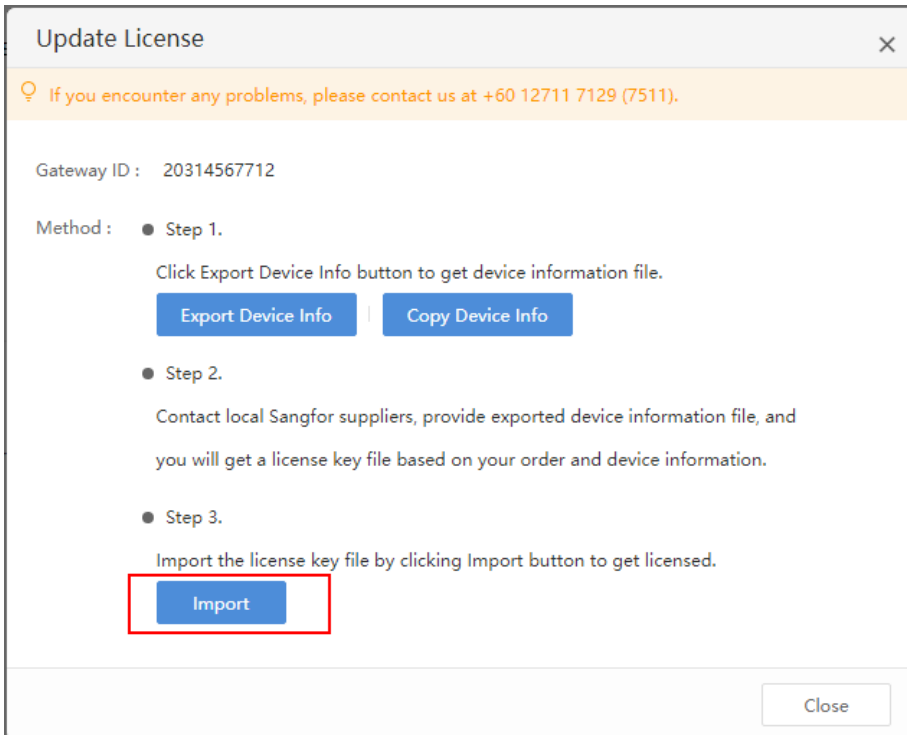
Step 1. Click Export Device Info button to get the device information file.



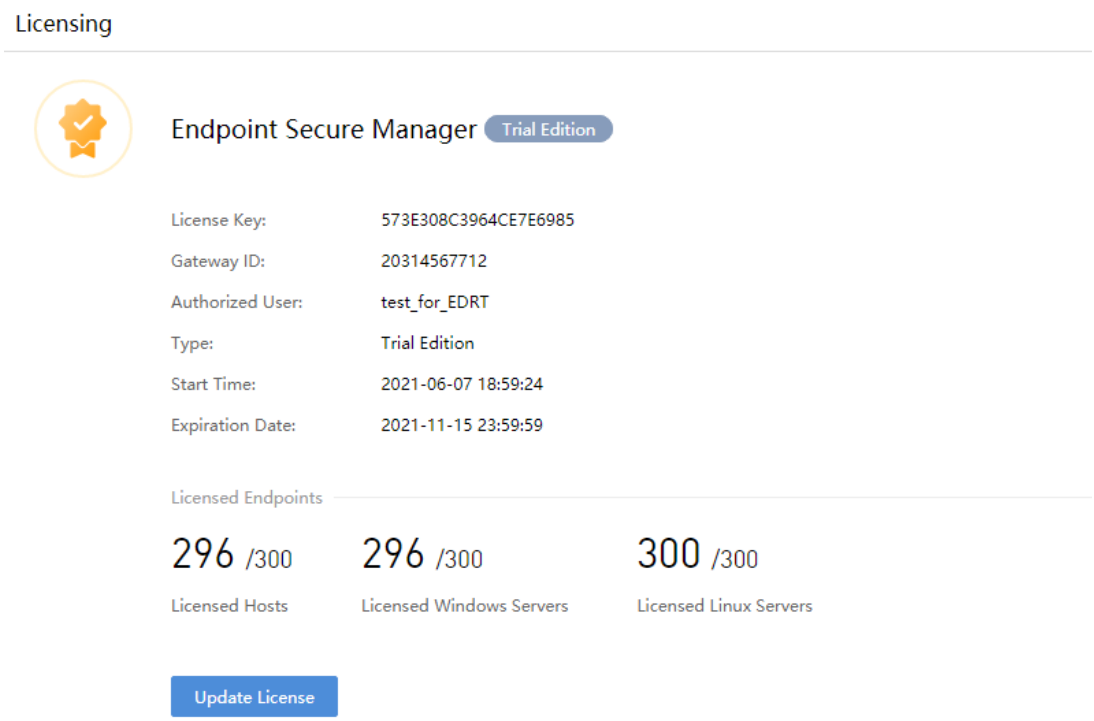
Step 2. Contact local Sangfor suppliers, provide exported device information files, and you will get a license key file based on your order and device information.

Step 3. Import the license key file by clicking the **Import** button to get licensed.

1. On the Manager, choose **System** > **Licensing**, click **Import** in step 2 shown in the following figure, and import the license file obtained in step 3.



2. Wait until the number of licensed endpoints of each type is displayed, indicating that the Manager is activated successfully.



2.4 Agent Installation

2.4.1 Installation on the Windows Operating System

On a PC or server running the Windows operating system, you can install the Agent by downloading the installation package in common installation scenarios or by distributing a link to an installation notice webpage, using the IAG, using a VM template, pushing the installation script by the domain controller, or distributing the installation package by desktop management software in large-scale installation scenarios. Select an installation mode based on the installation scenario on the customer side.

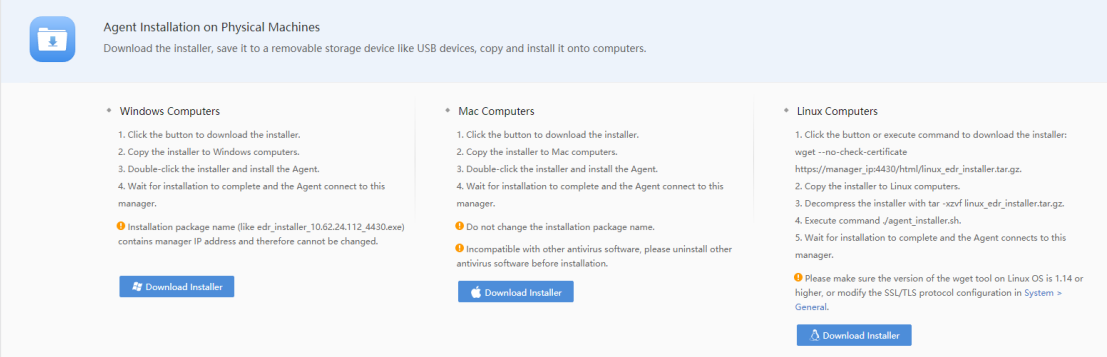
2.4.1.1 Common Installation Scenarios

In common installation scenarios, you need to download the Agent installation package from the Manager and use a USB flash drive or other mobile media to import the package to the endpoint for installation as an administrator. The installation procedure is as follows:

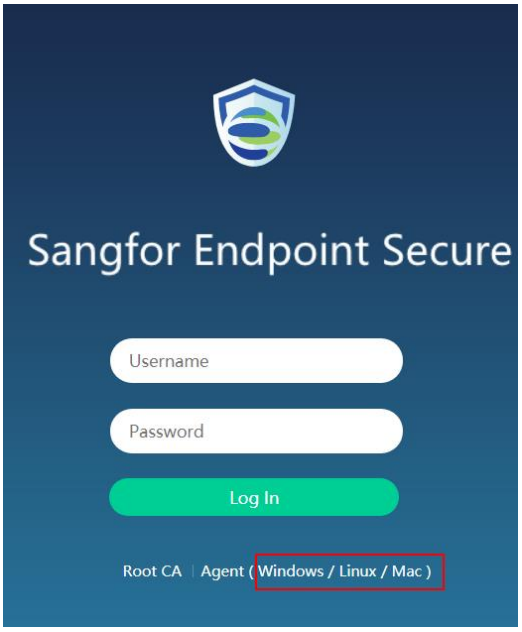
1. On the Manager, choose **System** > **Agent Deployment** and click **View Details** next to **Agent Installation on Physical Machines**.

NOTE

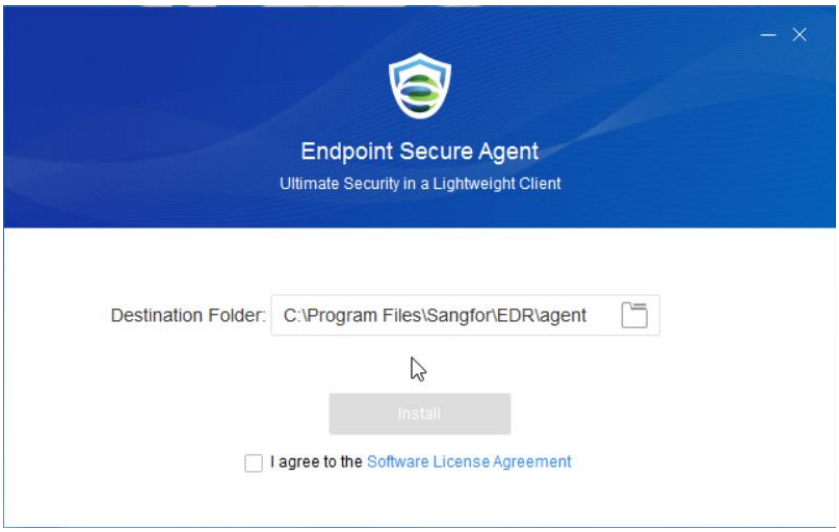
The default PC Agent installation package name (similar to **edr_installer_117.48.147.100_443.exe**) contains the Manager communication address information. Do not change the installation package name after the installation package is downloaded.



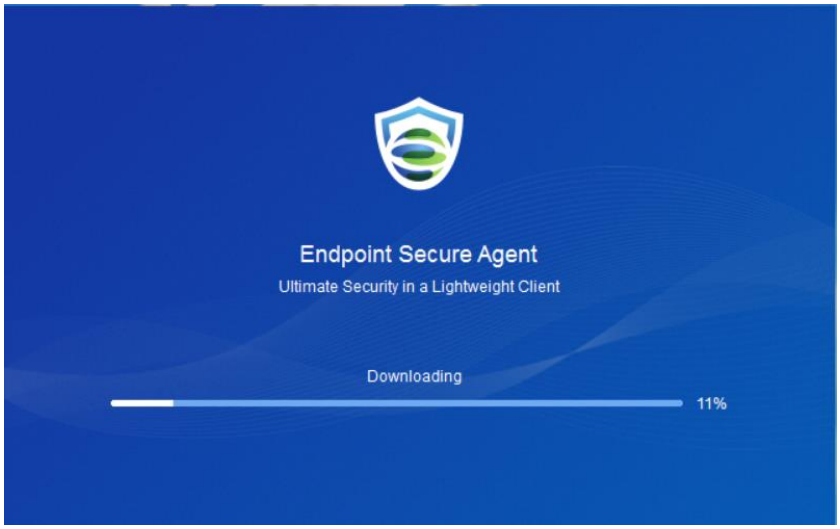
Alternatively, download the installation package from the login page of the Manager, as shown in the following figure.

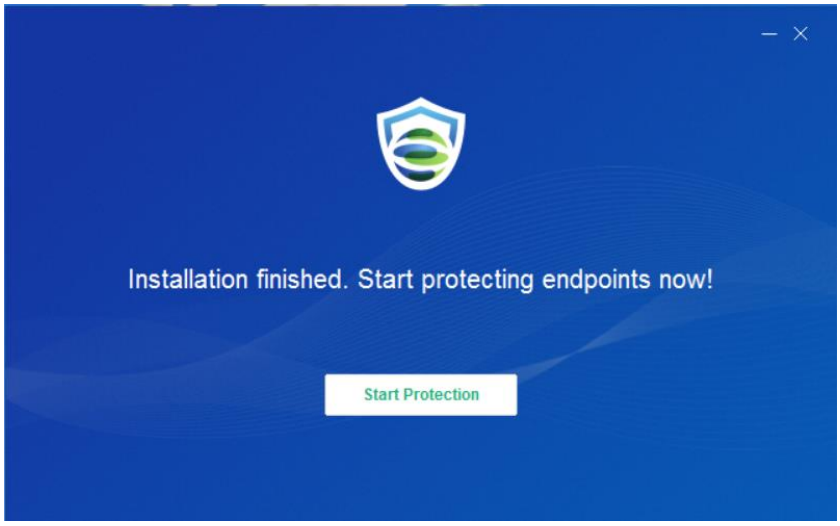


2. Copy the installation package to the endpoint on which the Agent needs to be installed.
3. Double-click the installation package on the endpoint.

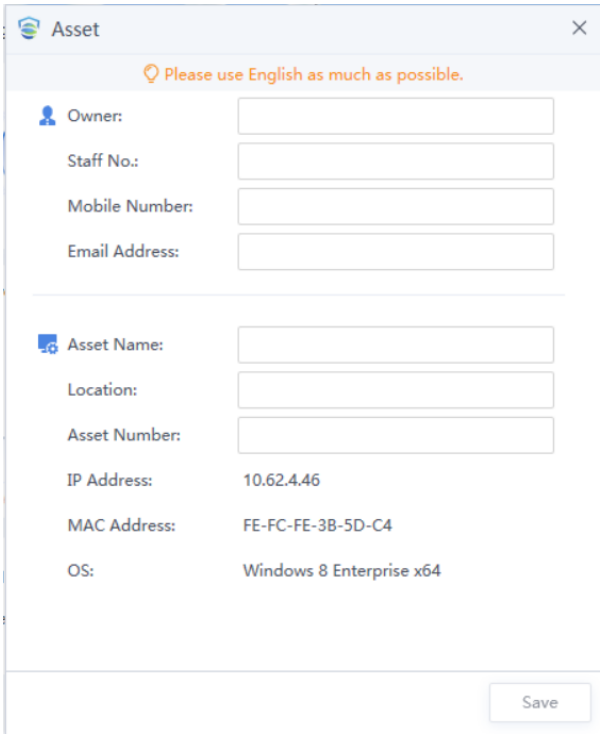


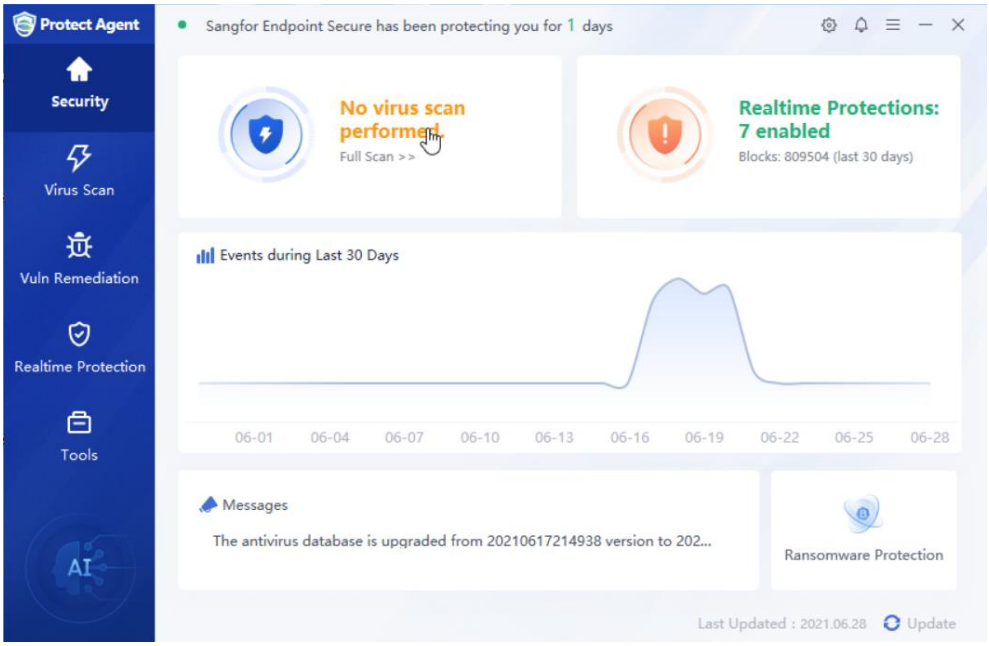
Select **I agree to the Software License Agreement** and click **Install**. The installation program connects to the Manager to download the required installation components, as shown in the following figure.



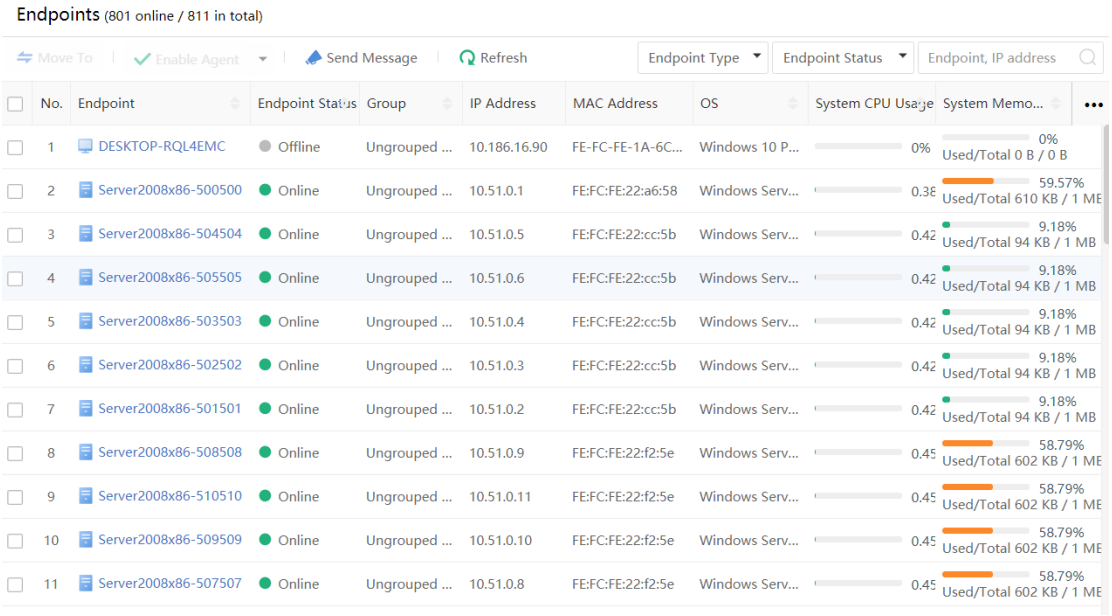


After the installation is complete, click **Start Protection** and enter asset information, as shown in the following figure.





After the installation is successful, the Agent on the endpoint automatically connects to the Manager. After logging in to the Manager and choosing **Endpoints** > **Groups**, you can view endpoint status, as shown in the following figure.



2.4.1.2 Large-scale Installation Scenarios

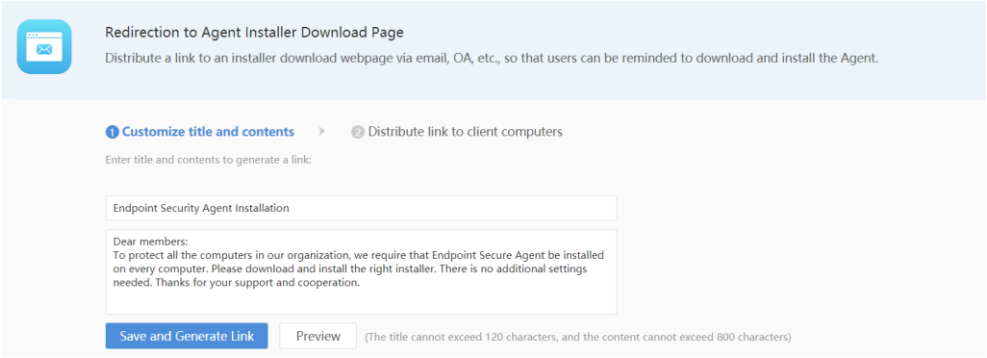
In large-scale installation scenarios, you can install the Agent by distributing a link to an installation notice webpage, using the IAG, using a VM template, or distributing the installation package by desktop management software. Select an installation mode based on the installation scenario on the customer side.

Redirection to Agent Installer Download Page

You can distribute a link to an installation notice webpage as an administrator in emails or using OA so that users can be reminded to download the Agent installation package and install the Agent. The installation procedure is as follows:

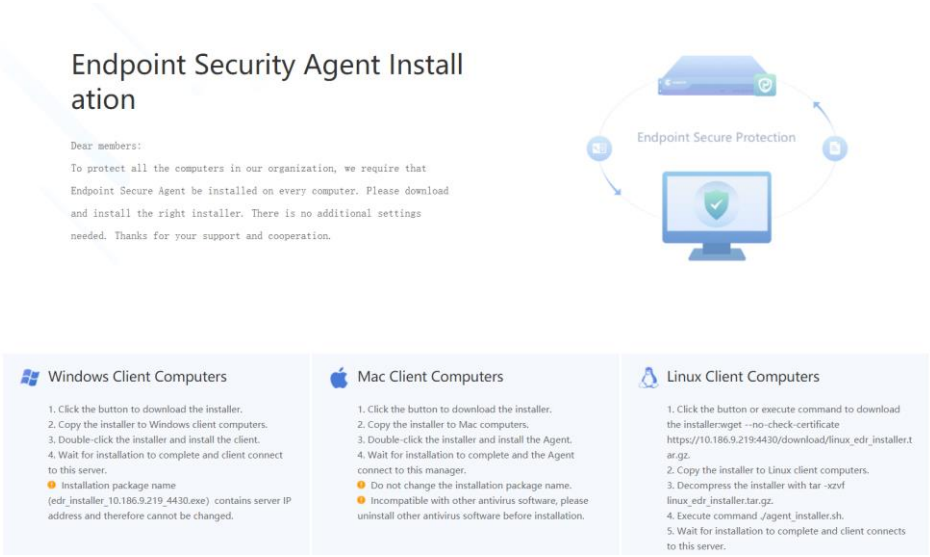
1. Create an installation notice.

Choose **System** > **Agent Deployment**, click **Redirection to Agent Installer Download Page**, and enter the installation notice page title and content. Preview the installation notice to verify the notice information and click **Save and Generate Link**.



2. Copy the link and send it to endpoints.

Send the link to endpoint users in emails, using OA, or using other methods. The endpoint users can click the link, download the installation package, and install the Agent. After an endpoint user clicks the link, a page similar to the following is displayed.



Integration to Sangfor IAG

If you select this installation mode, either of the following schemes can be used:

Scheme 1: Use the IAG admission function to check whether the Agent has been installed on an endpoint (by checking for Agent-related processes). If not, IAG forcibly redirects to the Agent installation page when the endpoint user attempts to open a webpage. The endpoint user is allowed to access the Internet only after installing the Agent. This scheme is recommended.

Scheme 2: Integrate Endpoint Secure with IAG. When an endpoint user attempts

to open a webpage on a PC where the Agent is not installed, IAG redirects to the Agent installation page. In addition, the Agent installation page is displayed at intervals until the agent is installed. This scheme implements batch Agent installation. The integration is configured only on the IAG GUI. The installation procedure is as follows:

NOTE

Endpoint Secure must be of the 3.2.22 or a later version, IAG must be of the 12.0.14 or a later version, and the endpoint operating system must be compatible with Endpoint Secure.

1. Log in to the IAG Manager and choose **Security** > **Security Capabilities** > **Endpoint Secure.** On the **ES** page, enter the Manager IP address and click **Connect Now**.
2. Wait until the service status is displayed as **Online** and the Manager IP address is displayed, indicating that the connection is successful. You can click **View Association Details** to view endpoints connected to the Endpoint Secure.
3. On the **ES** page, click **Push Configuration** in the upper right corner. On the page that is displayed, configure the network segment where the policy is used, redirected-to address, and push interval.

NOTE

The redirected-to address is that configured under **System** > **Agent Deployment** > **Integration to Sangfor IAG** of the Manager.

4. Attempt to open a webpage as an endpoint user. The Agent installation page is displayed. In addition, the Agent installation page is displayed at intervals until you download the Agent installation package and install the Agent.

Agent Installation on Virtual Machines

This installation mode applies when the customer's desktop office environment is a virtual environment. Using the template update function on the visualization platform, you can quickly install the Agent components on endpoints in batches as an administrator. Assume that Sangfor aDesk is used. The installation procedure is as follows:

1. Import the downloaded Agent components to the VM template.
2. Install the Agent components on the VM.
3. Configure the template update policy to immediate or scheduled update to install the Agent components in batches.

Desktop Management Software

This installation mode applies when desktop management software or similar software is available in the customer's desktop office environment. The desktop management software can distribute and install the Agent components on endpoints in a centralized mode, implementing batch installation. For details about the procedure, contact the desktop management software vendor.

2.4.2 Installation on Linux Servers

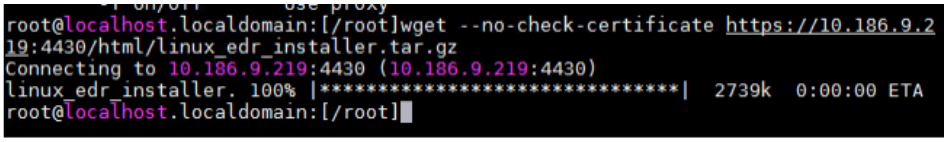
You can download the Agent installation package on Linux servers to install the Agent in common installation scenarios or use a script tool to install the Agent in large-scale installation scenarios.

2.4.2.1 Common Installation Scenario

In common installation scenarios, you can download the Agent installation package from the Manager and use a USB flash drive or other mobile media to import the installation package to the endpoint for installation as an administrator. Alternatively, you can use the **wget** command on the endpoint to remotely download the Agent installation package and install the Agent as an administrator. The procedure for using the **wget** command to install the Agent is as follows:

1. Run the **wget --no-check-certificate**

https://*Manager_IP*/html/linux_edr_installer.tar.gz command on the host running the Linux operating system to download the Agent installation package, as shown in the following figure. In the preceding command, ***Manager_IP*** indicates the actual IP address of the Manager.



2. Run the **tar -xzvf linux_edr_installer.tar.gz** command to decompress the Agent installation package.
3. Go to the directory extracted after the decompression and run **./agent_installer.sh** to install the Agent. The default installation path is **/Sangfor/EDR/agent**.

NOTE

1. You can run the **./agent_installer.sh *Manager IP address Installation path*** command to specify the Agent installation path.
2. If a message asking whether to install ipset is displayed during installation, you can select **y** or **n**. It is recommended that you select **y** to install ipset and then install the Agent.

2.4.2.2 Large-scale Installation Scenarios

In large-scale installation scenarios, you can also distribute a link to an installation notice webpage, use the IAG, or use a VM template to install the Agent on Linux servers as an administrator.

In addition, a script tool can be used for large-scale installation of the Agent on Linux servers. The root accounts and passwords of all Linux servers must be imported to the script tool, and the script tool must connect to the Linux servers in SSH mode.

During script execution, the script tool connects to the Linux servers in SSH mode, automatically downloads the Agent components from the Manager, installs the Agent components, and brings the Agent components online to the

Manager. The whole process is automatic.

NOTE

For details about the batch Agent installation tool on Linux servers, please contact our Sangfor Technical support.

2.4.3 Installation on the Mac Operating System

On endpoints running the Mac operating system, you can download the Agent installation package to install the Agent in common installation scenarios or use a script tool to install the Agent in large-scale installation scenarios.

2.4.3.1 Common Installation Scenarios

In common installation scenarios, you can download the Agent installation package from the Manager and use a USB flash drive or other mobile media to import the installation package to the endpoint for installation as an administrator. The procedure for install the Agent is as follows:

1. Click the button to download the installer.
2. Copy the installer to Mac computers.
3. Double-click the installer and install the Agent.
4. Wait for the installation to complete and the Agent connects to this manager.

2.4.3.2 Large-scale Installation Scenarios

In large-scale installation scenarios, you can also distribute a link to an installation notice webpage, use the IAG, or use a VM template to install the Agent on the Mac operating system as an administrator.

2.5 Agent Uninstallation

2.5.1 Uninstallation on the Windows Operating System

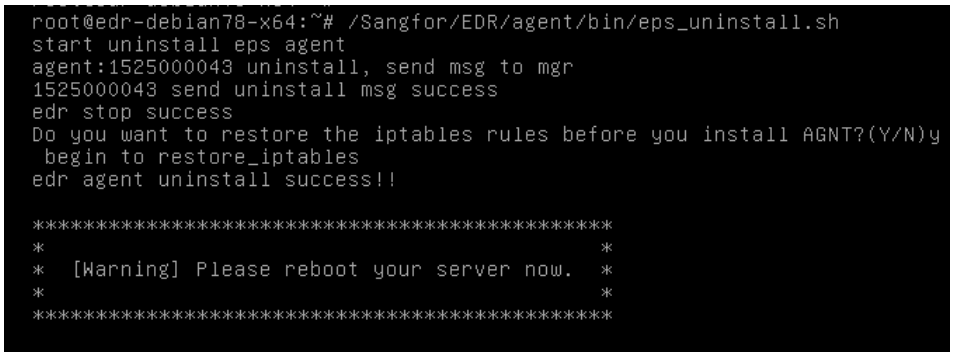
Click **Start**, locate **Endpoint Secure,** and click **Uninstall**. Alternatively, uninstall the Agent on the control panel.

NOTE

You can also run **uninstall.bat** in the installation directory **%ProgramFiles%\Sangfor\EDR** to uninstall the Agent.

2.5.2 Uninstallation on Linux Servers

In the CLI of the endpoint running the Linux operating system, locate the Endpoint Secure directory **/Sangfor/EDR/agent/bin** and run **eps_uninstall.sh** to uninstall the Agent, as shown in the following figure.



2.5.3 Uninstallation on the Mac Operating System

In the CLI of an endpoint running the Mac operating system, locate the Endpoint Secure directory **/Library/sangfor/ed/agent/bin** and run **eps_uninstall.sh** to uninstall the Agent, as shown in the following figure.

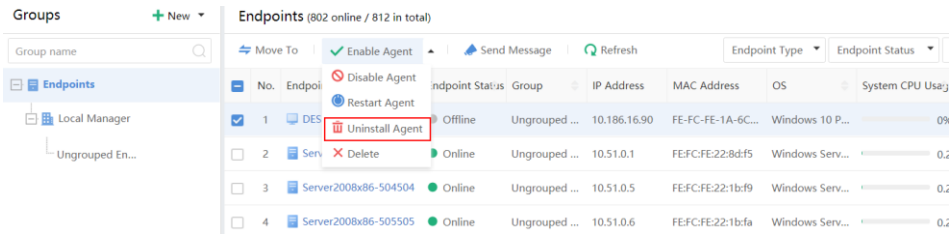
```
LSSs-Mac:~ root# /usr/local/sangfor/edr/agent/bin/eps_uninstall.sh
start uninstall eps agent
start stop eps_services
uninstall
edr stop success
start clean file
No matching processes were found
edr agent uninstall success!!

*********************************************
*                                           *
*  [Warning] Please reboot your server now.  *
*                                           *
*********************************************

LSSs-Mac:~ root#
```

2.5.4 Uninstallation on the Manager

1. On the Manager, choose **Endpoints** > **Groups** and select endpoints on which the Agent components need to be uninstalled.
2. Choose **Uninstall Agent** from the drop-down list above the endpoint list, as shown in the following figure.

NOTE

The Agent can be uninstalled only on endpoints in an **Online** or **Disabled** state.



3 Manager

3.1 Manager Login

To ensure security, use the standard HTTPS port to log in to the Manager. The login procedure is as follows:

1. Open the browser, enter **https://*EDR_IP*:*EDR port number*** in the address box, and press **Enter**. The default port number is 443.

NOTE

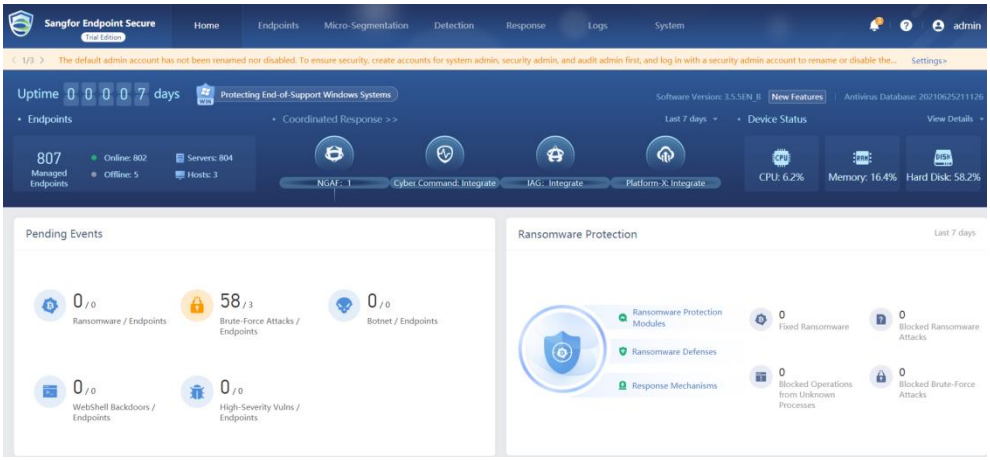
If a message "The identity of this website or the integrity of this connection cannot be verified" is displayed, click **Yes**.

Internet Explorer 11 or later, Firefox, and Google Chrome are supported.

2. Enter the username, password, and verification code and click **Log In**. The default username and password are admin/admin.
3. The system prompts you to change the default password upon first login to ensure security.

3.2 Home Page Display

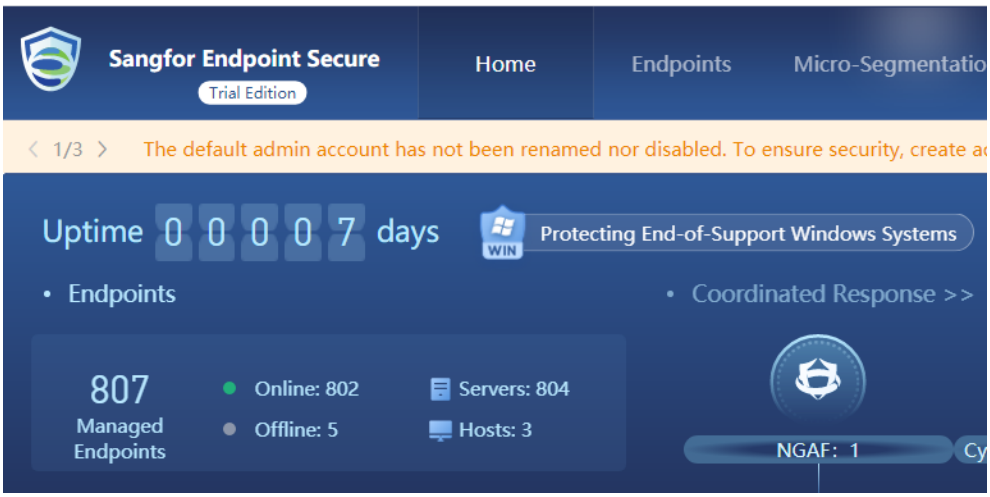
On the **Home** page of the Manager, the Manager and endpoint running status is displayed. The **Home** page contains the **Endpoints**, **Pending Events**, **Ransomware Protection**, **Target Endpoints**, **Security Events**, and **Coordinated Response** modules, as shown in the following figure.



3.2.1 Endpoints

The **Endpoints** module shows the total number of managed endpoints (including hosts and servers), online endpoints, and offline endpoints.

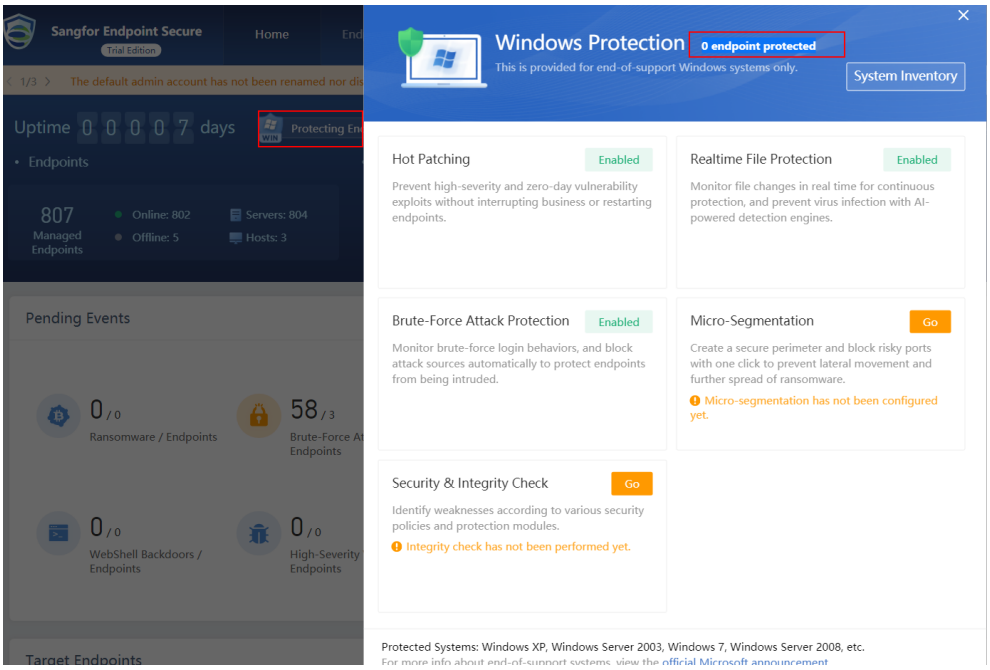
If you click **Managed Endpoints**, the **Groups** page under **Endpoints** is displayed. You can view detailed endpoint information on the Groups page, including the names, statuses, IP addresses, and operating systems.



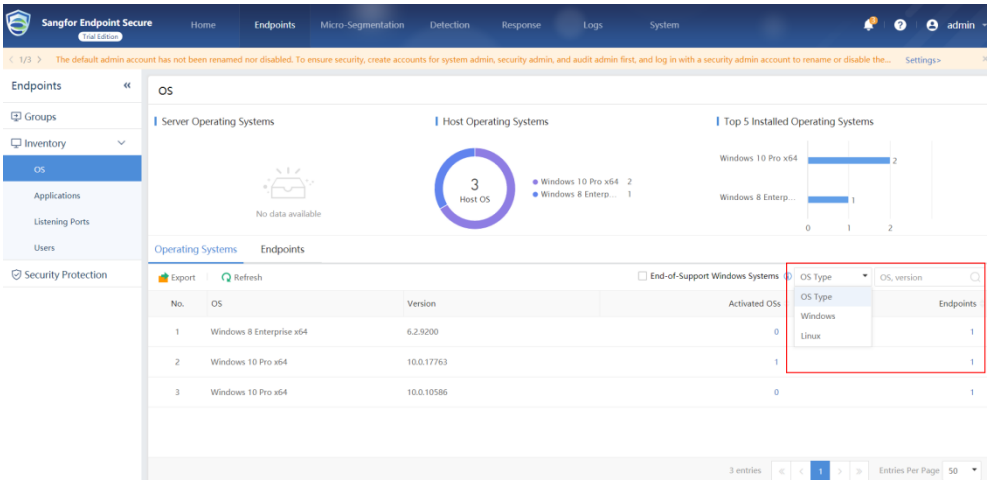
3.2.2 Windows Protection

Windows Protection is a dedicated protection plan provided by Endpoint Secure for Microsoft end-of-support Windows operating systems. This plan allows Endpoint Secure to provide multiple core functions, such as zero-day vulnerability prevention, file protection, brute-force attack protection, system weakness identification, risky port blocking, and to work with the AI engine to detect potential unknown threats so that dedicated protection and security hardening are provided for end-of-support Windows operating systems.

1. Click **Protecting End-of-Support Windows Systems** on the **Home** page to view endpoints running end-of-support operating systems and protection of the endpoints, as shown in the following figure.



2. Click **System Inventory**. On the **OS** page under **Inventory**, filter Microsoft end-of-support operating systems by **OS Type** (Windows/Linux) or enter the operating system name or version number to search for required operating systems. In the filter or search results, you can view the number of endpoints running the specified operating system. It helps O&M personnel determine the endpoint status and take corresponding measures, such as operating system update or replacement or endpoint iteration.



3. View the statuses (**Enabled** or **Go**) of protection measures, including **Hot Patching**, **Realtime File Protection**, **Brute-Force Attack Protection**, **Micro-Segmentation**, and **Security & Integrity Check**.

Hot Patching: This lightweight function does not interfere with the system. It can prevent high-severity and zero-day vulnerability exploits without

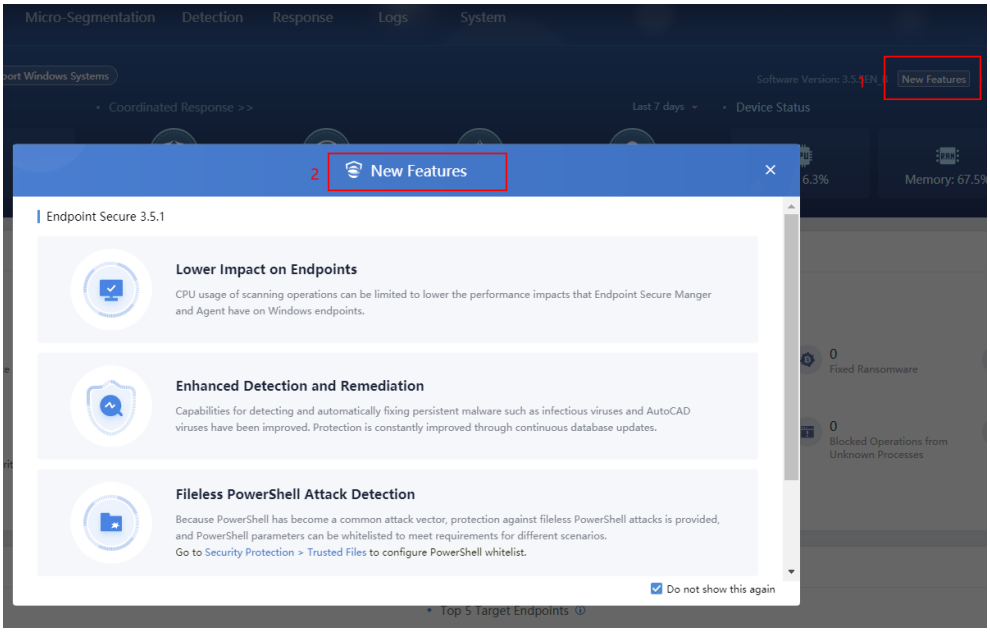
interrupting businesses or restarting endpoints. You can click **Enabled** next to the function name to go to the **Vuln Remediation** tab page. On the **Vuln Remediation** tab page, you can view details or disable this function.

- **Realtime File Protection**: This function is an AI-powered multidimensional threat detection mechanism. This function allows the Endpoint Secure to monitor file changes of endpoints running end-of-support operating systems in real-time to provide continuous protection and prevent virus infection. You can click **Enabled** next to the function name to go to the **Realtime Protection** tab page. On the **Realtime Protection** tab page, you can view details or disable this function.
- **Brute-Force Attack Protection**: This function allows the Endpoint Secure to monitor hackers' brute-force login attempts continuously and automatically block attack sources to prevent endpoints from being intruded. You can click **Enabled** next to the function name to go to the **Realtime Protection** tab page. On the **Realtime Protection** tab page, you can view details or disable this function.
- **Micro-Segmentation**: This function allows the Endpoint Secure to create a dynamic secure perimeter for all types of endpoints and block risky ports with one click to ensure visible and controllable endpoint security and reduce lateral movement and further spread of ransomware. You can click **Go** next to the function name. On the **Policies** page under **Micro-Segmentation** that is displayed, you can switch the **ON** button and add micro-segmentation policies.
- **Security & Integrity Check**: This function allows the Endpoint Secure to identify weaknesses of end-of-support operating systems using the identity policy, access control policy, security audit policy, history information protection policy, intrusion prevention, and malicious code prevention to enhance system security. You can click **Go** next to the function name to go to the **Security & Integrity Check** page under **Detection**. On the **Security & Integrity Check** page, you can click **Start Now** to start the check.

New Features

The **New Features** page shows new features of the version. On the **Home** page, click **New Features**. You can view the new features of the version and the

product introduction video on the **New Feature** page. You can click the video to play it.



Banner Reminder

1. ISLP compliance reminder

When the ISLP requirements are not met, for example, when the **admin** account has not been disabled or renamed, a banner reminder is displayed, as shown in the following figure.

Click **Settings**. The **Administrators** page under **System** is displayed. Use the security administrator account to rename or disable the default **admin** account. You can also assign account permissions properly to prevent information leakage due to improper permission assignment as the security administrator.

2. Port change reminder

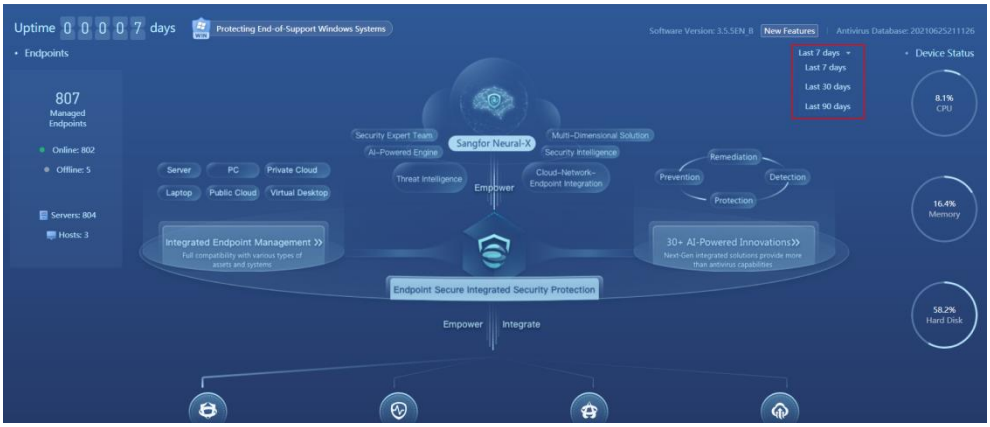
When a port vulnerable to brute force cracks or attacks is detected, a banner reminder is displayed reminding you to change the port number, as shown in the following figure.

Click **Settings**. The **Advanced** tab page under **System** > **System** > **Network** is displayed. On the **Advanced** tab page, change the port number to prevent virus infection due to brute force cracks and ensure system security.

Coordinated Response

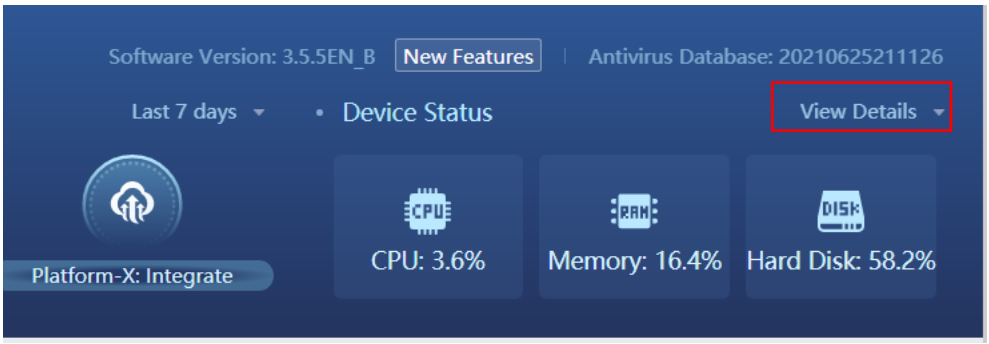
The **Coordinated Response** module displays integration between the Endpoint Secure and NGAF, Cyber Command, IAG, and Platform-X. Click ***Product Name*: Integrate**. On the **Integrated Devices** page under **System** displayed, you can connect to and manage integrated devices.

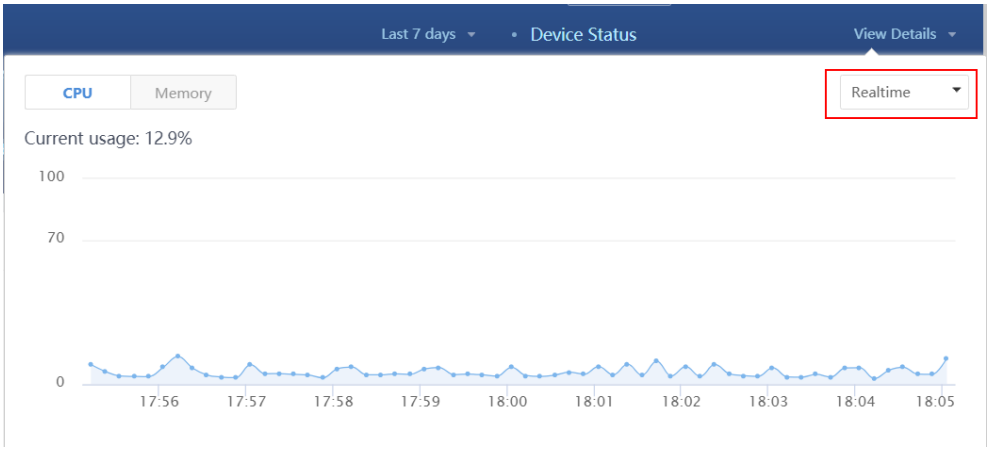
On the **Home** page, you can click the down arrow to view the integration value and overall capability framework of the Endpoint Secure more intuitively. In the upper right corner, you can select **Last 7 days**, **Last 30 days**, or **Last 90 days** from the drop-down list to view the Endpoint Secure working status in the selected period.



Device Status

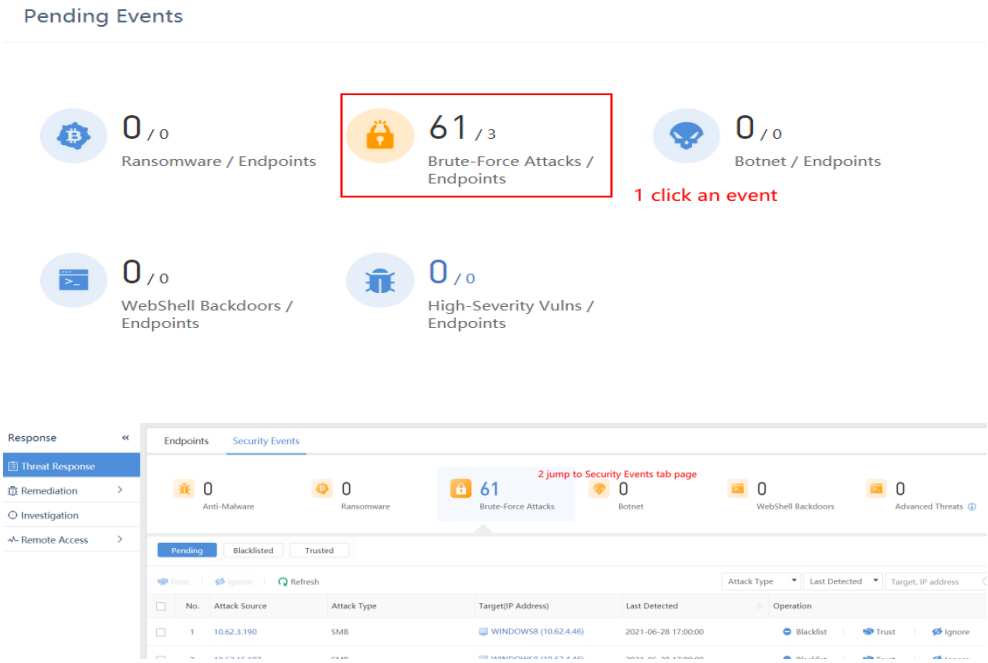
The **Device Status** module displays the CPU usage, memory usage, and hard disk usage of the Manager. You can click **View Details** to view the CPU and memory usage in **Realtime**, **Last 24 hours**, and **Last 30 days**, as shown in the following figure.


Software Version: 3.5.5EN_B
New Features
Antivirus Database: 20210625211126
Last 7 days
Device Status
View Details
Platform-X: Integrate
CPU: 3.6%
Memory: 16.4%
Hard Disk: 58.2%


Last 7 days
Device Status
View Details
CPU
Memory
Realtime
Current usage: 12.9%
100
70
0
17:56
17:57
17:58
17:59
18:00
18:01
18:02
18:03
18:04
18:05

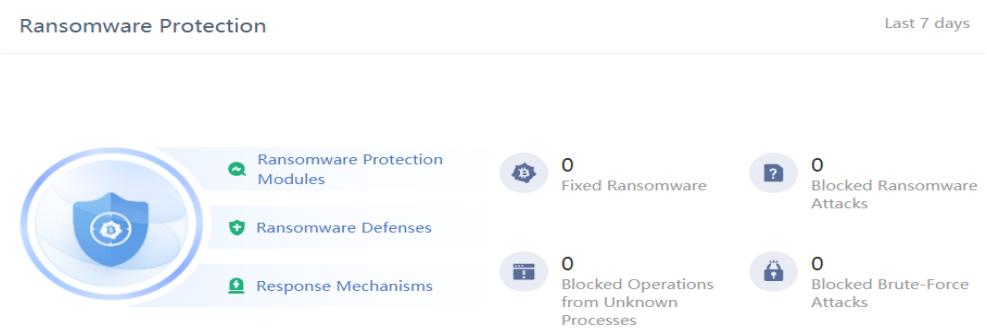
Pending Events

The **Pending Events** module displays the number of pending security events, such as ransomware, brute force attacks, botnets, WebShell backdoors, and high-risk vulnerabilities, and the number of endpoints affected by each type of event. You can click on an event. On the **Security Events** tab page under **Response** > **Threat Response** displayed, you can view details about the security event and the handling status. The following figure shows details about the status of brute force attacks.



Ransomware Protection

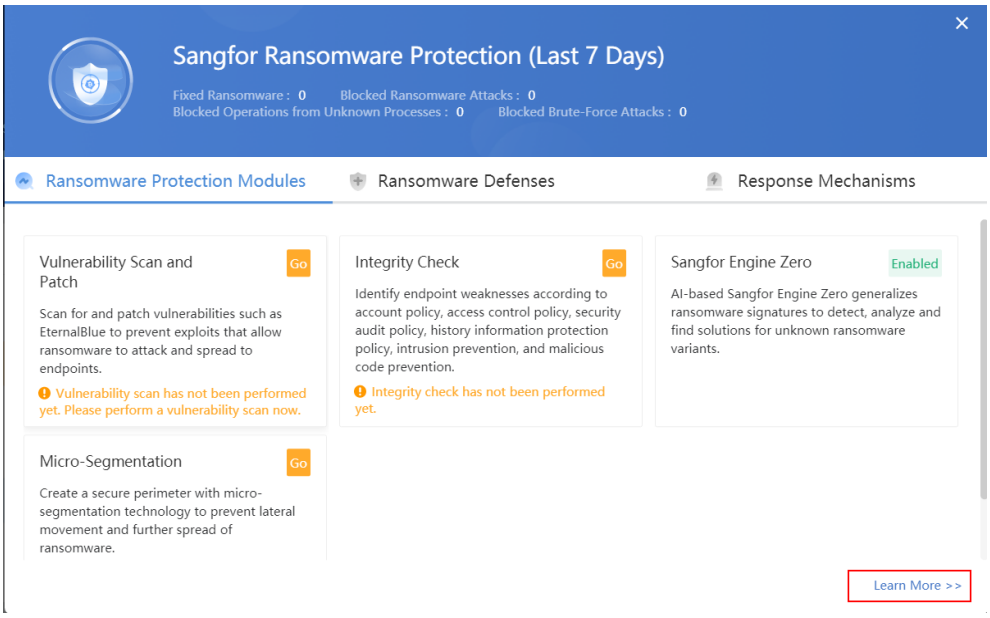
The **Ransomware Protection** module displays **Fixed Ransomware**, **Blocked Ransomware Attacks**, **Blocked Operations from Unknown Processes**, and **Blocked Brute-Force Attacks**, as shown in the following figure.



- **Fixed Ransomware**: number of ransomware viruses that the administrator or Manager has handled.
- **Blocked Ransomware Attacks**: number of suspicious ransomware behavior times detected and blocked by the ransomware honeypot on the Manager.
- **Blocked Operations from Unknown Processes**: number of Manager-detected and blocked operations or running times by non-whitelisted processes on protected directories.
- **Blocked Brute-Force Attacks**: number of brute force attacks blocked by the Manager.

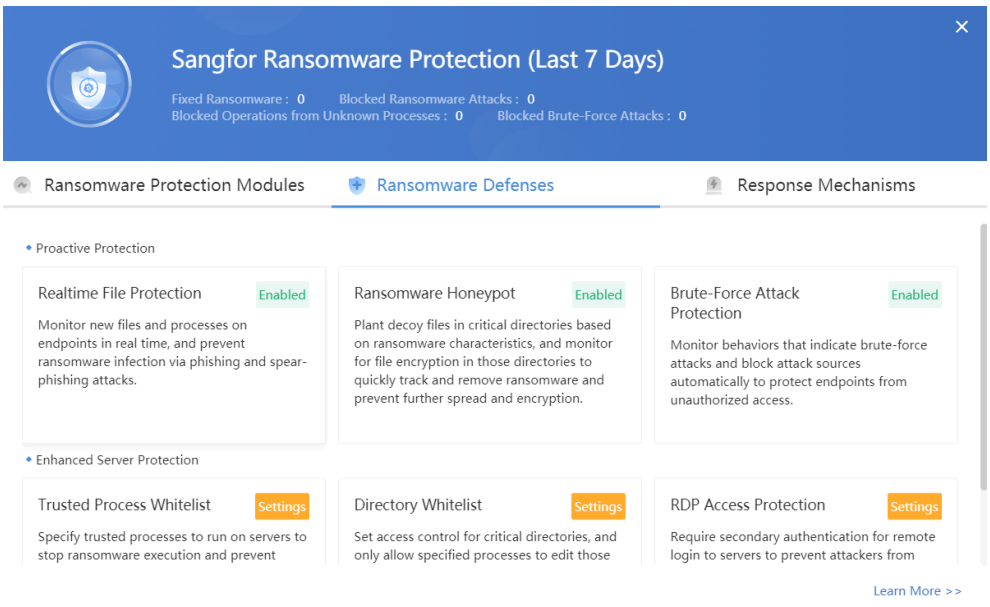
The **Ransomware Protection** module consists of **Ransomware Protection Modules**, **Ransomware Defenses**, and **Response Mechanisms**.

1. The following figure shows **Ransomware Protection Modules**.



- **Vulnerability Scan and Patch**: This function implements the Endpoint Secure to scan for and patch vulnerabilities such as EternalBlue with one click. The vulnerabilities can be exploited by ransomware to initiate attacks and spread. You can click **Go**. On the **Vulnerability Scan** page under **Detection** displayed, you can view the scan status, vulnerability quantity, and handling status and create vulnerability scan tasks to scan vulnerabilities.
- **Integrity Check**: This function allows the Endpoint Secure to identify endpoint weaknesses by the identity policy, access control policy, security audit policy, history information protection policy, intrusion prevention, and malicious code prevention. You can click **Go**. On the **Security & Integrity Check** page under **Detection** displayed, you can view endpoint integrity check details and perform an integrity check for a specified endpoint.
- **Sangfor Engine Zero**: AI-based Sangfor Engine Zero generalizes ransomware signatures to detect, analyze, and find solutions for unknown ransomware variants.
- **Micro-Segmentation**: This function allows the Endpoint Secure to create a dynamic security perimeter using the micro-segmentation technology to prevent lateral movement and further ransomware spread.

2. The following figure shows **Ransomware Defenses**.

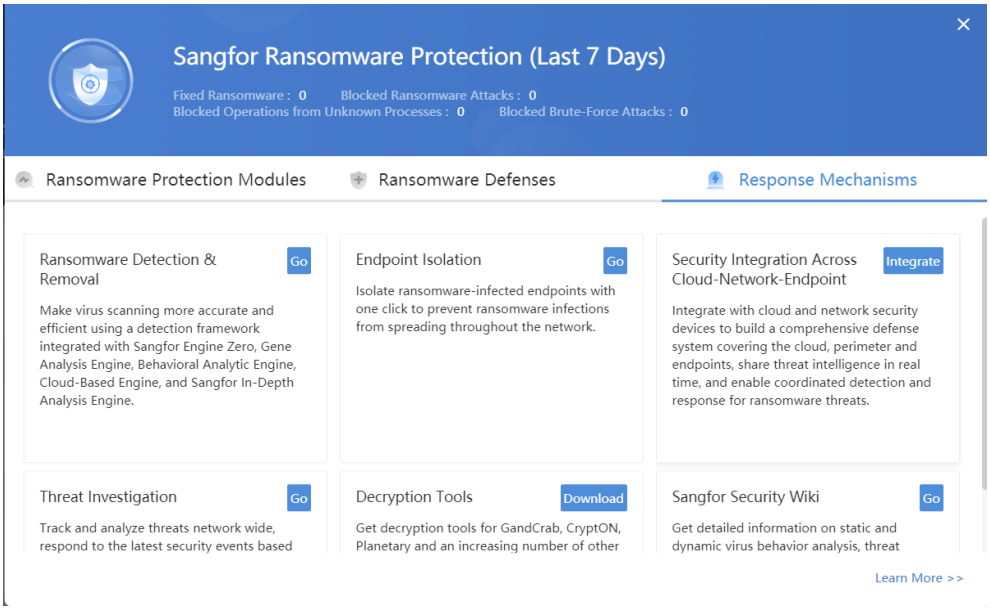


- **Realtime File Protection** (proactive protection): This function allows the Endpoint Secure to monitor new or changed files and processes on

endpoints in real-time to prevent ransomware infection by phishing and spear-phishing attacks.

- **Ransomware Honeypot** (proactive protection): This function allows the Endpoint Secure to plant decoy files in critical directories based on ransomware characteristics and monitor file encryption in those directories to quickly track and remove the ransomware, to prevent further ransomware spread and encryption.
- **Brute-Force Attack Protection** (proactive protection): This function allows the Endpoint Secure to monitor brute force password cracks and block attack IP sources automatically to protect endpoints from unauthorized access.
- **Trusted Process Whitelist** (enhanced server protection): This function allows the Endpoint Secure to specify trusted processes on servers running stable and fixed businesses so that ransomware processes can be stopped before being executed and unknown ransomware variants can be prevented from attacking critical assets.
- **Directory Whitelist** (enhanced server protection): This function allows the Endpoint Secure to set access control for critical directories and only allows specified processes to edit those directories to protect critical files from unauthorized access or modification.
- **RDP Access Protection** (enhanced server protection): This function adds secondary authentication for remote login to prevent attackers from controlling servers and launching ransomware attacks.

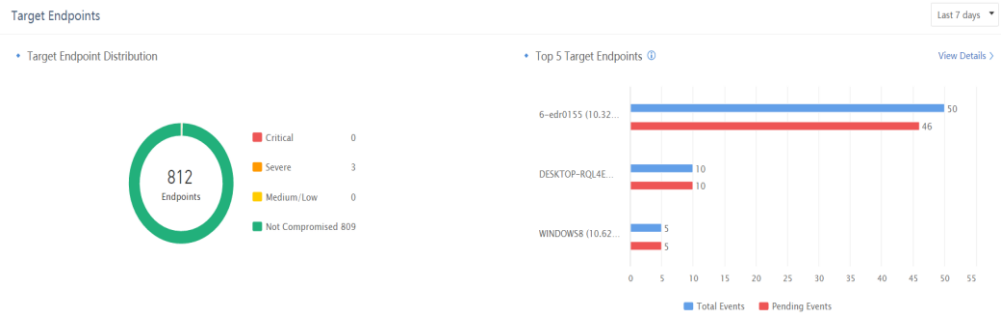
3. The following figure shows **Response Mechanisms**.



- **Ransomware Detection & Removal**: makes virus scanning more accurate and efficient using a detection framework integrated with Sangfor Engine Zero, Gene Analysis Engine, Behavior Analytic Engine, Cloud-based Engine, and Sangfor In-Depth Analysis Engine.
- **Endpoint Isolation**: isolates ransomware-infected endpoints with one click to prevent ransomware infections from spreading throughout the network.
- **Security Integration Across Cloud-Network-Endpoint**: integrates with cloud and network security devices to build a comprehensive defense system covering the cloud, perimeter, and endpoints, shares threat intelligence in real-time, and enables coordinated detection and response for ransomware threats.
- **Threat Investigation**: tracks and analyzes threats network-wide, responds to the latest security events based on IoC intelligence, and rapidly locates, fixes infected endpoints.
- **Decryption Tools**: gets decryption tools for GandCrab, CryptON, Planetary, and an increasing number of other ransomware that encrypt your files.
- **Sangfor Security Wiki**: gets detailed information on static and dynamic virus behavior analysis, threat reports, impacts, targeted attack events, and other related threat intelligence.

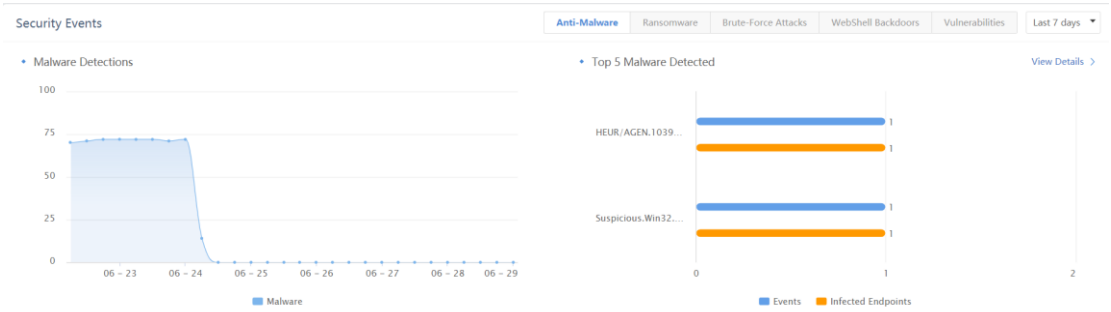
Target Endpoints

The **Target Endpoints** module consists of the **Target Endpoint Distribution** and **Top 5 Target Endpoints** charts, as shown in the following figure. **Target Endpoint Distribution** displays the numbers of critical, severe, medium/low, and not compromised endpoints. You can click a severity to go to the **Thread Response** page under **Response** and view details about the endpoints with this severity. **Top 5 Target Endpoints** lists the top 5 endpoints with the most found events and pending events. You can click **View Details** to go to the **Thread Response** page under **Response**.



Security Events

The **Security Events** module consists of the **Malware Detections** and **Top 5 Malware Detected** charts, as shown in the following figure.



- **Malware Detections**: displays statistics about malware detected in the last 7 days, last 30 days, and last 90 days, including ransomware, Trojan horses, and other malware.
- **Top 5 Malware Detected**: lists the top 5 malware detected on endpoints. You can click **View Details** in the upper-right corner to view detailed malware information. You can also click **Anti-Malware**, **Ransomware**, **Brute-Force Attacks**, **WebShell Backdoors**, or **Vulnerabilities** in the

upper-right corner of the **Security Events** module to view corresponding information and select a statistical period (**Last 7 days**, **Last 30 days**, or **Last 90 days**).

3.3 Endpoints

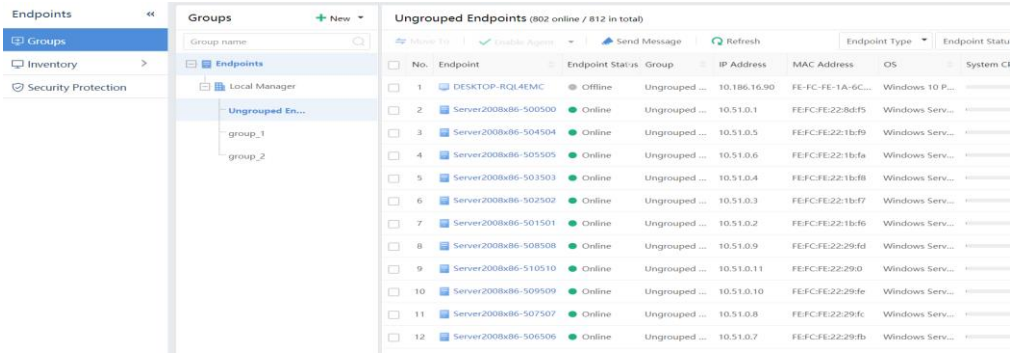
The **Endpoints** page allows you to discover, check, and group endpoints and use policies to manage endpoints and endpoint groups. The policies include **Basic Config**, **Anti-Malware**, **Realtime Protection**, **Server Protection**, **Trusted Files**, **Vuln Remediation**, **Unauthorized External Access**, and **USB Control**.

3.3.1 Groups

The **Groups** module uses tree-based grouping to manage connected endpoints in a unified manner.

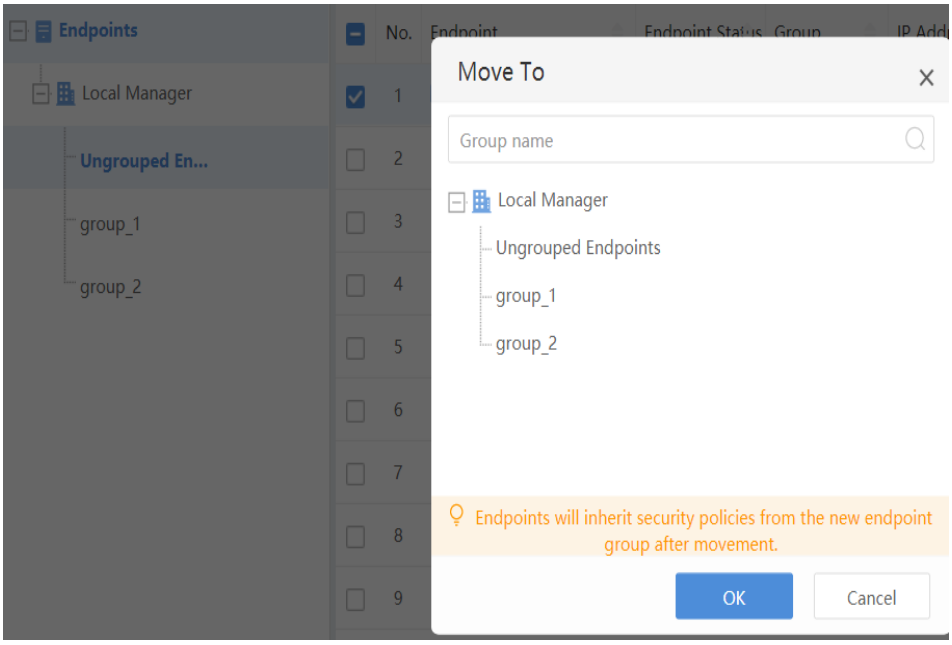
1. **Endpoint Information Display**

Endpoint information includes the endpoint name, status, group, IP address, MAC address, operating system, CPU usage, memory usage, owner, asset number, and asset location. You can click **...** on the right to filter and specify display options.

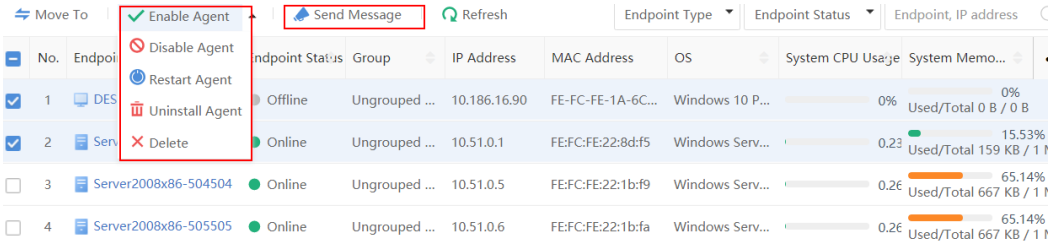


2. **Endpoint Management**

You can select endpoints and click **Move To** to move them to different groups, as shown in the following figure.



You can also select **Enable Agent**, **Disable Agent**, **Restart Agent**, or **Uninstall Agent**, **Delete**, and **Send Message** for selected endpoints, as shown in the following figure.



3.3.1.1 Creating Endpoint Groups

After the Agent is installed on an endpoint, the endpoint is automatically listed to **Ungrouped Endpoints** under **Groups**. You can group ungrouped endpoints based on business. Endpoints can be grouped manually, automatically, or using an XLS or XLSX file.

Manual Grouping

You can create a group, manually select endpoints, and move them to the group. The procedure is as follows:

1. Choose **Endpoints** > **Groups**, and click **New**.
2. On the displayed **Add Group** page, specify **Group Name** and **Added To Group**, do not enable **Auto Grouping**, and click **OK**.

3. Select endpoints from **Ungrouped Endpoints** and click **Move To**. On the **Move To** page, select the specific group and click **OK**.

NOTE

Endpoints will inherit security policies from the new endpoint group after movement.

Auto Grouping

You can specify IP addresses or IP address ranges when creating a group. After the group is created, the system automatically moves endpoints with the specified IP addresses or the group's specified IP address ranges to the group. The procedure is as follows:

1. Choose **Endpoints** > **Groups**, and click **New**.
2. On the **Add Group** page, specify **Group Name** and **Added To Group**, enable **Auto Grouping**, set IP addresses or IP address ranges, and click **OK**.
3. After the group is generated, you can find that the endpoints with the specified IP addresses or in the specified IP address ranges are already in the group. You can also select endpoints from **Ungrouped Endpoints** and move them to the group.

NOTE

Endpoints will inherit security policies from the new endpoint group after movement.

Importing and Exporting Groups

After editing an XLS or XLSX file of endpoints, you can import the file to batch add endpoints to a group. For existing groups, you can export endpoints in a group to an XLSX file. The procedures are as follows:

Importing a Group

1. Choose **Endpoints** > **Groups**, click the drop-down list icon next to **New** and

choose **Import**.

2. Click **Sample File** to download it and edit the file content as instructed.
3. Click **Browse**, select the edited XLS or XLSX file, and upload it.
4. Select an import method and click **OK**. Import methods include:
   - Retain unchanged and existing objects take higher priority.
   - Retain unchanged but imported objects take higher priority.
   - Clear all groups except Local Manager and Ungrouped Endpoints and group endpoints based on the new auto grouping rules.
5. On the **Add Group** page, specify **Group Name** and **Added To Group**, enable **Auto Grouping**, set IP addresses or IP address ranges, and click **OK**.
6. After the group is generated, you can find that the endpoints with the specified IP addresses or in the specified IP address ranges are already in the group. You can also select endpoints from **Ungrouped Endpoints** and move them to the group.

NOTE

Endpoints will inherit security policies from the new endpoint group after movement.

Exporting a Group

1. Choose **Endpoints** > **Groups**, click the drop-down list icon next to **New** and choose **Export**.
2. On the displayed **Export** page, select **Groups** or **Endpoints** for **Object**. When **Endpoints** are selected, you can select endpoints from different groups.
3. Select a group and endpoints and click **OK**. The system automatically exports the endpoints to an XLSX file.

Auto Grouping

The **Auto Grouping** module creates and manages auto grouping policies in a unified manner. The detailed operations are as follows:

Creating and Deleting an Auto Grouping Policy

1. To create an auto grouping policy, choose **Endpoints** > **Groups**, click the drop-down list icon next to **New** and choose **Auto Grouping**.
2. On the **Auto Grouping** page, click **New**. Next, specify **Group Name**, enable **Auto Grouping**, set IP addresses or IP address ranges, and click **OK**.
3. Select the auto grouping policy on the **Auto Grouping** page and click **Delete** in the **Operation** column to delete an auto grouping policy.

NOTE

After an auto grouping policy is deleted, the auto grouping will be disabled for this group.

Editing Auto Grouping

1. Choose **Endpoints** > **Groups**, click the drop-down list icon next to **New** and choose **Auto Grouping**.
2. On the **Auto Grouping** page, select an auto grouping policy and click **Edit** in the **Operation** column.

NOTE

You can edit IP addresses or IP address ranges for an auto grouping policy only when it is enabled.

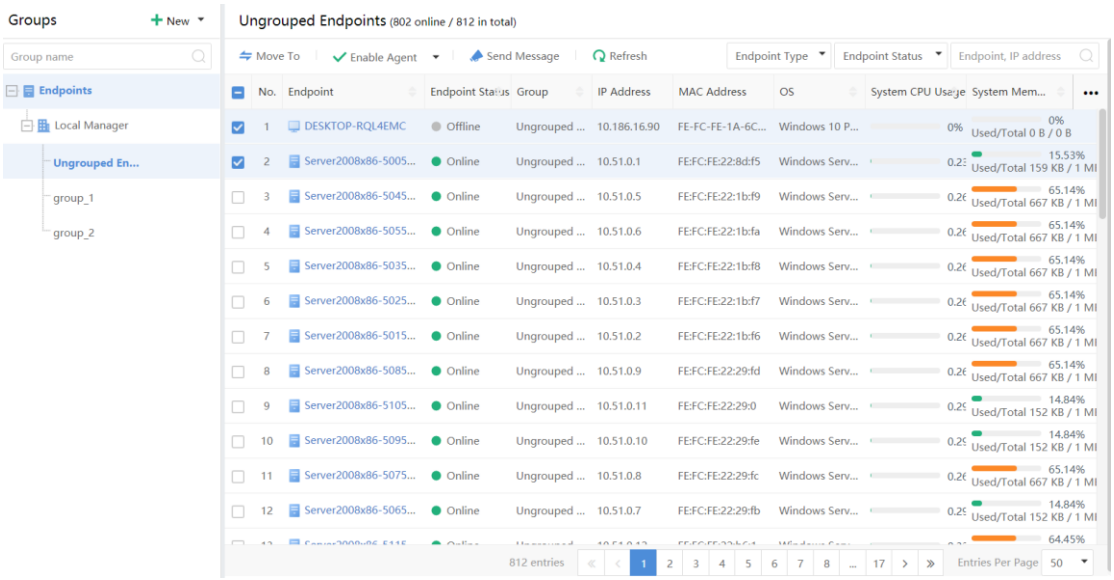
Enabling and Disabling Auto Grouping

You can enable and disable auto grouping based on business. The procedure is as follows:

1. Choose **Endpoints** > **Groups**, click the drop-down list icon next to **New** and choose **Auto Grouping**.
2. On the **Auto Grouping** page, click **Enable** or **Disable** in the **Status** column to enable or disable auto grouping. Alternatively, click **Edit** in the **Operation** column and enable or disable **Auto Grouping** on the editing page.

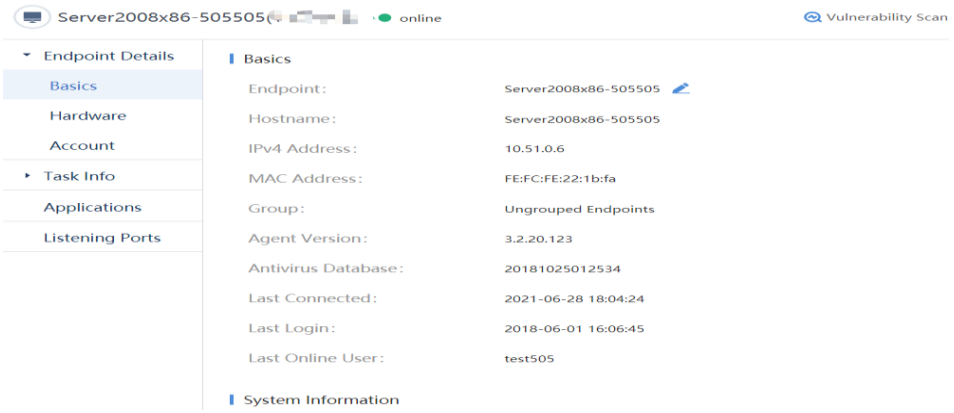
3.3.1.2 Endpoint Information Display

The **Groups** page displays basic information about all endpoints, as shown in the following figure.



Basic information includes the endpoint status, group, IP address, MAC address, operating system, CPU usage, memory usage, owner, asset number, and asset location. You can click **...** on the right to filter and specify display options.

When you click an endpoint name, the **Endpoint Details** page is displayed, as shown in the following figure.



The information is classified as follows:

Endpoint Details

1. **Basics**

The **Basics** page displays the following information:

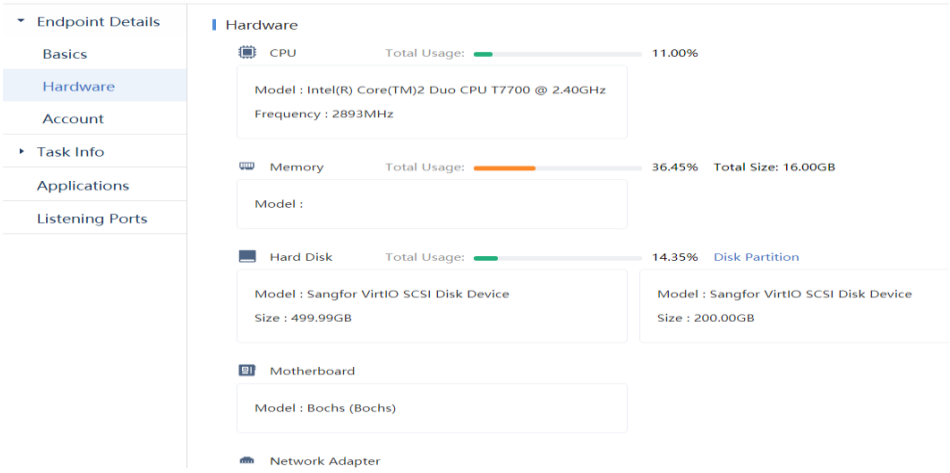
Basic information: includes the endpoint name (editable), hostname, IPv4 address, MAC address, group, Agent version, antivirus database version, last connected time, last login time, and last online user.

System information: includes the operating system, version number, activation status, and installation time.

Management information (editable): includes the asset owner, host, asset number, asset location, staff No., phone number, and email address.

2. **Hardware**

The **Hardware** page displays the models and usage of the CPU, memory, hard disk, motherboard, network adapter, sound card, and graphics card.

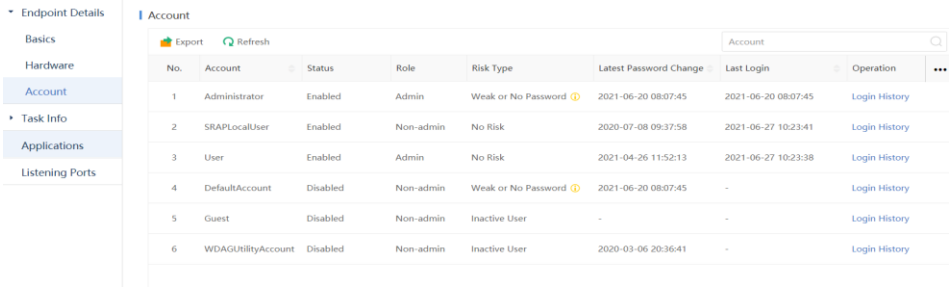


3. **Account**

The **Account** page displays the name, status, type, role, risk type (click the exclamation mark to view detailed risks), latest password change time, last login time, password status, and login history of accounts created for the endpoint.

NOTE

You can click **...** on the right to filter and specify display options.

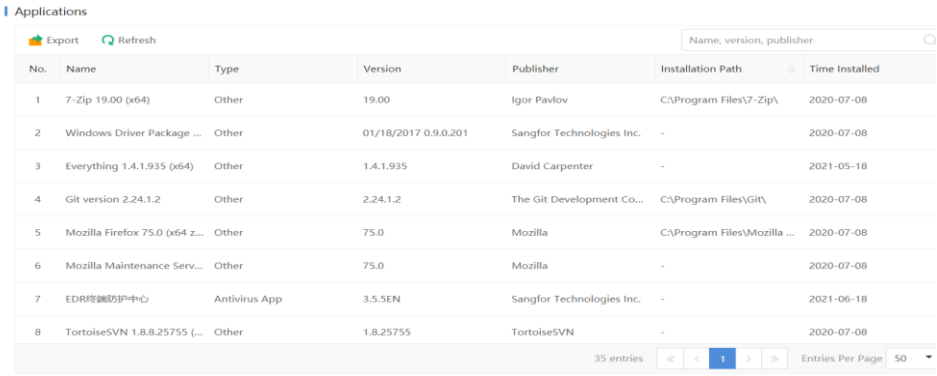


Task Info

Task Info contains the **Processes**, **Services**, **Connections**, **Startup Items**, **Scheduled Tasks**, and **Sharing** nodes.

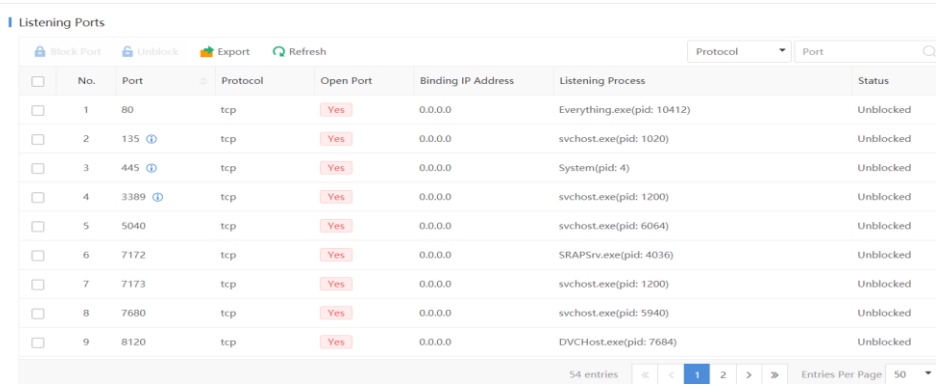
Applications

The **Applications** page displays the name, type, version, publisher, installation path, and installation time of software installed on the endpoint. You can click **Export** to export all installed software and filter software by software name, version, or publisher.



Listening Ports

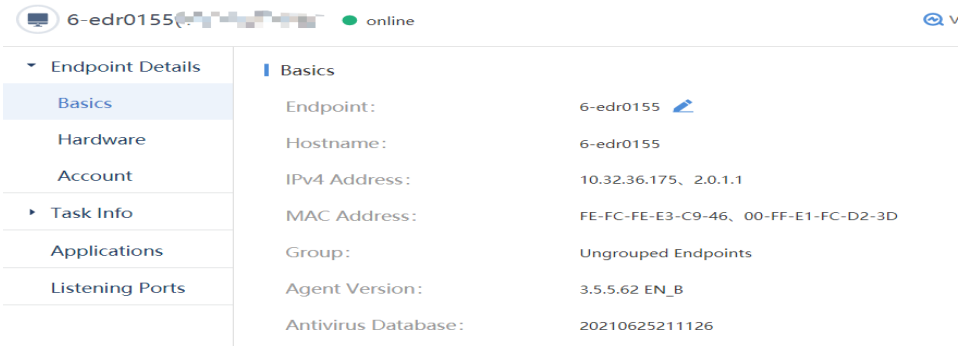
The **Listening Ports** page displays the port number, protocol, bound IP address, listening process, open port, and status (blocked or unblocked) of listening ports on the endpoint. You can select ports to block or unblock, click **Export** to export all listening ports, and search ports by protocol and port number.



3.3.1.3 Remote Endpoint Management

Command Delivery

After you click the name of an online endpoint to enter the **Endpoint Details** page, you can deliver commands, such as **Vulnerability Scan**, **Quick Scan**, and **Full Scan** to the endpoint, as shown in the following figure.



If Agent installation is abnormal, you can perform **Enable Agent**, **Disable Agent**, **Uninstall Agent**, and other operations for the endpoint on the Endpoint Secure Manager.

NOTE

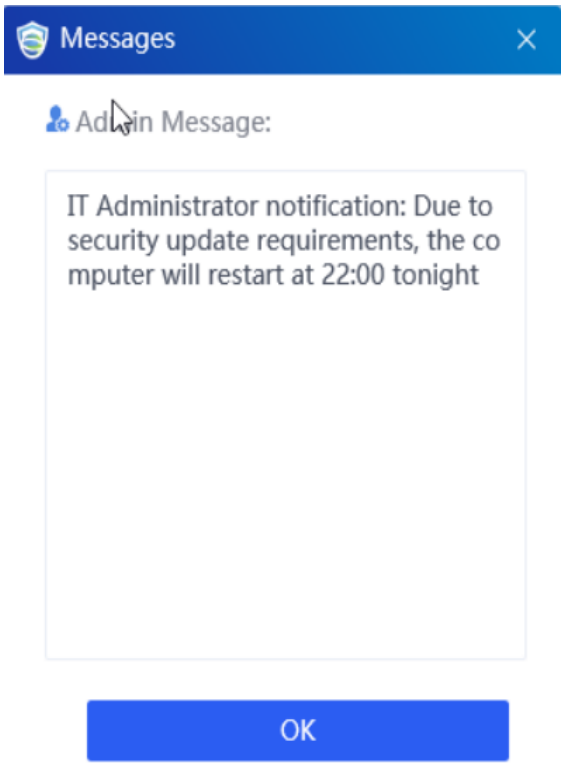
On the **Endpoints** page, you can select multiple endpoints and perform **Enable Agent**, **Disable Agent**, and other operations for these endpoints.

To release a license, uninstall the Agent from an endpoint and delete the endpoint from the Endpoint Secure Manager.

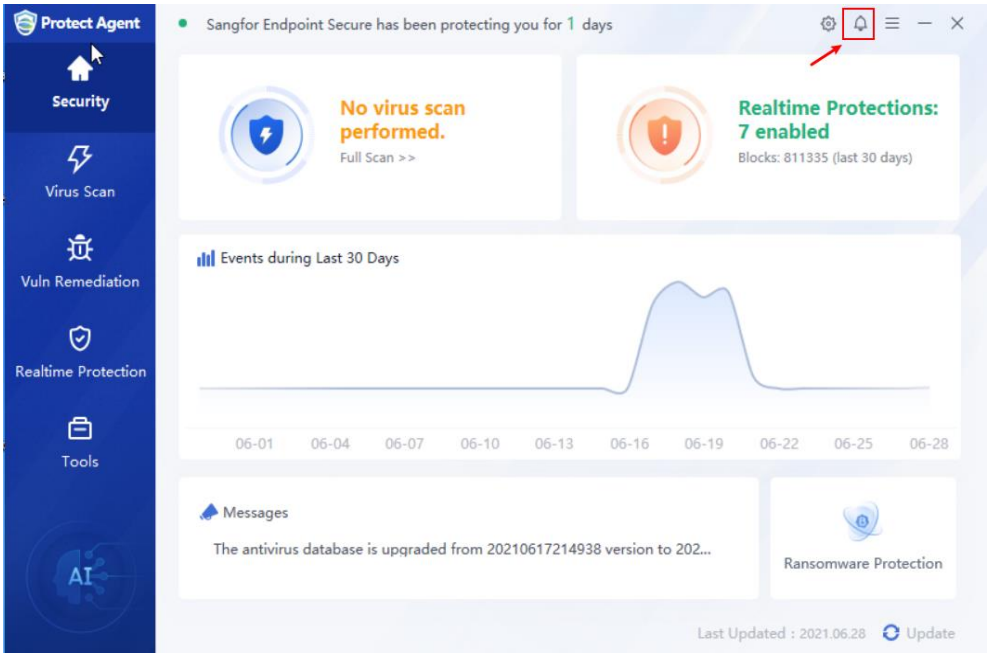
Send Message

On the **Endpoints** page, you can select one or more endpoints with the Agent installed and send messages to these endpoints. The procedure is as follows:

1. Choose **Endpoints** > **Group**, select one or more endpoints, and click **Send Message** in the status bar.
2. On the **Send Message** page, complete information editing and click **OK**. Selected endpoints will receive the corresponding message, as shown in the following figure.



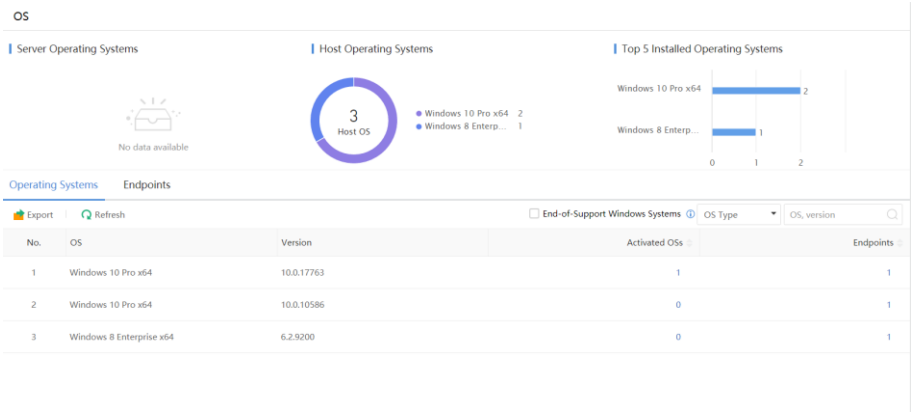
3. Click **OK** or **X** in the upper-right corner on the endpoint to close the message. You can click the **Messages** icon shown in the following figure to view historical messages.



3.3.2 Inventory

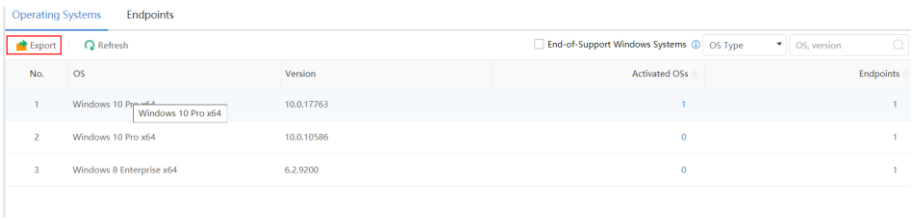
The **Inventory** module checks up endpoints on the entire network and displays endpoint statistics. It includes the **OS**, **Applications**, **Listening Ports**, and **Users** nodes. Endpoint inventory data does not contain Mac endpoints because Mac endpoint information is not collected.

OS

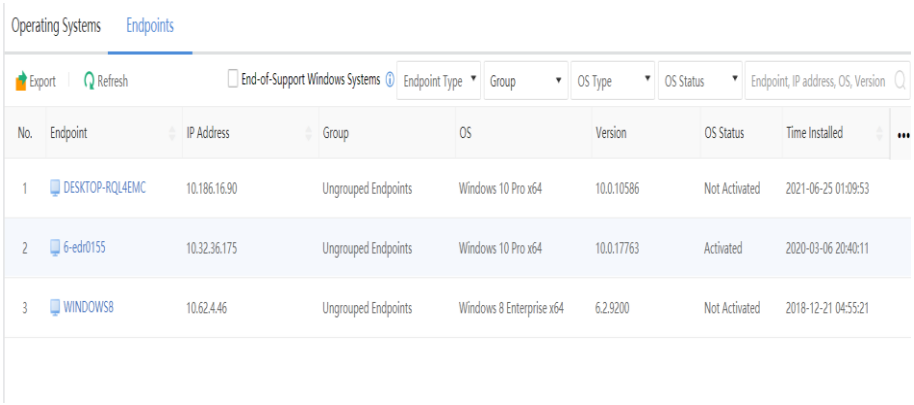


The **OS** page displays the distribution of operating system versions of endpoints on the entire network, as shown in the preceding figure.

1. The detailed information includes the proportion of server and PC operating system versions and the top 5 operating systems installed on the entire network.
2. On the **Operating Systems** tab, you can view the number of endpoints that installed and activated each operating system. When you click the quantity, the details page is displayed. You can also click **Export**, to export the operating system information to a form, as shown in the following figure.



3. On the **Endpoints** tab, you can view the IP address, group, OS type, version, activation status, installation time, and owner information of endpoints, as shown in the following figure.

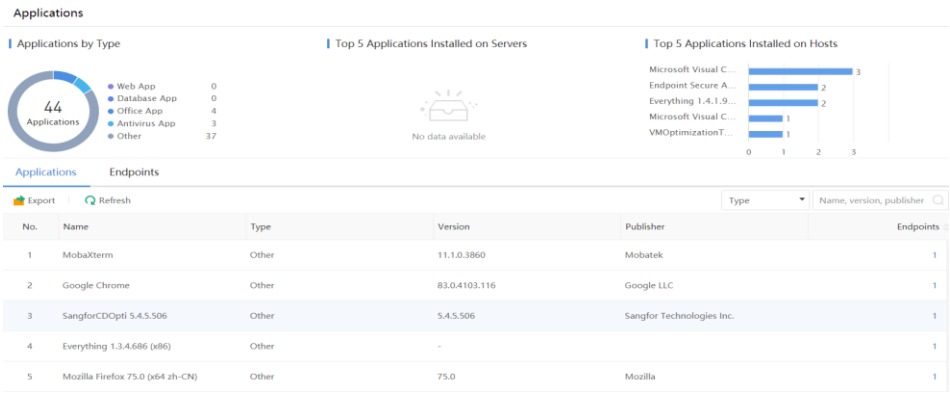


NOTE

You can click **Export** to export endpoint information to a form to facilitate further statistical analysis.

You can filter endpoints by endpoint type, group, OS type, and activation status and search for endpoints in the search box.

Applications

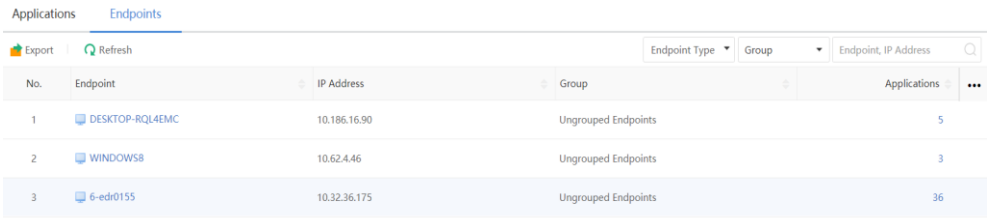


The **Applications** page displays the summary and detailed information of applications installed on hosts on the entire network, as shown in the preceding figure. The information helps check risky applications on the entire network and take security protection measures, such as version update and application security hardening.

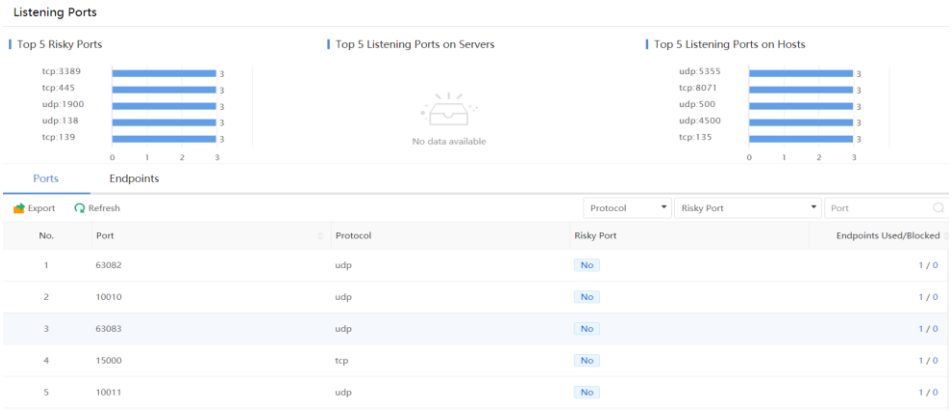
1. The detailed information includes applications type statistics of endpoints on the entire network and the top 5 applications installed on servers and PCs.
2. On the **Applications** tab, you can view information, such as the application

type, version, publisher, and endpoints that install the applications.

3. On the **Endpoints** tab, you can view groups and installed applications of different types of endpoints. You can click the application quantity to view detailed information, filter endpoints by endpoint type or group, and search for endpoints in the search box.

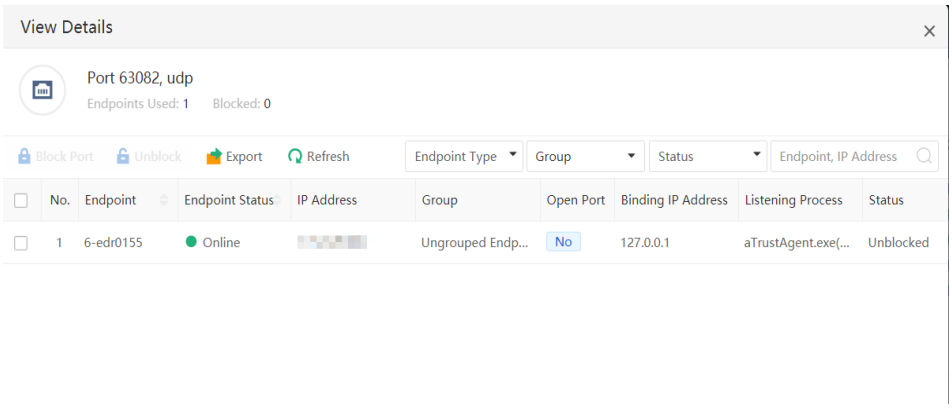


Listening Ports



The **Listening Ports** page displays open ports of endpoints on the entire network. You can view and handle risky ports globally or by server or host, as shown in the preceding figure.

1. The detailed information includes the top 5 risky ports and top 5 listening ports on servers and PCs.
2. You can view the number of endpoints on which a specific port is opened on the **Ports** tab. You can click a number in the **Endpoints Used/Blocked** column to go to the endpoint details page of a port for further analysis, as shown in the following figure.

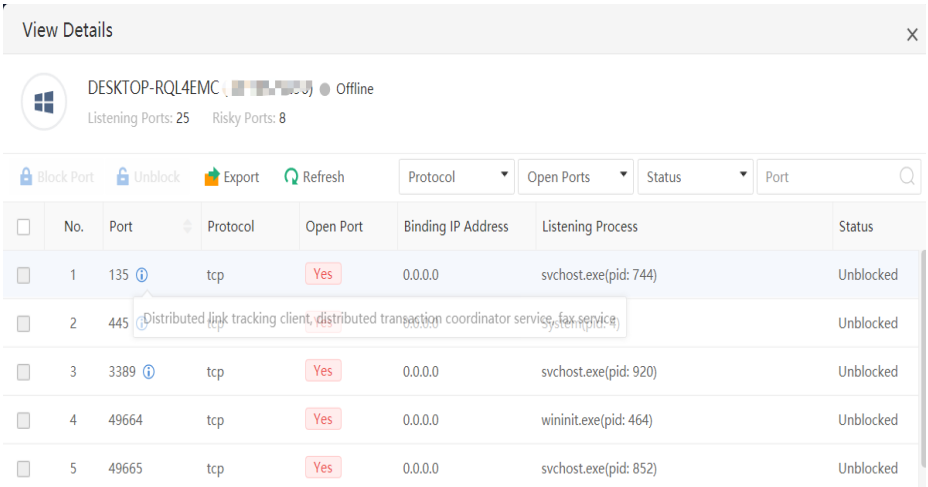


NOTE

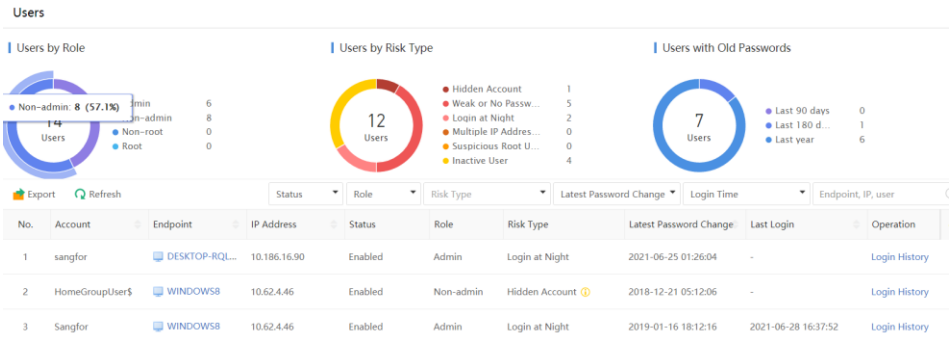
Block Port: You can select endpoints for which a port needs to be blocked and click **Block Port** to block the port for the selected endpoints. You can click **Unblock** to unblock a blocked port.

Export: You can click **Export** to export endpoint information to a form to facilitate further statistical analysis.

3. On the **Endpoints** tab, you can view the listening port quantity, status, name, IP address, and each group of the endpoint. You can click the listening port quantity of an endpoint to view detailed information about the listening ports of the endpoint. You can block ports based on actual requirements, as shown in the following figure.

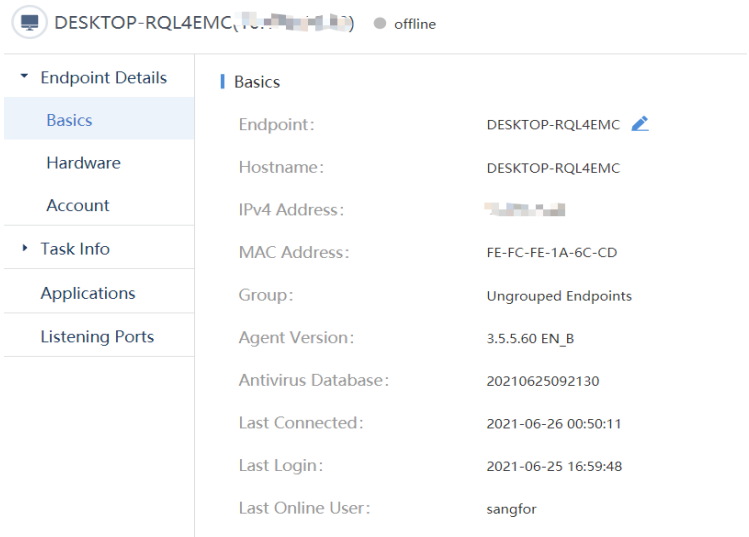


Users



The **Users** page displays account information of hosts on the entire network, including the account status, account type, role, and password status. Based on account information, the Manager further analyzes risks and provides account risk notifications, such as hidden account, weak password, suspicious root user, inactive user, log in at night, and multiple IP addresses, as shown in the preceding figure. It helps reduce host risks.

1. The detailed information includes statistics of users by role, by risk type, and with old passwords.
2. You can filter accounts by status, role, risk type, latest password change, and last login. You can also enter an endpoint name, IP address, or account name in the search box to search for an account. When you click an endpoint, the **Endpoint Details** page is displayed, as shown in the following figure.



3.3.3 Security Protection

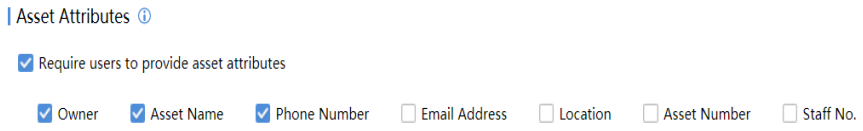
The **Security Protection** module formulates security policies for endpoint groups. It consists of the **Basic Config**, **Anti-Malware**, **Realtime Protection**, **Server Protection**, **Trusted Files**, **Vuln Remediation**, **Unauthorized External Access**, and **USB Control** tabs.

3.3.3.1 Basic Config

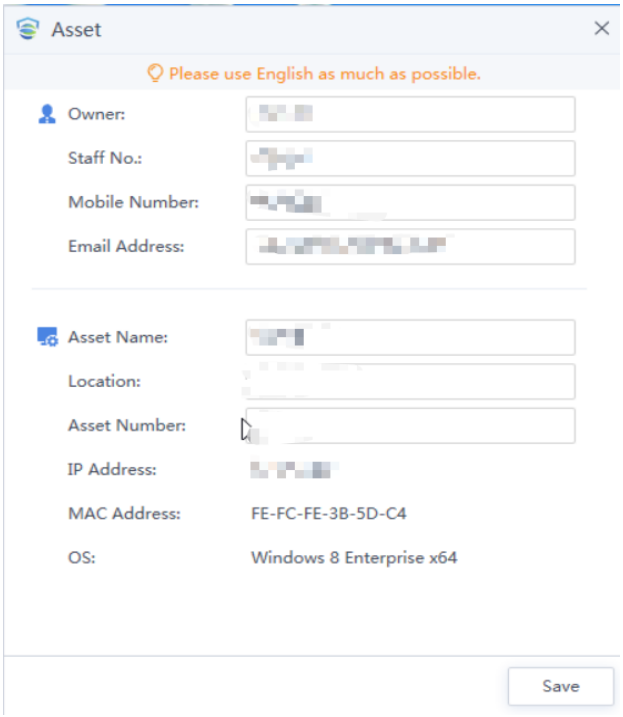
You can configure **Asset Attributes**, **Administrator Contact Information**, **Notifications**, **Agent Administration Passwords**, and **Endpoint Behavior Data & Log Collection** for Windows endpoints on the **Basic Config** tab. The configuration methods are as follows:

Asset Attributes

If you select **Require users to provide asset attributes**, managed endpoints need to register asset information on the Manager. You can specify the asset information to be reported to the Manager. The asset information includes the owner, asset name, phone number, email address, asset location, asset number, and staff No., as shown in the following figure.

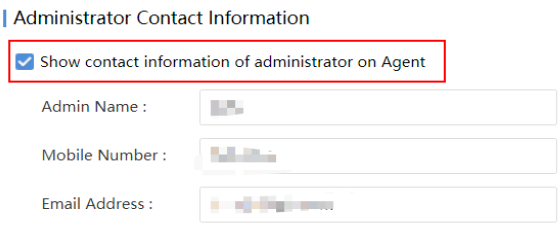


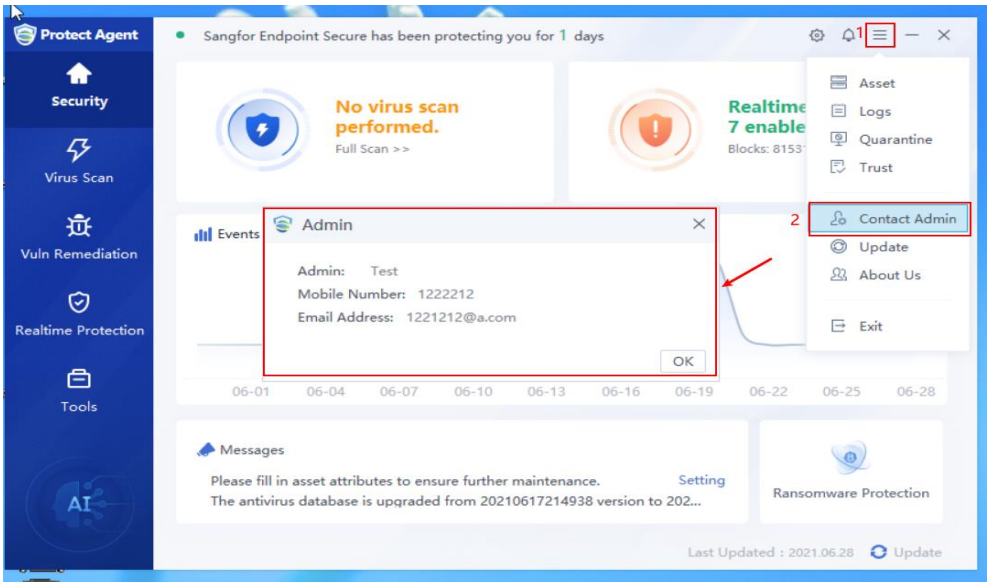
After **Asset Attributes** is configured, endpoint users can view details in system messages and complete endpoint registration as required, as shown in the following figure.



Administrator Contact Information

If you select **Show contact information of administrator on Agent** and edit the administrator's contact information, including the name, mobile number, and email address, as shown in the following figure, endpoint users can view the administrator's contact information.

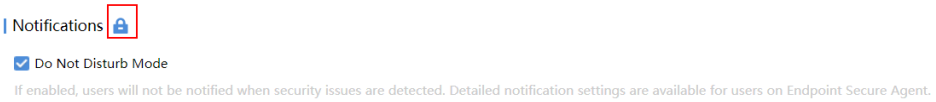




To query the administrator's contact information on an endpoint, perform the operations shown in the following figure.

Notifications (Do Not Disturb Mode)

If you select **Do Not Disturb Mode**, endpoint users will not be notified when detected security issues. The following figure shows the configuration page.

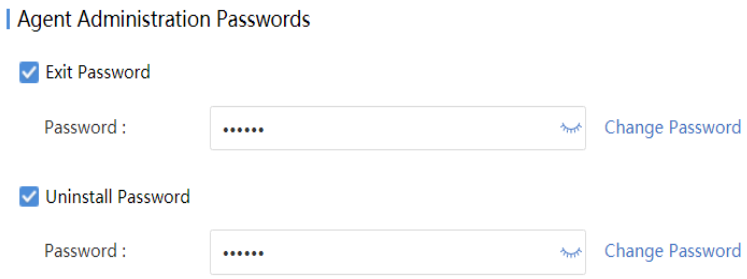


NOTE

If you click the lock icon next to **Notifications** to lock the notification settings, endpoint users cannot modify notification settings on the Agent. In this case, notification settings on the Manager prevail. If you click the lock icon next to **Notifications** again to unlock the notification settings, endpoint users can modify notification settings on the Agent.

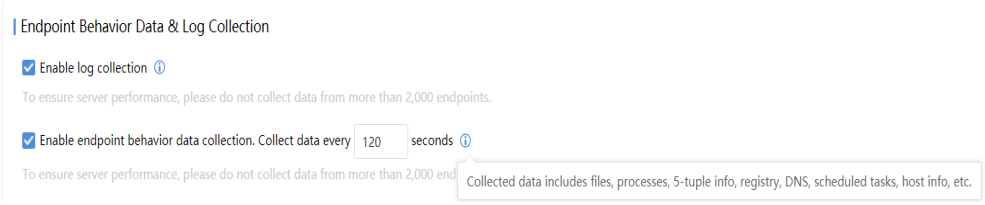
Agent Administration Passwords

After you configure agent administration passwords, endpoint users need to enter the configured password when they exit or uninstall the Agent. You can set the Password parameter to different values for **Exit Password** and **Uninstall Password**, as shown in the following figure.



Endpoint Behavior Data & Log Collection

If you select **Enable log collection**, logs, including event management logs of Windows endpoints, are collected. You can also select **Enable endpoint behavior data collection** and set the data collection interval. The collected behavior data includes information about files, processes, networks, registries, DNS, scheduled tasks, and hosts.



NOTE

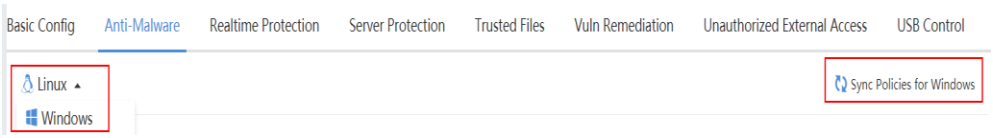
It is recommended that the number of endpoints collecting data does not exceed 2000 to ensure server performance.

After you configure information on the **Basic Config** tab, click **Save** to save the settings. To restore the default settings, click **Restore Defaults**. To apply the settings to subgroups, click **Apply to Subgroups**.

3.3.3.2 Anti-Malware

The **Anti-Malware** tab enables you to configure scheduled scan policies, virus

scan policies, and antivirus database and security engine update policies for Windows and Linux endpoints. macOS endpoints support virus scan but do not support policy configuration. The following sections describe how to configure the policies.

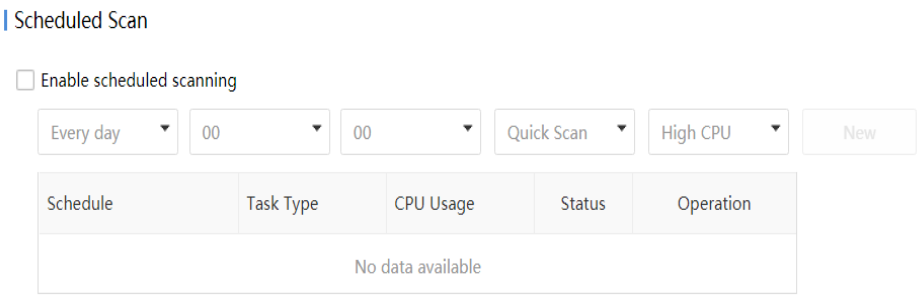


NOTE

You can click the downwards arrow next to **Windows** or **Linux** to switch between the Windows and Linux operating systems. You can synchronize the policies that are configured for Windows endpoints to Linux endpoints.

Scheduled Scan

After you configure the scheduled scan, the system will perform scans and removes viruses for endpoints based on the virus scan configuration on the internal network at the specified time. The following figure shows the configuration page.



Scheduled scan supports the quick scan and scan types, and each scan type supports the **High CPU**, **Balanced**, and **Low CPU** scan modes. The three modes differ from each other mainly in CPU usage.

- **High CPU**: Scan is performed at full speed, and the CPU usage of the scanning is not limited.
- **Balanced**: A balance is reached between the scan speed and CPU usage, and the CPU usage cannot exceed 30%.

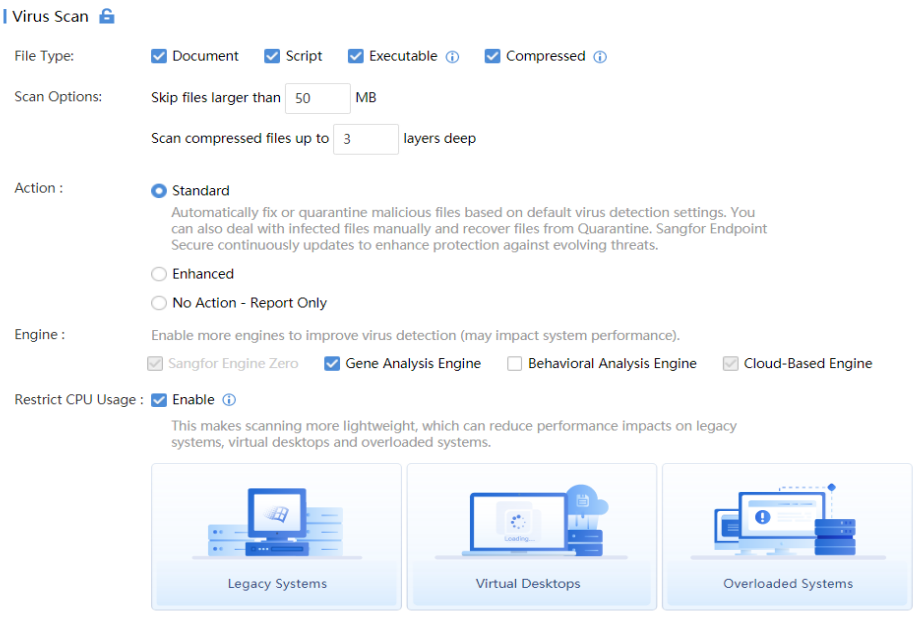
- **Low CPU**: Less CPU resources are occupied during the scan, and the CPU usage cannot exceed 10%.

Virus Scan

In the **Virus Scan** area, you can configure the types of files to be scanned, scan options, action to perform when malicious files are detected, scan engine, and limits on the CPU usage. The following figure shows the configuration page.

NOTE

If you click the lock icon next to **Virus Scan** to lock the virus scan settings, endpoint users cannot modify virus scan settings on the Agent. In this case, virus scan settings on the Manager prevail. If you click the lock icon next to **Virus Scan** again to unlock the virus scan settings, endpoint users can modify virus scan settings on the Agent.



File Type: The options include **Document**, **Script**, **Executable**, and **Compressed**.

NOTE

1. Most viruses are executable files. If executable files are not scanned, significant risks may arise. In quick scan mode, Sangfor Endpoint Secure scans only executable files. Therefore, you are advised to select **Executable** for **File Type**. By default, all file types are selected.
2. Sangfor Endpoint Secure supports 23 types of compressed files, including 7z, XZ, BZIP2, GZIP, TAR, ZIP, and WIM. You can click ⓘ next to **Compressed** to view the details.

Scan Options: You can specify the limit on the size of files to be scanned and the number of directory levels to be scanned for compressed files.

Action: You can specify the action to perform when malicious files are detected. The options include **Standard**, **Enhanced**, and **No Action - Report Only**. By default, **Standard** is selected.

- **Standard**: quarantines malicious files in the blacklist and reports detection logs for files that threaten system security but are not on the blacklist.
- **Enhanced**: quarantines all the detected files that threaten system security.
- **No Action - Report Only**: reports security logs for all files that threaten system security but does not quarantine the files. This option is suitable for scenarios in which an on-duty security expert is responsible for fixing threats.

Engine: The options include **Sangfor Engine Zero**, **Cloud-Based Engine**, **Gene Analysis Engine**, and **Behavioral Analysis Engine**.

- By default, **Sangfor Engine Zero** and **Cloud-Based Engine** are selected and cannot be deselected.
- **Gene Analysis Engine** and **Behavioral Analysis Engine** are optional.
- If you select more engines, the virus detection rate is improved. However, the system performance is affected.

Restrict CPU Usage: If you select **Enable**, the amount of CPU resources that Sangfor Endpoint Secure can use to scan for viruses is limited, and the virus scan time may increase. You can select Enable if you want to scan viruses in legacy

systems, virtual desktops, and high-load systems.

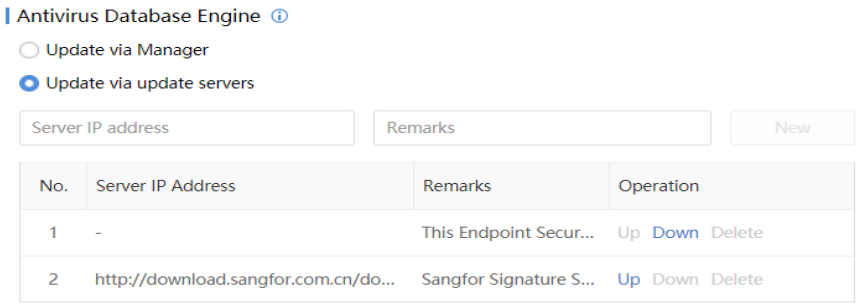
NOTE

If you select **Enable** for **Restrict CPU Usage**, the number of CPU resources that Sangfor Endpoint Secure can use varies based on the scan mode.

1. **High CPU**: The CPU usage cannot exceed 50%.
2. **Balanced**: The CPU usage cannot exceed 20%.
3. **Low CPU**: The CPU usage cannot exceed 5%.

Antivirus Database Engine

You can select **Update via Manager** or **Update via update servers** to specify the update server for the antivirus database. If you select **Update via update servers**, you can configure multiple update servers, as shown in the following figure.



Advanced (Supported Only for Windows Endpoints)

In the **Advanced** area, you can select **Enable heuristic scanning**. The heuristic scan mode increases the sensitivity of AI-based computing and the heuristic level of analysis, which improves the virus detection rate. However, false positives may occur. Before you enable heuristic scan, ask the service provider to analyze the impact.

After you configure information on the **Anti-Malware** tab, click **Save** to save the settings. To restore the default settings, click **Restore Defaults**. To apply the settings to subgroups, click **Apply to Subgroups**.

3.3.3.3 Realtime Protection

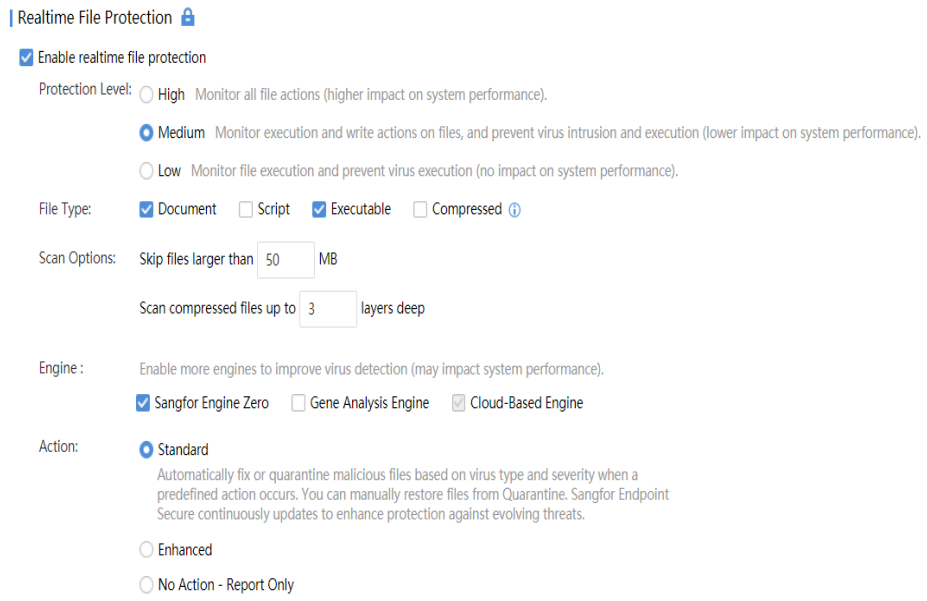
You can configure **Realtime File Protection**, **WebShell Detection**, **Brute-Force Attack Protection**, **Ransomware Protection**, and **Fileless Attack Protection** for Windows endpoints on the **Realtime Protection** tab. You can also configure **WebShell Detection** and **Brute-Force Attack Protection** for Linux endpoints on the tab. Currently, you cannot configure real-time protection for macOS endpoints.

NOTE

You can click next to **Realtime File Protection** to lock real-time file protection settings. In this case, the Manager delivers the configured real-time file protection policy to the Agent, and endpoint users cannot configure real-time file protection policies on the Agent. By default, endpoint users are allowed to configure real-time file protection policies on the Agent.

Realtime File Protection (Only for Windows Endpoints)

If you select **Enable realtime file protection**, the system protects files on endpoints in real-time. The following figure shows the configuration page.



You can configure the following parameters:

Protection Level: The options include **High**, **Medium**, and **Low**. The capabilities to defend against malicious files vary based on the protection level.

- **High**: monitors all actions performed on files. Protection at this level has a significant impact on system performance.
- **Medium**: monitors execute and write actions performed on files to prevent virus intrusion and execution. Protection at this level has little impact on system performance.
- **Low**: monitors execute actions performed on files to prevent virus execution. Protection at this level has no impact on system performance.

File Type: You can select multiple types of files to be scanned.

Scan Options: You can specify the limit on the size of files to be scanned and the number of directory levels to be scanned for compressed files. Most malicious files are small in size.

Engine: Three engines are available for real-time file protection. By default, **Cloud-Based Engine** is selected and cannot be deselected. **Sangfor Engine Zero** and **Gene Analysis Engine** are optional. If you select more engines, the virus detection rate is improved. However, the system performance is affected.

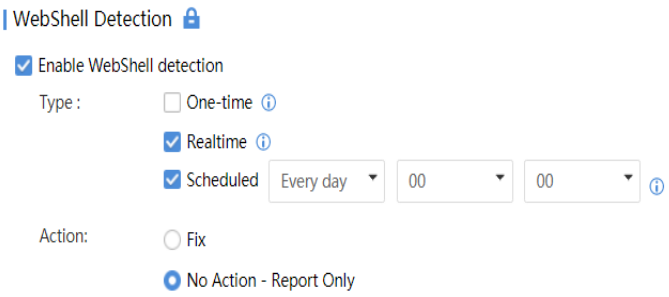
Action: You can specify the action to perform when malicious files are detected. The options include **Standard**, **Enhanced**, and **No Action - Report Only**. By default, **Standard** is selected.

- **Standard**: quarantines malicious files in the blacklist and reports detection logs for files that threaten system security but are not on the blacklist.
- **Enhanced**: quarantines all the detected files that threaten system security.
- **No Action - Report Only**: reports security logs for all files that threaten system security. This option is suitable for scenarios in which an on-duty security expert is responsible for fixing threats.

WebShell Detection

In the **WebShell Detection** area, you can configure the WebShell detection type and the action to perform when WebShell backdoors are detected. WebShell detection detects WebShell backdoors in the root directories and their subdirectories on web servers running Windows Server or Linux operating

systems. The following figure shows the configuration page.



You can configure the following parameters:

Type: The options include **One-time**, **Realtime**, and **Scheduled**.

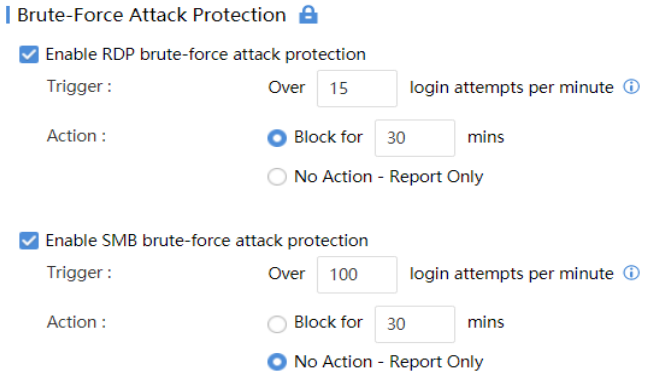
- **One-time**: scans the root directories and their subdirectories on web servers upon the first installation of the Agent.
- **Realtime**: scans new files in the root directories and their subdirectories on web servers.
- **Scheduled**: periodically scans all files in the root directories and their subdirectories on web servers.

Action: You can specify the action to perform when WebShell backdoors are detected. The options include **Fix** and **No Action - Report Only**.

Brute-Force Attack Protection

In the **Brute-Force Attack Protection** area, you can enable RDP brute-force attack protection and SMB brute-force attack protection for Windows endpoints. For Linux endpoints, you can enable SSH brute-force attack protection.

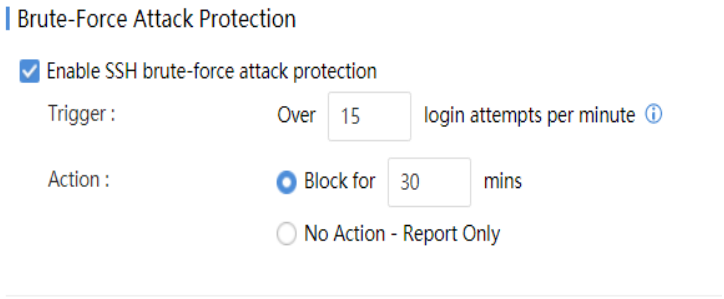
1. The following figure shows the configuration page for Windows endpoints.



You can configure the following parameters:

- **Trigger**: You can specify a threshold for the number of login attempts per minute. Brute-force attack protection is triggered when the threshold is reached. Enter an integer ranging from 1 to 100 for RDP brute-force attack protection and an integer ranging from 20 to 1,000 for SMB brute-force attack protection. Slow and distributed brute-force attacks are detected by using intelligent algorithms.
- **Action**: The options include **Block** and **No Action - Report Only**.

2. The following figure shows the configuration page for Linux endpoints.

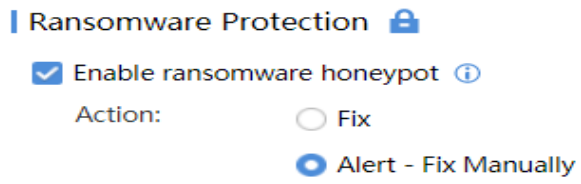


You can configure the following parameters:

- **Trigger**: You can specify a threshold for the number of login attempts per minute. Brute-force attack protection is triggered when the threshold is reached. Enter an integer ranging from 1 to 100 for SSH brute-force attack protection. Slow and distributed brute-force attacks are detected by using intelligent algorithms.
- **Action**: The options include **Block** and **No Action - Report Only**.

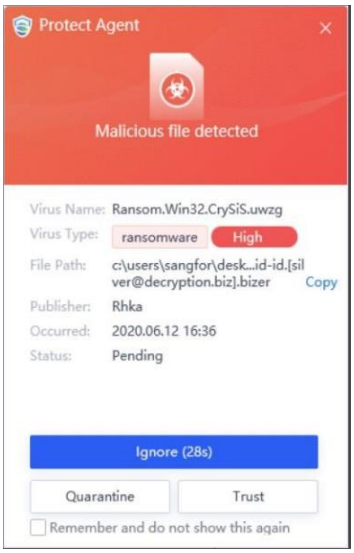
Ransomware Protection (Only for Windows Endpoints)

In ransomware protection, Sangfor Endpoint Secure places decoy files in critical system directories of endpoints and monitors the encryption of the files in real-time. When an endpoint is infected with ransomware, the Agent reports an alert and clears unknown ransomware in time to prevent business files on the endpoint from being encrypted. The following figure shows the configuration page.



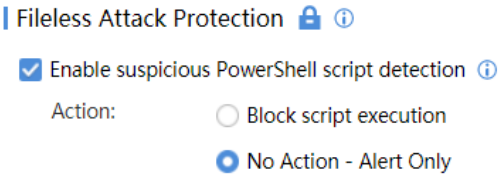
You can configure the following parameters:

- **Enable ransomware honeypot**: This function takes effect only when real-time file protection is enabled.
- **Action**: You can specify the action to perform when ransomware is detected. You are advised to select **Alert - Fix Manually**. When ransomware is detected on an endpoint, an alert is displayed in the lower right corner. The following figure shows an example.



Fileless Attack Protection (Only for Windows Endpoints)

A fileless attack is an advanced attack that exploits flawed programs to inject code into normal system processes, such as memory, registries, PowerShell scripts, and Office documents, to obtain the access permissions and execute attack commands on target devices. Fileless attack protection enables you to detect and handle suspicious PowerShell scripts. The following figure shows the configuration page.



You can configure the following parameters:

Enable suspicious PowerShell script detection: This function takes effect only when real-time file protection is enabled.

Action: The options include **Block script execution** and **No Action - Alert Only**. You are advised to select **No Action - Alert Only**.

- If suspicious PowerShell script execution is detected on a PC, Sangfor Endpoint Secure reports an alert but does not suspend the script execution. You can determine whether to allow or block the script execution.
- If suspicious PowerShell script execution is detected on a server, Sangfor Endpoint Secure reports an alert but does not suspend the script execution. You can determine whether to allow or block the script execution.

The following figure shows sample alert information.

3.3.3.4 Server Protection

Server protection is to protect the operating systems or specific directories of Windows servers. It allows trusted processes to run or perform read and write operations. You can also enable protection against RDP brute-force logins.

NOTE

Server protection is supported only for endpoints running Windows Server operating systems.

Operating System Protection

Application scenario:

Protect server operating systems against untrusted processes such as unknown ransomware to ensure server security.

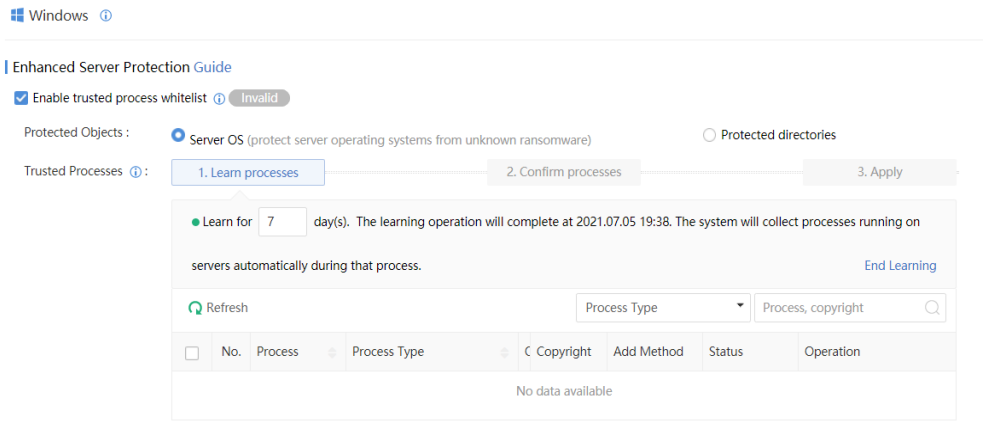
Configuration procedure:

Step 1. Scan for and remove viruses on servers.

Scan for and remove viruses on servers to ensure that the servers are secure.

Step 2. Learn processes.

Select **Enable trusted process whitelist**, select **Server OS** for **Protected Objects**, specify a period for process learning, which ranges from 1 to 30 days, and click **Save**, as shown in the following figure.

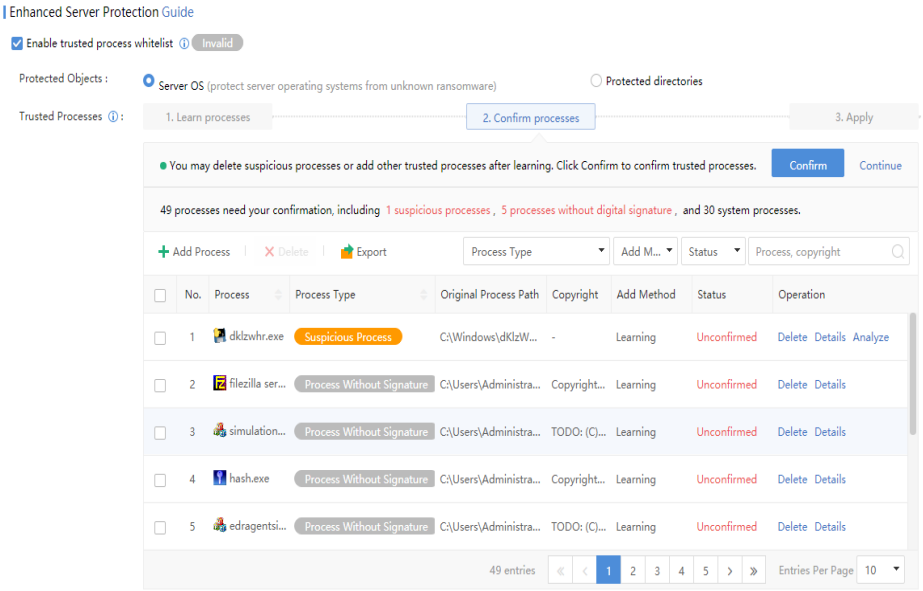


After process learning, you can view the learned processes and check the process information, for example, whether a process is suspicious or has no signature. The process information provides a reference for you to confirm

trusted processes.

Step 3. Confirm trusted processes.

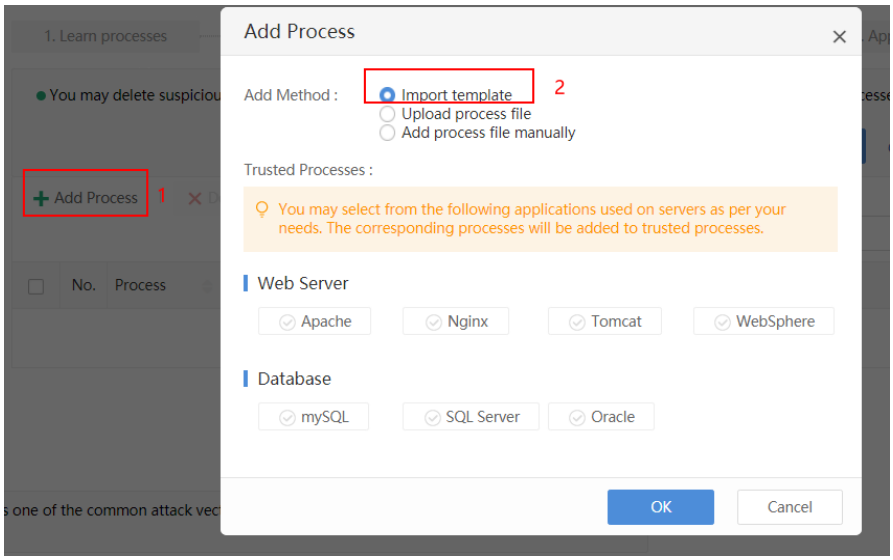
After process learning, you need to confirm trusted processes. You can delete untrusted processes based on the process learning result and add trusted processes that are not contained in the learning result. The following figure shows the configuration page.



The process parameters are described as follows:

- **Process Type**: the type of a process. The options include **Suspicious Process**, **Process Without Signature**, and **System File**.
- **Original Process Path**: the path in which the files of a process are stored.
- **Add Method**: the method that is used to add a process. The options include **Learning**, **Manual Add**, and **Template**.
- **Status**: the status of a process. **Unconfirmed** indicates that whether the process is trustful is not confirmed.
- **Operation**: the operation that you can perform on a process. You can delete processes, view process details, and analyze processes.

1. If you cannot determine whether a process is trustworthy, click **Analyze** to analyze the process based on Sangfor threat intelligence. Then, determine whether the process is trustful based on the analysis result.
2. If a trusted process is not contained in the learning result, click **Add Process** to add the process. The following figure shows the **Add Process** dialog box.



You can configure the following parameters:

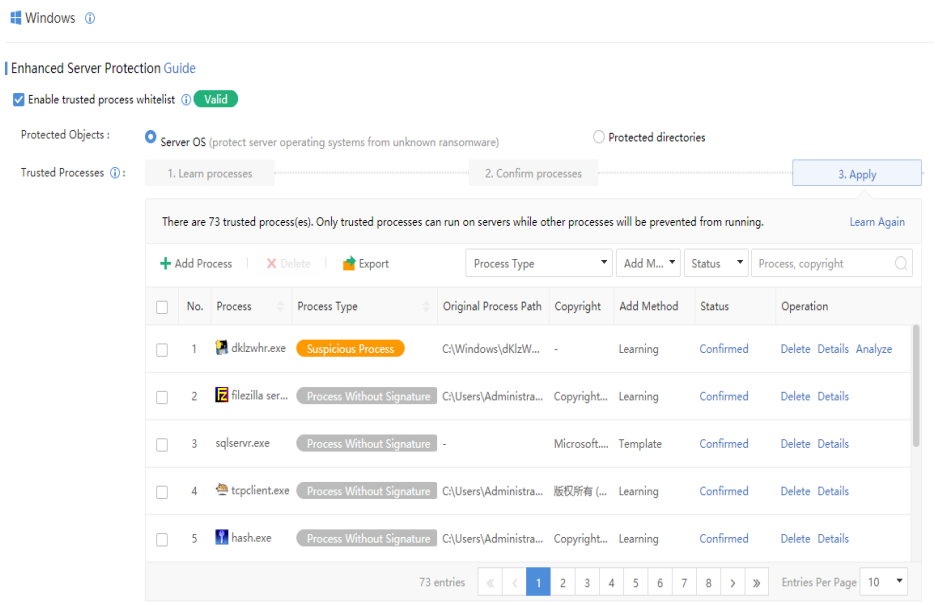
Add Method: The options include **Import template**, **Upload process file**, and **Add process file manually**.

- **Import template**: If the server that you want to protect is a web server or a database server in the template, select this option.
- **Upload process file**: If you want to upload a trusted process file, select this option and upload the file.
- **Add process file manually**: If you want to enter information about a trusted process manually, select this option and enter the process information. You need to enter the process name, original file name, and copyright information about the trusted process.

After you check trusted processes, click **Confirm**.

Step 4. Save the settings for the trusted process whitelist to take effect.

After you click **Save**, **Valid** is displayed next to **Enable trusted process whitelist**.



Specific Directory Protection

Application scenario:

Protect critical directories against ransomware.

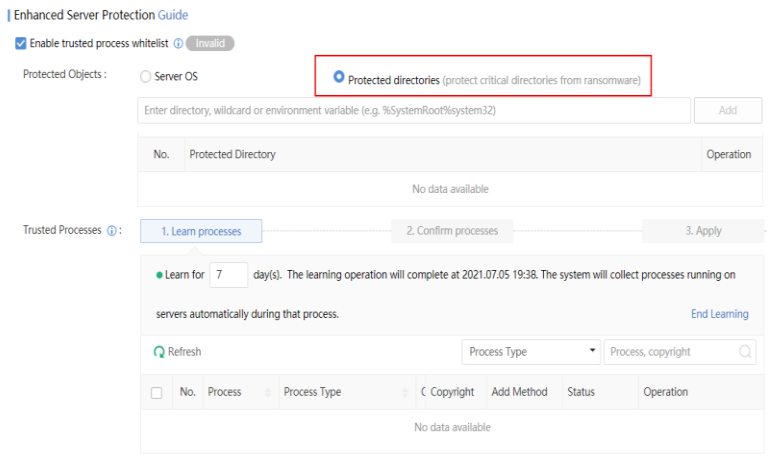
Configuration procedure:

Step 1. Scan for and remove viruses on servers.

Scan for and remove viruses on servers to ensure that the servers are secure.

Step 2. Add directories that you want to protect.

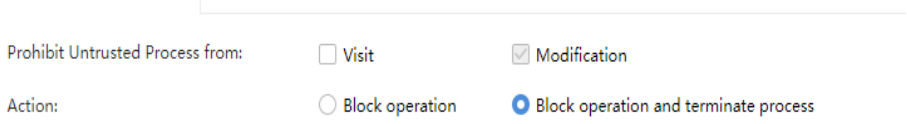
Select **Enable trusted process whitelist**, select **Protected directories** for **Projected Objects**, and add critical directories that you want to protect. You can enter wildcard characters (*) and environment variables.



Step 3. Learn and confirm trusted processes.

The operations to learn processes and confirm trusted processes are the same as those performed to implement operating system protection. For details, see Operating System Protection.

You can specify the action to perform when an untrusted process is detected.



You can configure the following parameters:

- **Prohibit Untrusted Process from**: Untrusted processes are not allowed to add, delete, or modify operations on protected directories. You can specify whether to allow untrusted processes to access protected directories.
- **Action**: You can specify the action to perform when an untrusted process operates protected directories. The options include **Block operation** or **Block operation and terminate process**.

RDP Access Protection

RDP brute-force login is a common attack vector, which enables hackers to control servers and initiate ransomware attacks. For business security, you are advised to enable protection against brute-force logins.

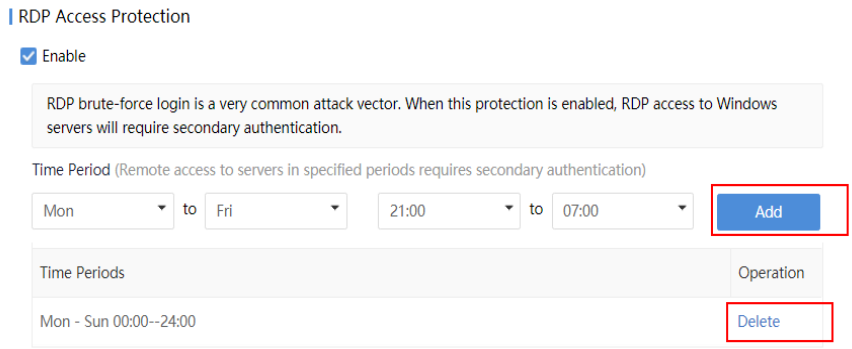
If you select **Enable**, Sangfor Endpoint Secure requires secondary authentication for remote access to servers in specified time segments.

NOTE

This function is supported only for hosts running Windows Server operating systems.

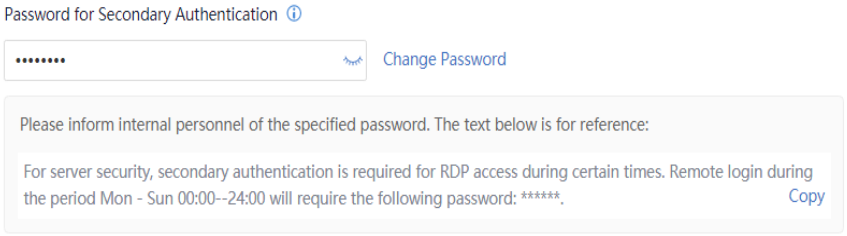
1. Specify the time segments in which secondary authentication is required for remote access.

   You can click **Add** to add a time segment and click **Delete** to delete a time segment.



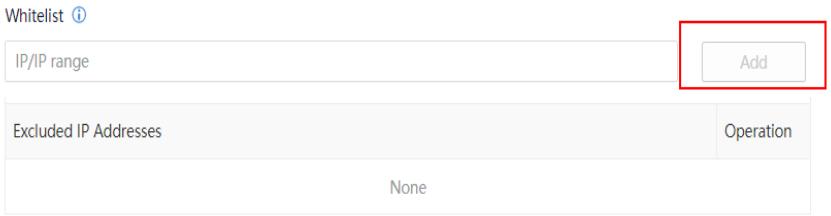
2. Change the password for secondary authentication.

   Users who use IP addresses not in the whitelist can access the protected server only after entering the correct password for secondary authentication. After you change the password for secondary authentication, provide the new password to related personnel in your enterprise as soon as possible. Otherwise, this personnel may fail to access the protected server in the specified time segments remotely.



3. Configure an IP address whitelist for remote login.

   Suppose users use IP addresses in the whitelist to remotely log in to the protected server through RDP in the specified time segments. In that case, the users do not need to enter the password for secondary authentication.

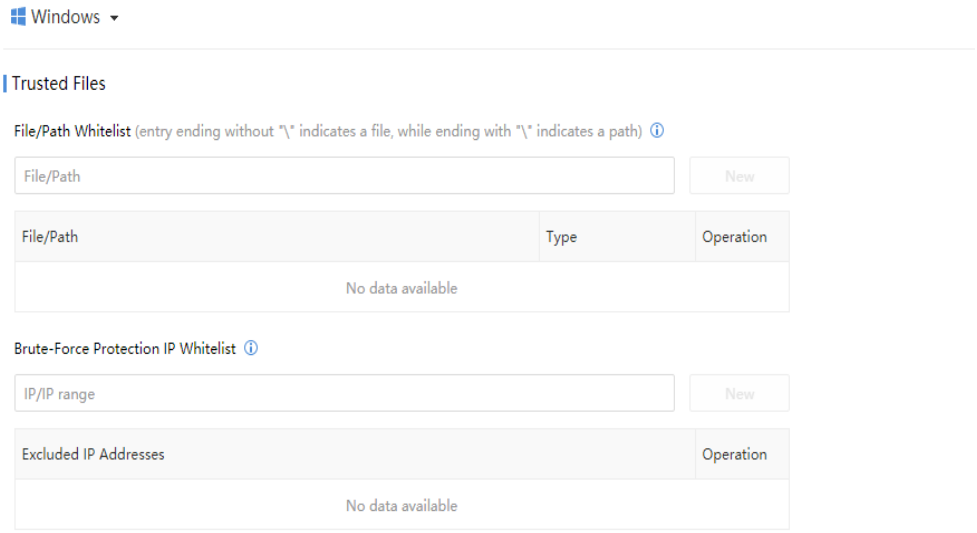


3.3.3.5 Trusted Files

The **Trusted Files** tab consists of the **Trusted Files** and **PowerShell Parameter Whitelist** areas.

Trusted Files

In the **Trusted Files** area, you can configure **File/Path Whitelist** and **Brute-Force Protection IP Whitelist**. **File/Path Whitelist** can be configured only for Windows endpoints. Virus scan and real-time monitoring are not performed on trusted files and directories. IP addresses in the brute-force protection whitelist are allowed to initiate brute-force attacks without triggering an alert. The following figure shows the configuration page.

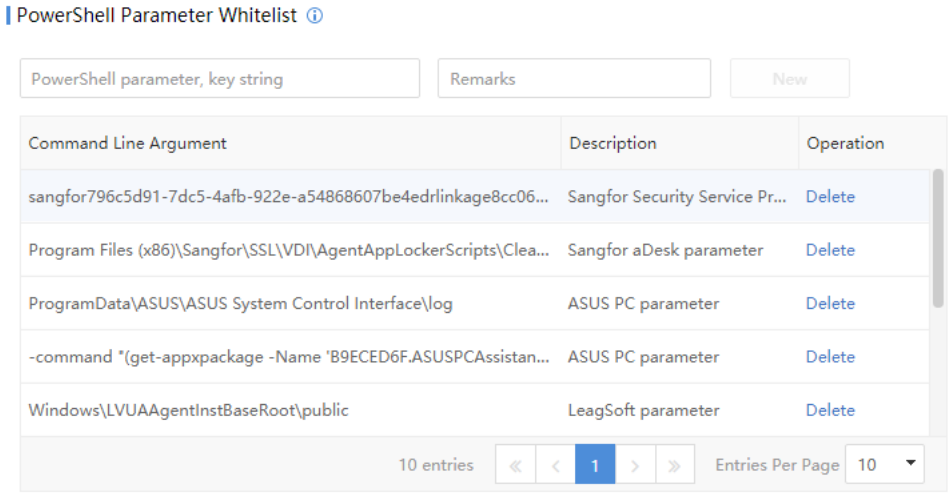


You can configure the following parameters:

- **File/Path Whitelist**: You can add files or directories to the whitelist. Entries that do not end with a backslash (\) are considered files, while entries that end with a backslash (\) are considered directories.
- **Brute-Force Protection IP Whitelist**: You can add IP addresses, IP address ranges, and subnets to the whitelist. If IP addresses in the whitelist initiate brute-force attacks, no alert is triggered.

PowerShell Parameter Whitelist

PowerShell commands that contain parameters in the whitelist are allowed to run. You can click **Delete** to delete a built-in whitelisted parameter. You can also add PowerShell command parameters to the whitelist.

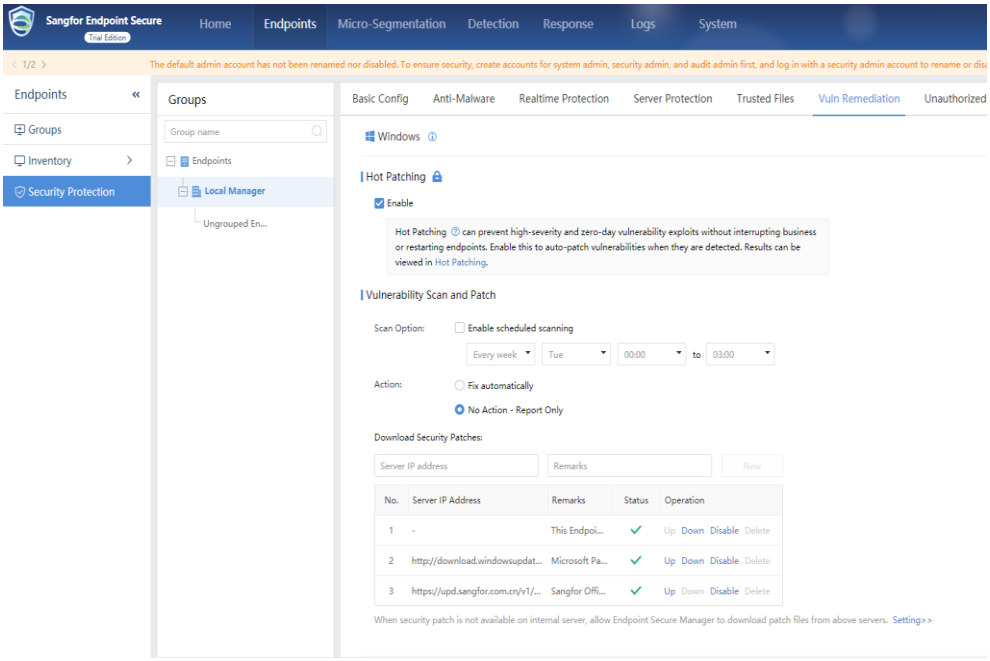


NOTE

PowerShell command parameters must be exactly matched. To prevent attackers from bypassing the protection, you are advised to enter ten or more characters for the name of each PowerShell command parameter.

3.3.3.6 Vuln Remediation

The **Vuln Remediation** tab consists of the **Hot Patching** and **Vulnerability Scan and Patch** areas.



NOTE

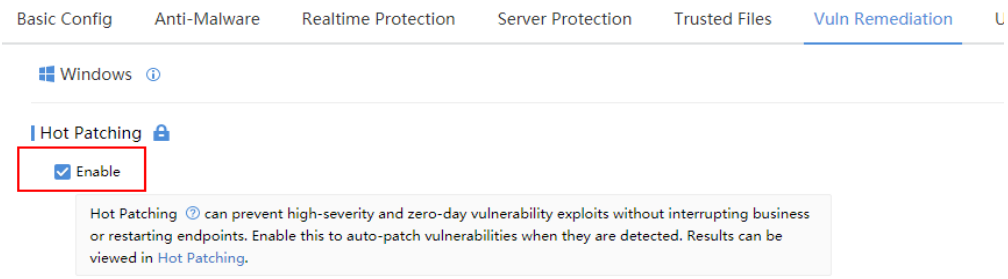
This function is supported only on Windows endpoints that can access the Internet.

Hot Patching

Hot patching is lightweight and has no impact or interference on the business system. It can prevent high-risk and zero-day vulnerability exploits without interrupting business or restarting endpoints. Hot patching does not involve compatibility issues and features a lightweight process, fast rectification, and high protection performance.

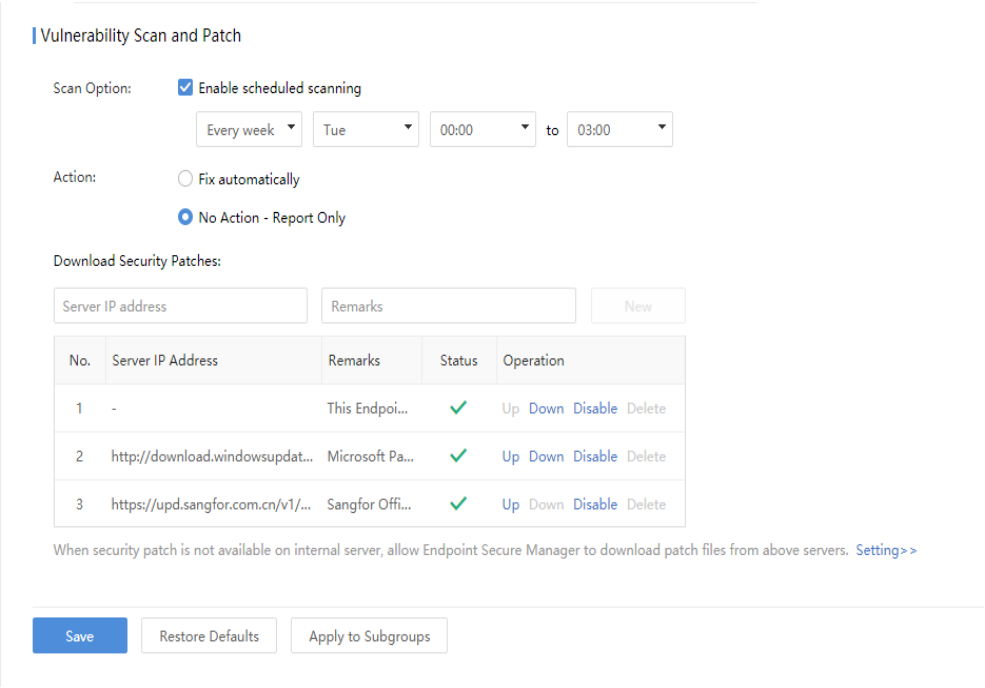
You can select or deselect **Enable** to enable or disable this function.

indicates that users are not allowed to modify hot patching settings on the Agent, and the settings on the Manager prevail. indicates that users are allowed to modify hot patching settings on the Agent, and the settings on the Agent prevail.



Vulnerability Scan and Patching

Select **Enable scheduled scanning** and specify a time when vulnerability scan and patching will be enabled.



The parameters are as follows:

- **Vulnerability Scan**: defines the period for scheduled vulnerability scan.
- **Action**: defines the action taken after system vulnerabilities are found. The options include **Fix automatically** and **No Action - Report Only** (recommended).
- **Download Security Patches**: defines the server from which endpoints download vulnerability patches. The default servers are the Sangfor CDN

server, Microsoft vulnerability patch server, and the Endpoint Secure Manager.

NOTE

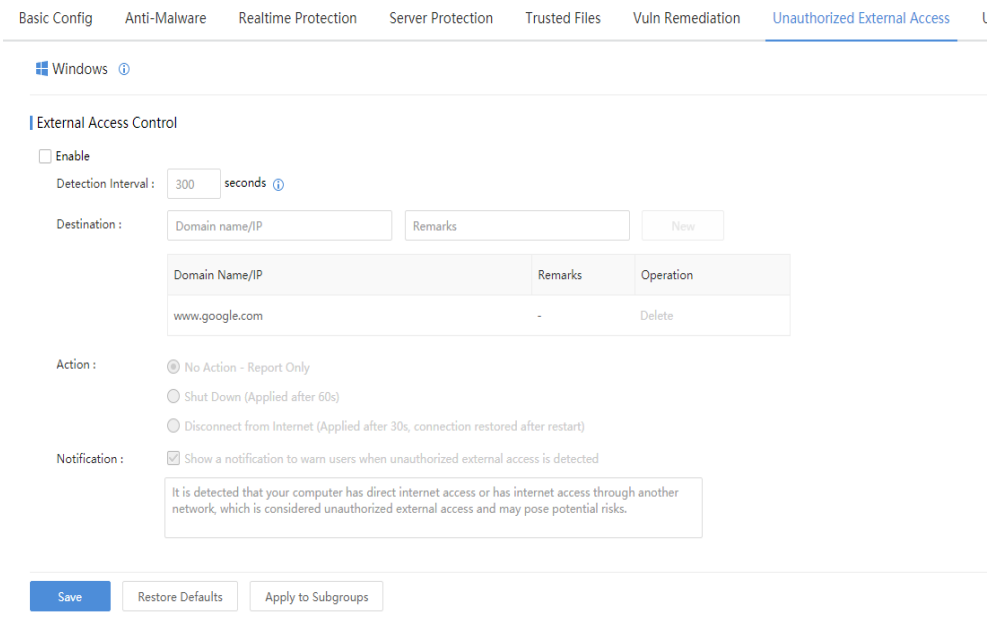
You can click **Up** or **Down** to change the server sequence. Endpoints obtain patch packages from the listed servers in sequence. Endpoint Secure Manager can proactively download the patch packages from the above servers.

3.3.3.7 Unauthorized External Access

External access control is only for Windows, not Linux endpoints. Direct access to the Internet and access to the Internet through another network from internal computers and dedicated network devices are regarded as unauthorized external access, where hackers can bypass the firewall, gateway, and other protection measures to intrude these computers and further penetrate important servers, causing major security risks to the internal network.

The **Unauthorized External Access** tab allows you to detect unauthorized external access by resolving domain names or pinging IP addresses and take actions, including network disconnection, shutdown, and email notification, to monitor unauthorized external access of endpoints in real-time.

The following figure shows the configuration page.



The parameters are as follows:

1. **Detection Interval**: intervals for detecting unauthorized external access of endpoints. The minimum value is 60s, and the maximum value is 3600s.
2. **Destination**: addresses defined as unauthorized external access. The default value is **www.google.com**. Administrators can add other IP addresses or domain names.
3. **Action**: actions taken when unauthorized external access is found. The options are as follows:

- **No Action - Report Only**: Only an alert is displayed.
- **Disconnect from Internet**: An endpoint is disconnected from the network after 30s. For endpoints running Windows Vista or later, the network disconnection effect is similar to endpoint isolation. Except for communications with the Endpoint Secure Manager, all accesses are not allowed for the endpoint. To restore the network connection, select **Restart Agent** on the **Endpoints** page. For endpoints running Windows Server 2003 and Windows XP, the network adapter is disabled and needs to be manually enabled or restarted.
- **Shut Down**: An endpoint is shut down after 60s.

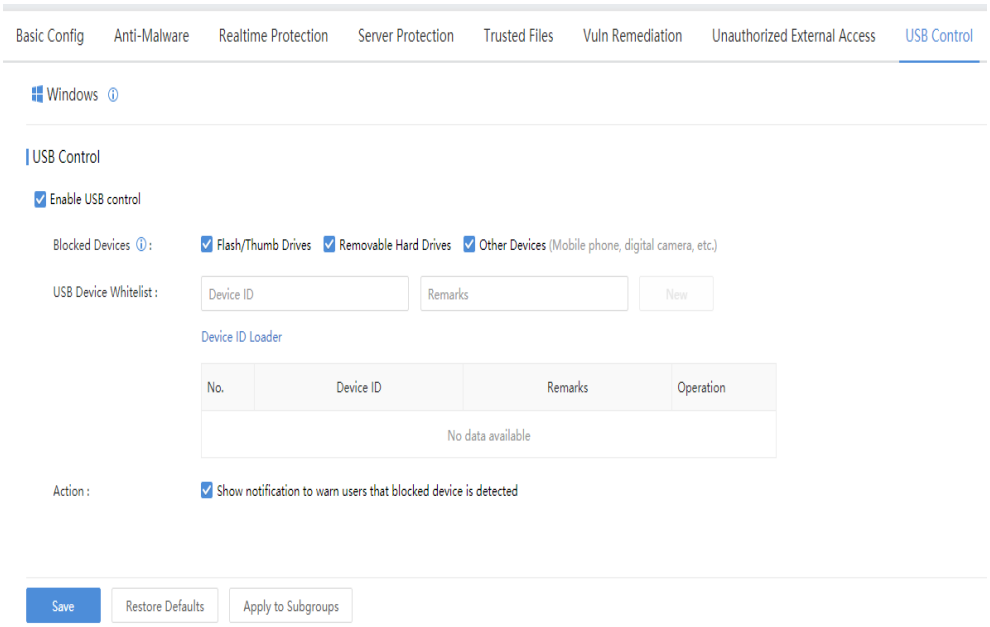
4. **Notification**: When an endpoint conducts unauthorized external access, a pop-up window will be displayed in the lower right corner of the desktop to warn users. You can set the notification content in the text box in this area.
5. **Email**: When an endpoint conducts unauthorized external access, an email notification is sent to the administrator.

3.3.3.8 USB Control

USB control is supported only for Windows, not Linux or Mac endpoints.

Unauthorized access to mobile storage media may cause security threats to endpoints, such as viruses, Trojan horses, data leakage, and data tampering. The **USB Control** tab page allows you to block or unblock mobile devices, including USB flash drives, removable hard disks, and mobile phones and set the Agent to show notifications to warn users. This helps reduce risks caused by insufficient USB device control.

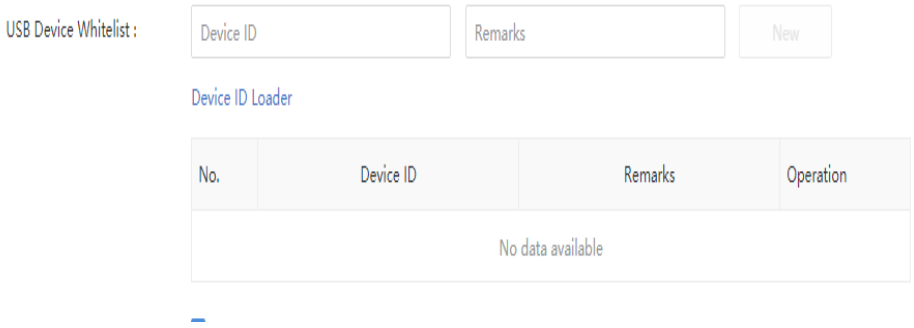
To enable the USB control function, select **Enable USB control** on the **USB Control** tab page. The following figure shows the configuration page.



1. Define blocked USB devices.

Blocked Devices: Only USB devices with the storage function will be blocked. Mouses and keyboards will not be blocked. Common USB devices include USB flash drives, removable hard disks, and portable devices (such as mobile phones and digital cameras).

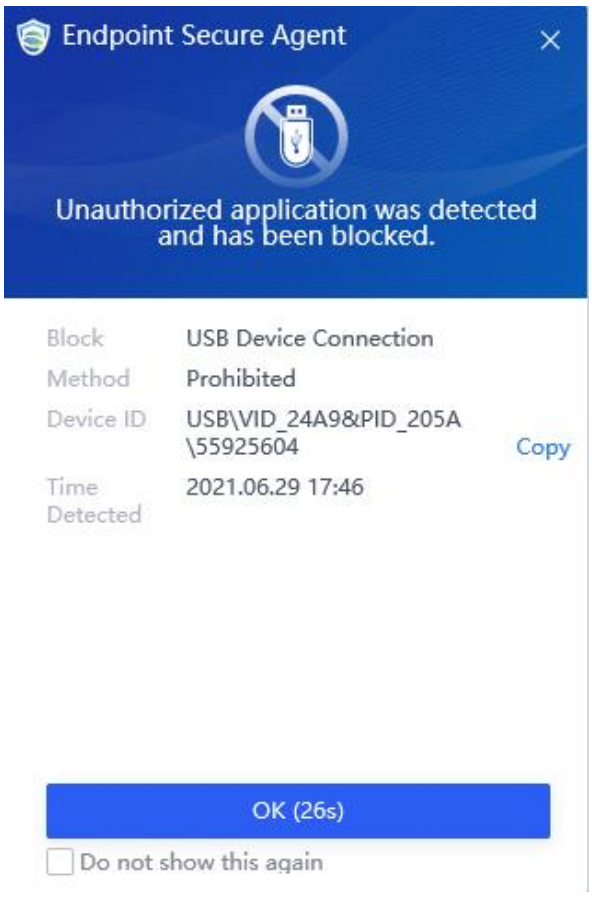
- Select to block USB devices based on actual requirements.
- When some USB devices are allowed to use, add them to the USB device whitelist and enter the device information as required, as shown in the following figure.



2. Set the Agent to show a pop-up window to warn users when blocked devices are detected.

   If **Show notification to warn users that a blocked device is detected** is

selected, a pop-up window is displayed when blocked devices are used on the server or PC, as shown in the following figure.



3.3.3.9 Security Policies Supported by Different Operating Systems

Security Policy	Windows PC	Windows Server	Linux	Mac
Basic policy	Yes	Yes	No	No
Virus scan	Yes	Yes	Yes	No
Realtime file monitoring	Yes	Yes	No	No
WebShell detection	No	Yes	Yes	No
Ransomware protection	Yes	Yes	No	No
Brute-force attack detection	Yes	Yes	Yes	No
Advanced threat protection	Yes	Yes	No	No

Server protection	No	Yes	No	No
Trusted files	Yes	Yes	No	No
Hot patching	Yes	Yes	No	No
Unauthorized external access	Yes	Yes	No	No
USB control	Yes	Yes	No	No

Table 4: Security policies supported by Windows PC, Windows Server, Linux, and Mac systems

NOTE

Mas OS currently only support trigger virus scan from Endpoint Secure Manager.

3.4 Micro-Segmentation

The **Micro-Segmentation** module allows you to enable necessary server/endpoint ports and disable unnecessary ports and visualize traffic statistics to enhance the business security of customers. Currently, Mac endpoints do not support the micro-segmentation function.

3.4.1 Business Clarification

The following table clarifies customers' business assets and the access relationship between business assets to prepare for micro-segmentation policies.

Object	Business assets	**Business Asset Name**	**Endpoint Group**	**Contained Endpoints**	-
		All	User zone 1, user zone 2, user zone 3, server zone 1, and server zone	PC1\PC2 Sever1 and Server2	-

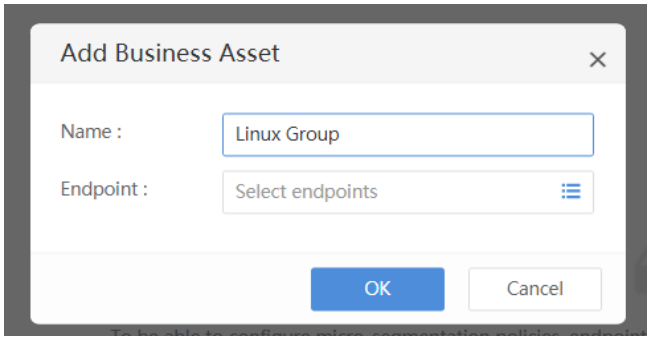
			2		
	IP groups	**IP Group Name**	**IP Address Range**	**IP Group Type**	-
		Office endpoints	172.16.200.1-172.16.200.254	Internal network	-
	Services (Clarify custom policies only.)	**Service Name**	**Protocol**	**Port**	**Traffic Type**
		SMB	TCP	135\136\137\139\445	Business traffic
		RTP	TCP	3389	Maintenance traffic
Access Relationship Between Objects	Access relationship	**Source**	**Destination**	**Service**	**Action**
		IP group: Internet by default	Business asset: All	SMB and RTP	Deny

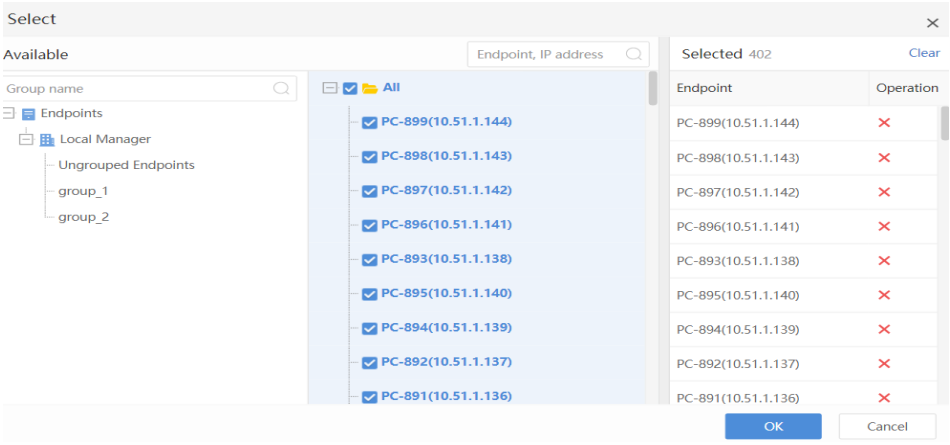
3.4.2 Creating Business Assets, Tags, IP Groups, and Services

Creating a Business Asset

You can add multiple server endpoints to a business asset to better invocate micro-segmentation policies and display traffic statistics. The configuration process is as follows:

1. Choose **Micro-Segmentation** > **Business Asset** and click **New**. In the displayed **Add Business Asset** dialog box, enter the business asset name and select server endpoints. The following figure shows the configuration page.



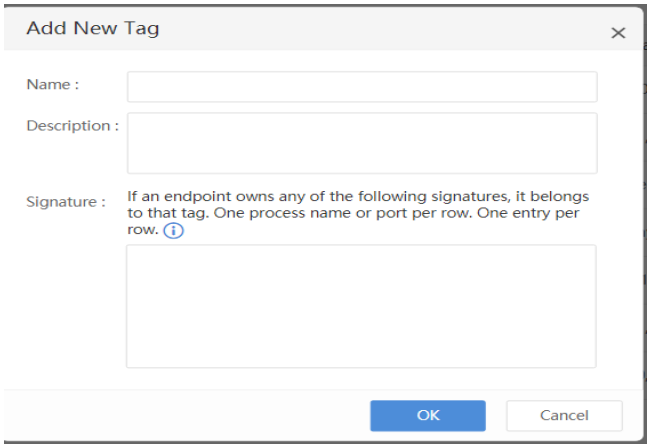


2. After a business asset is created, you can view the created business asset and corresponding server endpoints, specify tags, and view the status on the **Business Asset** page.

Creating a Tag

Tags are used to define the roles of server endpoints in a business asset and can be regarded as the types of services provided by the server endpoints. The Endpoint Secure Manager has embedded the web, database, FTP, SLB, email, message queue, WebSphere, WebLogic tags, and the corresponding tag signature. To add a tag, perform the following steps:

1. Choose **Micro-Segmentation** > **Tags** and click **New**. On the **Add Tag** page, edit the tag name, description, and signature, as shown in the following figure.



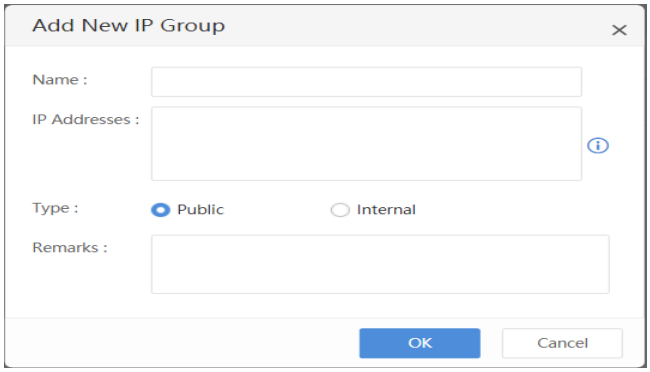
The signature can be a process name or port. Specify one signature in each line.

2. After editing the information, click **OK** to complete the creation. You can specify tags for server endpoints on the **Business Assets** page to better invocate micro-segmentation policies and display traffic statistics.

Creating an IP Group

The **IP Groups** page allows you to classify internal and public IP addresses to corresponding IP groups. The Endpoint Secure Manager has embedded the default internal IP groups- 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 and the default public IP groups 0.0.0.0 to 255.255.255.255. IP addresses are matched to IP groups from up to down to facilitate invocation of micro-segmentation policies are matched from up to down to facilitate invocation. To create an IP group, perform the following steps:

1. Choose **Micro-Segmentation** > **IP Groups** and click **New**. On the **Add IP Group** page, specify IP group information, as shown in the following figure.



Address supports single IP addresses, IP address ranges, and subnets.

2. Click **OK**. The IP group is created. On the **IP Groups** page, you can move

created IP groups up or down to match the policies.

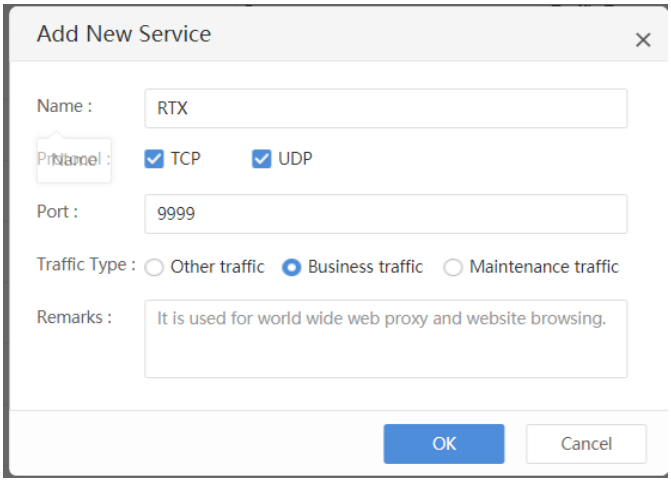
Creating a Service

On the **Services** page, you can define service ports for invoking micro-segmentation policies. The Endpoint Secure Manager is embedded with 35 services for customization. The configuration process is as follows:

NOTE

Custom service ports cannot be the same as existing ports.

1. Choose **Micro-Segmentation** > **Services** and click **New**. On the **Add Service** page, specify service information, as shown in the following figure.



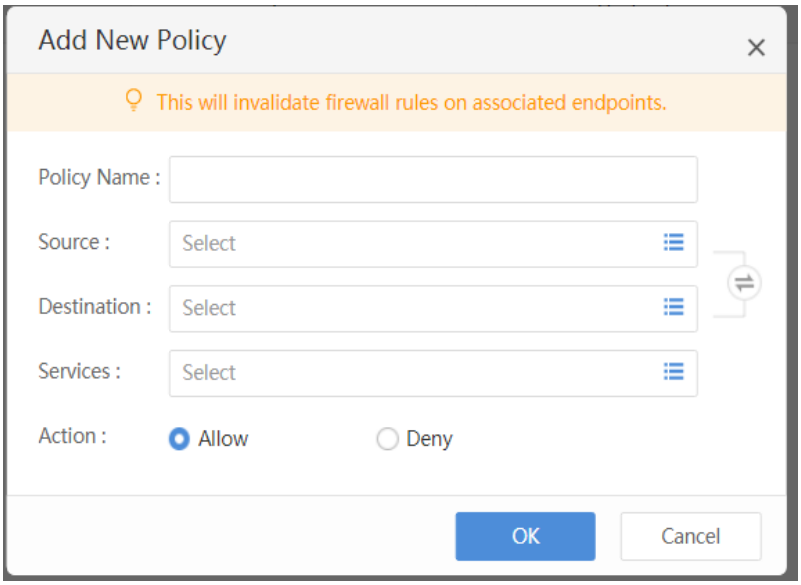
Traffic types include **Business traffic**, **Maintenance traffic**, and **Others**. Select a traffic type to display the corresponding traffic statistics.

2. After configuration is complete, click **OK**.

3.4.3 Policies

Micro-segmentation policies use 5-Tuple data to allow or reject access. You can click the policy switch in the upper right corner to globally enable or disable the function. The detailed configuration process is as follows:

1. Choose **Micro-Segmentation** > **Policies** and click **New**. On the **Add Policy** page, specify policy information, as shown in the following figure.



The parameters are as follows:

- **Source**: the source object that accesses the target endpoint. You can select a business asset, tag, server, or IP group.
- **Destination**: the accessed target endpoint.
- **Services**: service port of the target endpoint.
- **Action**: The options include **Allow** and **Deny**.

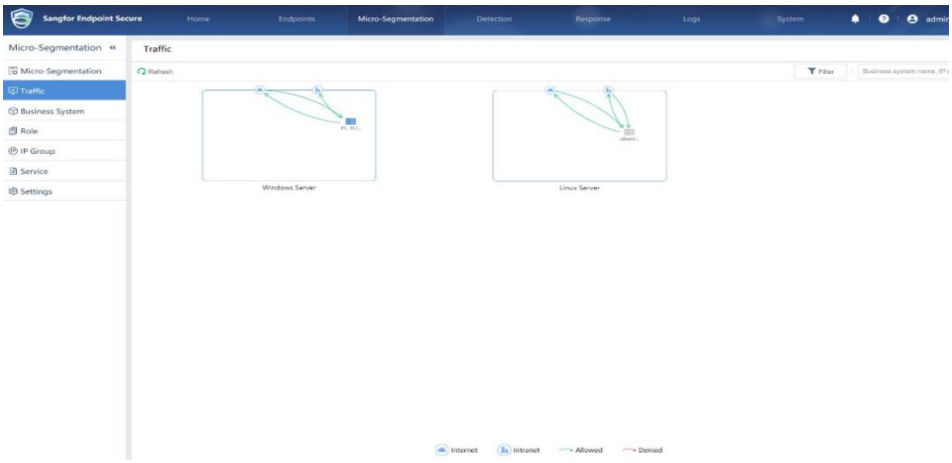
NOTE

You can click ⇌ to exchange the source and destination.

2. After the configuration is complete, click **OK**. On the **Policies** page, you can view details about existing policies and move up or down and enable or disable policies.

3.4.4 Traffic Statistics

On the **Traffic Statistics** page, you can view traffic statistics of endpoint systems, including public, internal, allowed, and denied traffic. You can also filter policies to view traffic statistics. The following figure shows the configuration page.

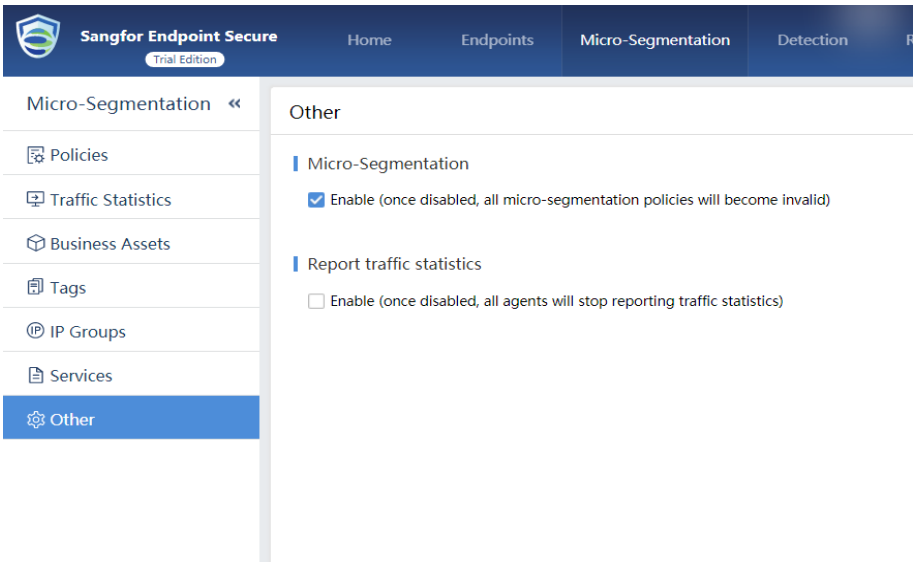


The options of **Filter** are as follows:

- **Denied traffic (Red)**: indicates denied traffic.
- **Allowed traffic (Green)**: indicates allowed traffic.
- **Inter-business asset traffic**: indicates traffic between business assets.
- **Intra-business asset traffic:** indicates traffic within a business asset.

3.4.5 Other

You can enable micro-segmentation, report traffic statistics, and back up and restore micro-segmentation policies on the **Other** page. The following figure shows the configuration page.



The parameters are as follows:

- **Micro-Segmentation**: If you select **Enable**, the micro-segmentation function is enabled. If this function is disabled, micro-segmentation policies of all business assets become invalid.
- **Report traffic statistics**: If you select **Enable**, traffic statistics are displayed on the **Traffic Statistics** page. If this function is disabled, all Agents will stop reporting traffic statistics, and no traffic statistics will be displayed on the **Traffic Statistics** page.

3.5 Detection

3.5.1 Virus Scan

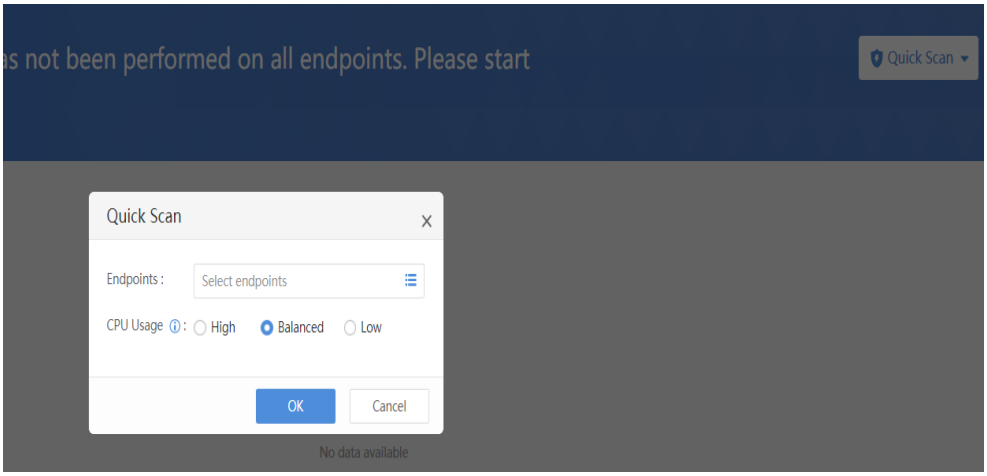
The **Virus Scan** module allows you to deliver security check tasks to endpoints connected to the Endpoint Secure Manager. It scans malicious files of endpoints using the local file reputation database, Sangfor Engine Zero, Behavioral Analysis Engine, Gene Analysis Engine, Cloud-Based Engine, and shows the scan result.

Virus scan modes include quick scan and full scan. You can click the triangle pointer next to **Quick Scan** to select a scan mode from the drop-down list. The following table describes the differences between a quick scan and a full scan.

Full Scan	Scan all disk files of an endpoint.
Quick Scan	Scan critical directories in the system disk. Critical directories include: Windows: /Windows and Windows/system32 /Windows/system32/drivers and its subdirectories Linux: /bin, /sbin, /usr/sbin, /usr/bin, /lib, /lib64 /usr/lib/usr/lib64, /usr/local/lib, /usr/local/lib64, /tmp, /var/tmp, /dev, /proc

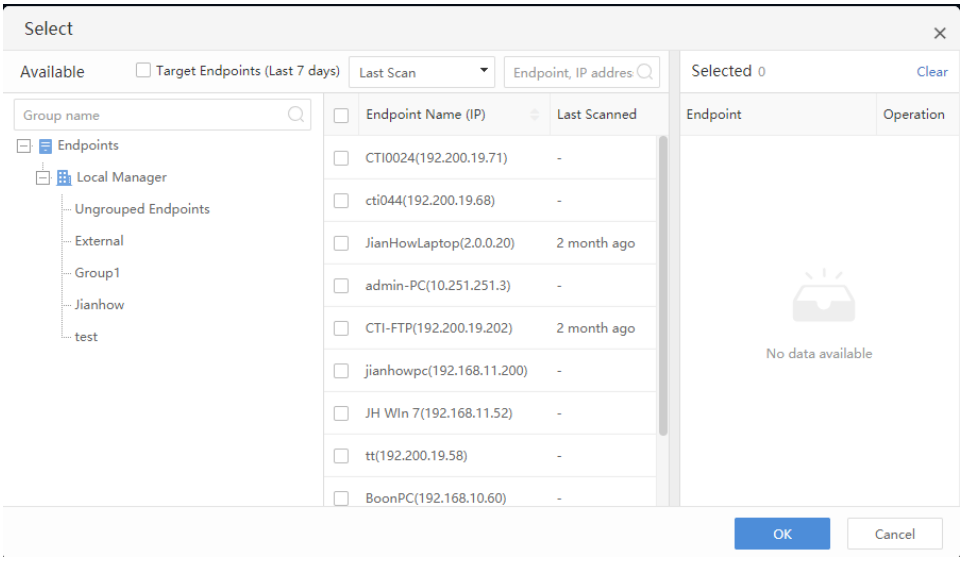
Table 5: Path that ES agent scan through in Full scan and Quick scan

1. Click **Quick Scan** or **Full Scan** to enter the corresponding configuration page, as shown in the following figure.



The parameters are as follows:

Endpoints: On the **Select** page, you can view target endpoints in the last 7 days, endpoints not scanned in the previous week, previous month, or last three months, and the last scanning time to filter endpoints that need to be scanned. You can also enter an endpoint name or IP address in the search box to search for the specific endpoint.

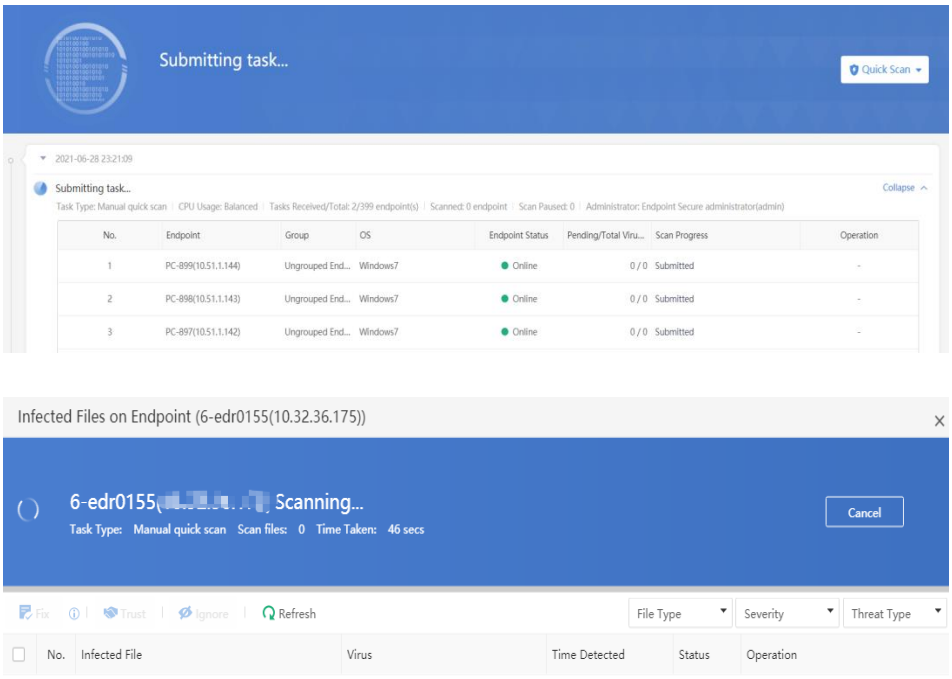


CPU Usage: The options include **High**, **Balanced**, and **Low**. Their differences are as follows:

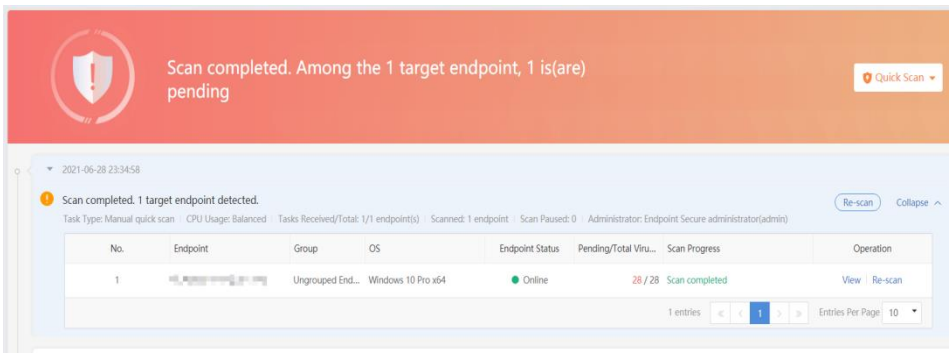
- **High**: Scan is performed at full speed, and the CPU usage of the scanning is not limited. (In resource optimization mode, the CPU usage does not exceed 50%.)

- **Balanced**: A balance is reached between the scan speed and CPU usage, and the CPU usage cannot exceed 30%. (In resource optimization mode, the CPU usage does not exceed 20%.)
- **Low**: Fewer CPU resources are occupied during scanning, and the CPU usage cannot exceed 10%. (In resource optimization mode, the CPU usage does not exceed 5%.)

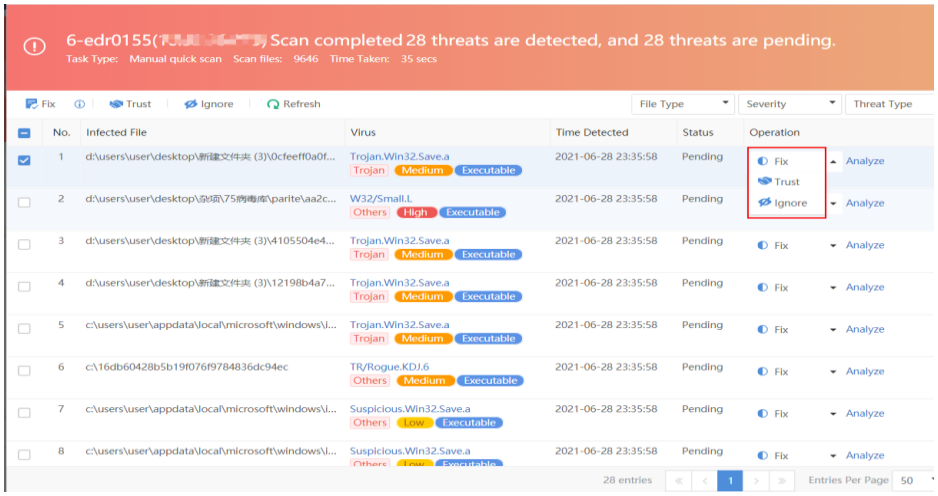
2. After the configuration is complete, the virus scan task is performed. You can click **Detection Details** in the **Operation** column of an endpoint to view the virus scan information, as shown in the following figure.



3. After the virus scan is complete, you can view the scan result. The displayed information includes the task type, scan mode, task received/total endpoints, scanned endpoints, scan paused endpoints, endpoint name, IP address, group, operating system, status, pending viruses, total viruses, and scan status, as shown in the following figure.



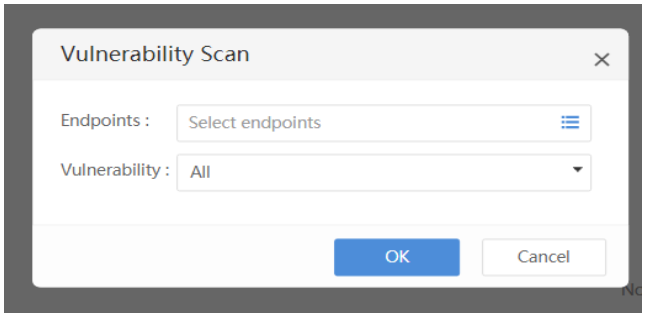
4. You can click **Detection Details** in the **Operation** column of a target endpoint to view the scan result and click the drop-down list icon next to **Fix** and select **Fix**, **Trust**, or **Ignore** for a virus, as shown in the following figure.



3.5.2 Vulnerability Scan

The **Vulnerability Scan** module detects and fixes Windows endpoints' system vulnerabilities, including remote code execution (RCE), denial of service (DoS), privilege escalation, security mode bypass, and information leakage. The vulnerability scan process is as follows:

1. Choose **Detection** > **Vulnerability Scan** and click **New Scan Task** to create a vulnerability scan task. The following figure shows the configuration page.

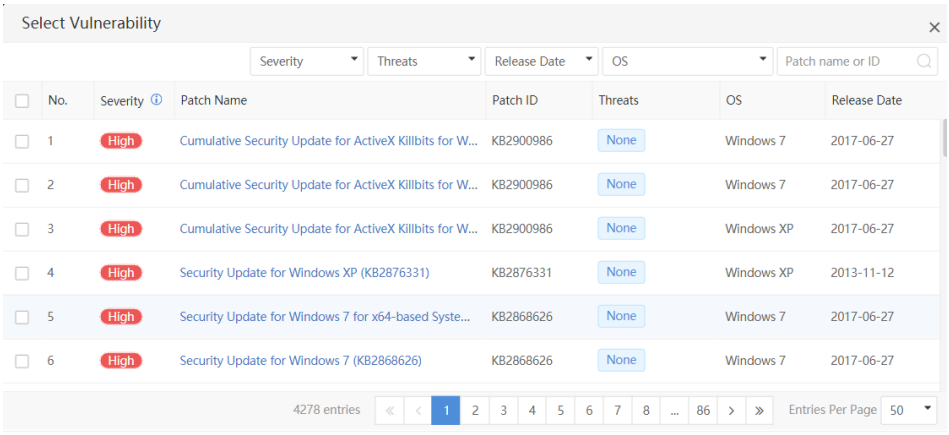


The parameters are as follows:

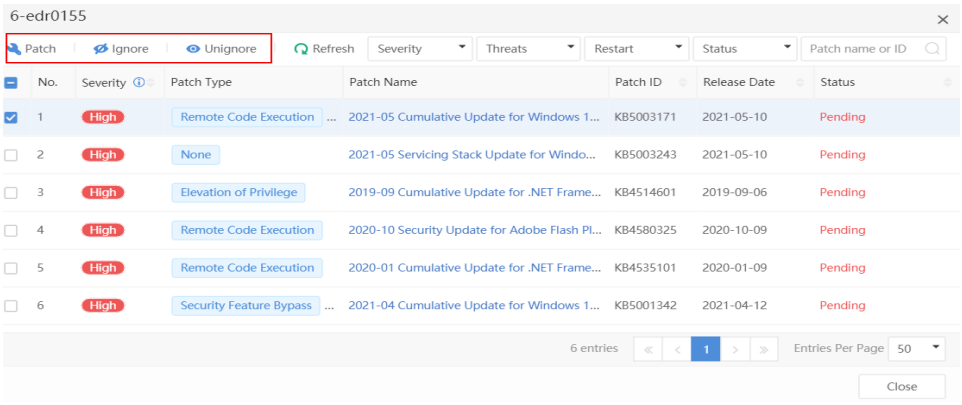
Endpoints: On the **Select** page, you can view endpoints not scanned in the last week, last month, or last three months, and the last scanning time to filter endpoints that need to be scanned. You can also enter an endpoint name or IP address in the search box to search for the specific endpoint.

Vulnerability: The options include **All**, **High**, and **Specified**.

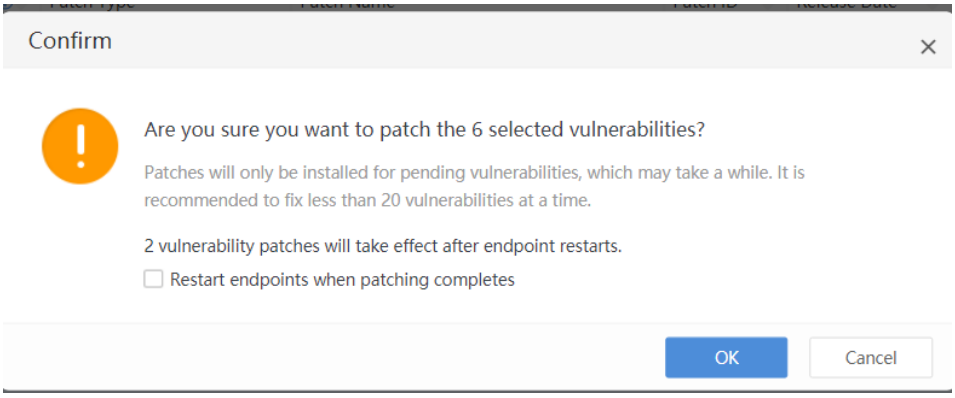
- **All**: Scan and fix the RCE, DoS, privilege escalation, security feature bypass, and information leakage vulnerabilities.
- **High**: Scan and fix only high-severity vulnerabilities. Select **High** from the vulnerability severity drop-down list box on the **Select Vulnerability** page for details about high-severity vulnerabilities.
- **Specified**: Customize vulnerabilities that need to be scanned. On the **Select Vulnerability** page, you can filter vulnerabilities by vulnerability severity, threat, patch release date, and OS, search for vulnerabilities by patch name or ID, and select vulnerabilities that need to be scanned in the filtering result, as shown in the following figure.



2. Click **OK**. The vulnerability scan task is automatically performed. In the left pane of the **Vulnerability Scan** page, you can filter tasks by task type and task status and click a specific task to view details. For endpoints with pending vulnerabilities, you can click **Fix** to select vulnerabilities to fix and deliver patching tasks, as shown in the following figure.



Click **Fix**. If a restart is required for the patch to take effect, a prompt shown in the following figure will be displayed when patching starts. Select **Restart endpoints after patching completes** only if it is allowed by the administrator to prevent the risk of data loss. It is not recommended to select this option. After patch installation, restart the endpoint in off-work time.



NOTE

Vulnerability patching mentioned in this section requires endpoint PCs to be able to access the Internet. If an endpoint PC cannot access the Internet, patch vulnerabilities by referring to section 3.6.2 Remediation.

3.5.3 Security & Integrity Check

The **Security & Integrity Check** module is for compliance checks of endpoints. The check content varies depending on the endpoint operating system.

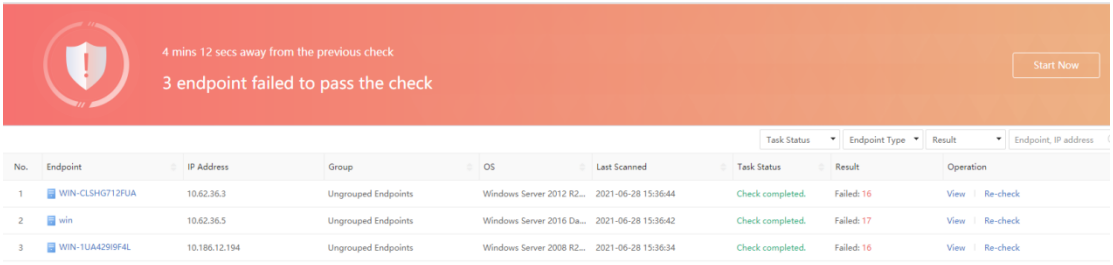
Windows endpoints: identity identification, access control, security audit, history

information protection, intrusion prevention, and malicious code prevention

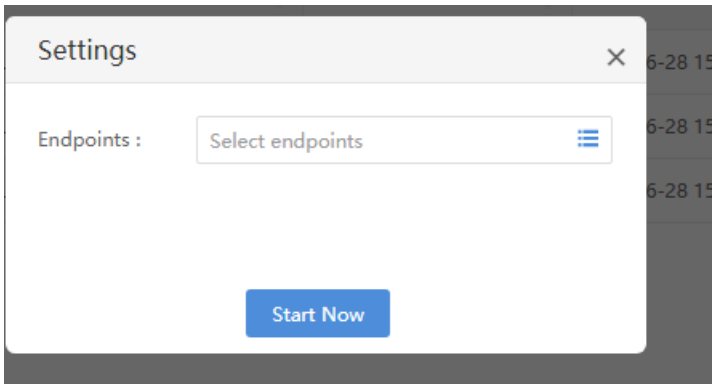
Linux endpoints: identity identification, access control, security audit, SSH policy detection, intrusion prevention, and malicious code prevention

Mac endpoints: For Mac endpoints, security and integrity check is not supported.

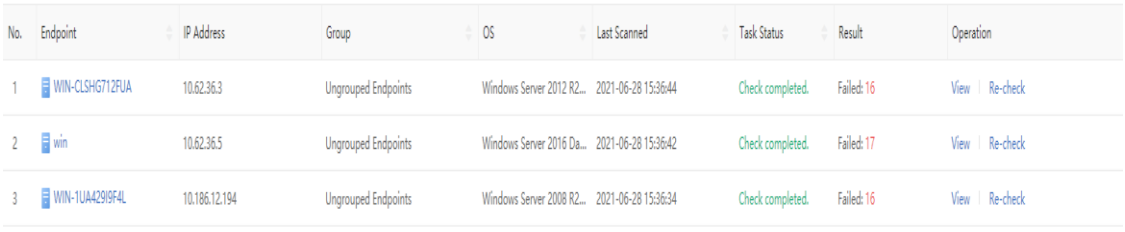
The following figure shows the configuration page.



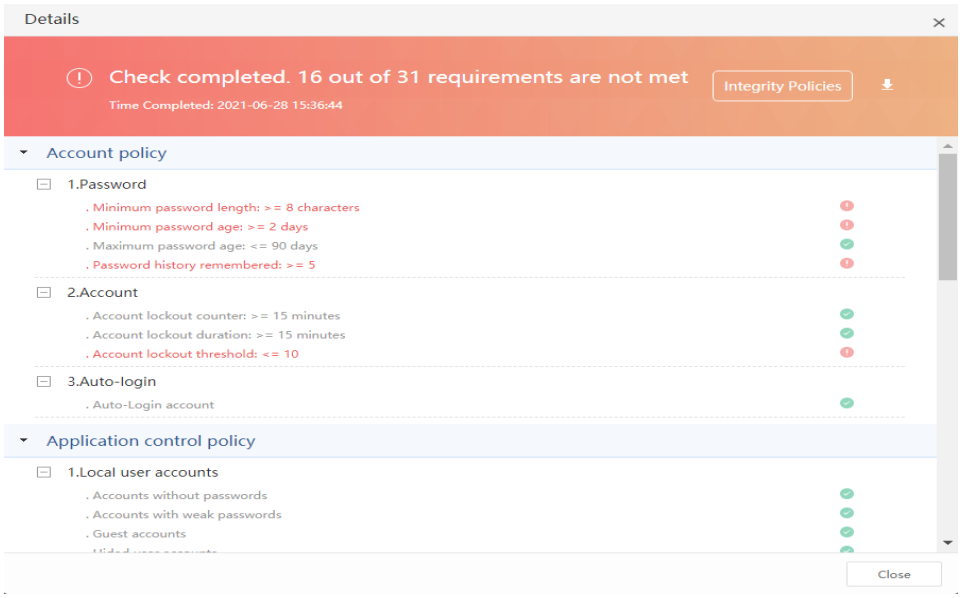
Click **Start Now** and select endpoints for which compliance check is required, as shown in the following figure.



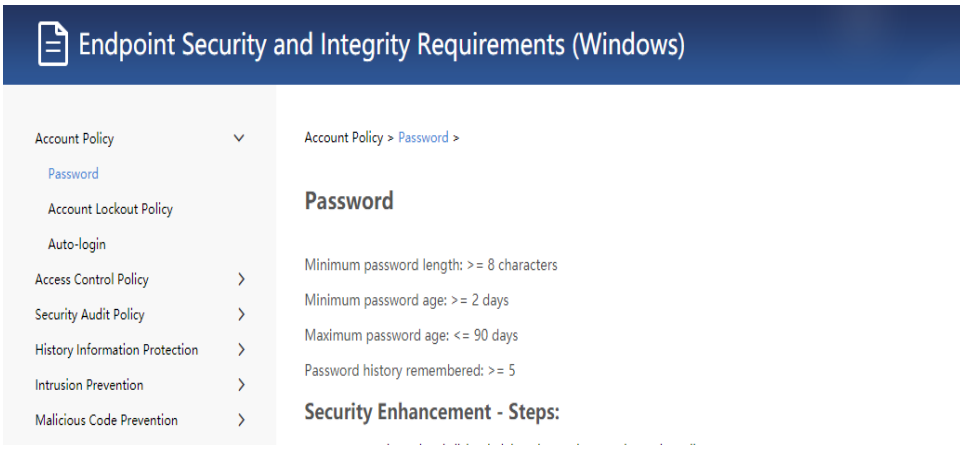
After detection is complete, you can view the detection result.



To view the compliance detection result, click **View Details**.



Integrity Policies: Click it to view the configuration requirements for a compliance check.



Modify configuration based on the endpoint compliance security setting document and click **Re-check** to perform compliance check again.

You can click  to download the compliance check report.

WARNING

Pay attention to compliance check items in orange.

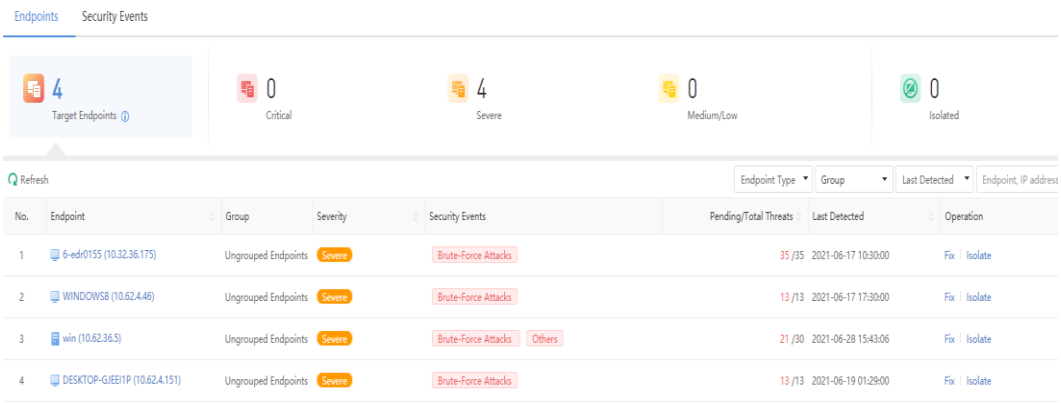
3.6 Response

3.6.1 Threat Response

The **Threat Response** module analyzes and displays all target endpoints and critical, severe, medium/low, and isolated endpoints in terms of endpoints and security events. You can filter endpoints by **Endpoint Type**, **Group**, and **Last Detected** and enter an endpoint name or IP address in the search box to search for a specific endpoint. This function is supported on Windows, Windows Server, Linux, and Mac endpoints.

3.6.2 Endpoints

On the **Endpoints** tab, you can select a target endpoint type to view the corresponding endpoint name, group, severity, security events, pending/total threats, and last detection time. You can also filter endpoints by **Endpoint Type**, **Group**, and **Last Detected** and perform the **Fix** or **Isolate** operation for target endpoints. The following figure shows the **Endpoints** tab.



1. **Severity**: The options include **Critical**, **Severe**, and **Medium/Low**.
   - **Critical:** indicates endpoints involved in high-severity viruses, WebShell backdoors, and botnets.
   - **Severe:** indicates endpoints involved in medium-severity viruses, WebShell backdoors, and brute-force attacks.
   - **Medium/Low:** indicates endpoints involved in low-severity viruses and botnets
2. **Last Detected**: latest threat detection time.

3. **Operation**: The operations include **Fix** and **Isolate**.

   - **Isolate:** After an endpoint is isolated, it cannot access any network. Ensure that business assets are not affected. You can click **Restore** to restore isolated endpoints.
   - **Fix:** Click **Fix**. On the displayed page, select infected files/processes and click **Fix**, **Trust**, or **Ignore**. You can filter infected files/processes by **Severity**, **Threat Type**, and **Last Detected**.

     i. **Fix**

     - Delete malicious files for malicious programs, such as Trojan horses.
     - Remove infectious viruses.
     - Block fileless PowerShell attacks.
     - After handling, you can view the records in the fixed area of the security events.

     ii. **Trust**

     - Add files to the whitelist.
     - Allow fileless PowerShell attacks.

     iii. **Ignore**

     - Ignore detected files/processes or attack source IP addresses.

NOTE

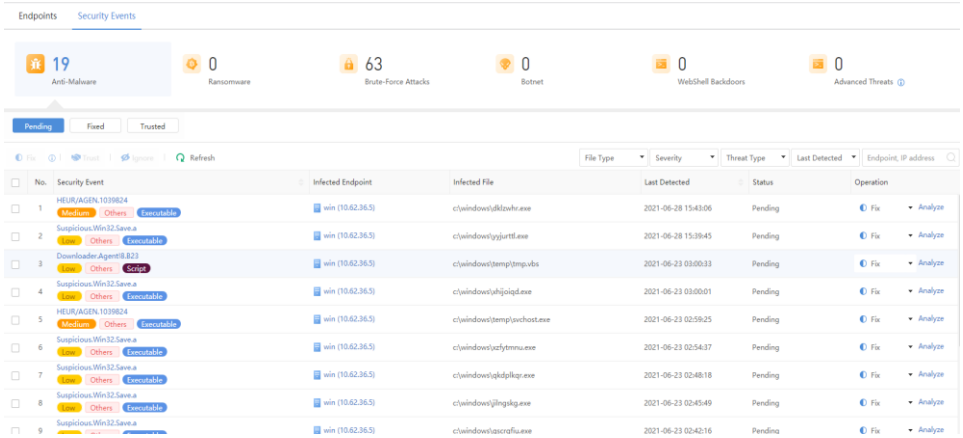
To ensure security, **Fix** is not available for brute-force attacks, and brute-force attacks need to be added to the blacklist manually.

3.6.3 Security Events

On the **Security Events** tab, you can select a security event type (including **Anti-Malware**, **Ransomware**, **Brute-Force Attacks**, **Botnet**, **WebShell Backdoors**, and **Advanced Threats**) to view the corresponding security event names, infected endpoints, infected files, detection time, and handling status.

You can filter security events by handling status and severity. You can also select multiple security events for batch operations.

The following figure shows the **Security Events** tab.



For each security event, you can select **Fix**, **Trust**, or **Ignore** in the **Operation** column. If you are unsure how to operate a security event, click **Threat Analysis** or click the security event to view the details, such as the virus name, infected file, virus type, detection engine, and handling suggestions.

NOTE

For the **Fix** and **Trust** operations, you can select **Also fix file with the same MD5 on other endpoints** to batch process the same files on other endpoints.

3.6.4 Remediation

The **Remediation** module consists of the **Patching** and **Hot Patching** nodes. The **Patching** page displays vulnerability patching by endpoint and vulnerability. The **Hot Patching** page shows all endpoints that have been patched against vulnerabilities.

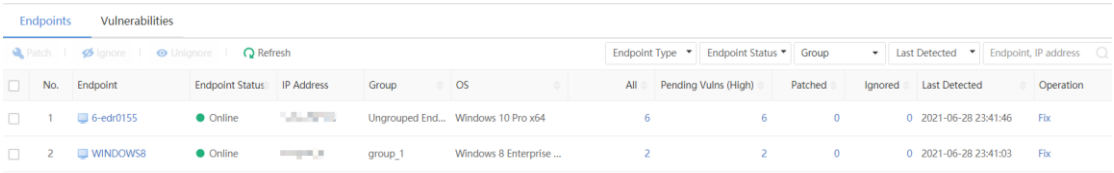
NOTE

Vulnerability patching can be performed only after vulnerability detection is complete.

3.6.4.1 Patching

Endpoints

On the **Endpoints** tab page, the Endpoint Secure Manager performs vulnerability remediation by the endpoint. You can view the total number of vulnerabilities, the number of pending high-severity vulnerabilities, and the number of patched or ignored vulnerabilities of each endpoint. You can select one or more endpoints and click **Fix** to fix vulnerabilities for these endpoints. The following figure shows the **Endpoints** tab page.

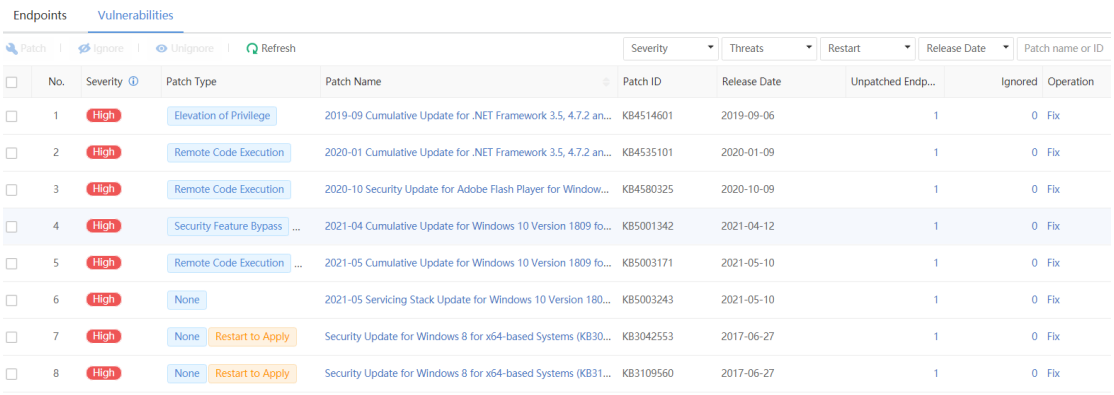


On the **Fix** page, you can:

1. View the vulnerability severity, threats, and patch status of a specific endpoint and filter vulnerabilities by severity, threat, whether restarted and patch status.
2. Select multiple vulnerabilities and click **Patch** or **Ignore** to patch or ignore these vulnerabilities.

Vulnerabilities

On the **Vulnerabilities** tab page, the Endpoint Secure Manager performs vulnerability remediation by the vulnerability. You can view pending vulnerabilities and patch information and fix one or more vulnerabilities at a time. The following figure shows the **Vulnerabilities** tab page.



On the **Fix** page, you can:

1. View information about endpoints prone to a vulnerability, including the endpoint name, status, IP address, group, and operating system. Filter endpoints by endpoint status, group, and patch status, or enter an endpoint name or IP address in the search box to search for the specific endpoint.
2. Select multiple endpoints and click **Patch** or **Ignore** to patch or ignore vulnerabilities for these endpoints.

3.6.4.2 Hot Patching

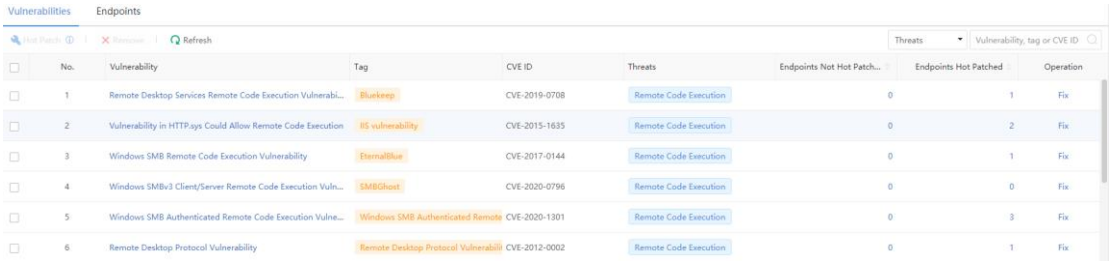
The hot patching function fixes vulnerability code in the memory to prevent vulnerabilities from being exploited. The **Hot Patching** page allows you to enable hot patching against high-severity vulnerabilities without affecting business.

The **Hot Patching** page displays endpoints that have been patched against all vulnerabilities on its **Endpoints** and **Vulnerabilities** tab pages by endpoint and vulnerability.

Vulnerabilities

1. Viewing and managing vulnerabilities

You can view information on the **Vulnerabilities** tab page, such as the vulnerability name, ID, threats, hot patched endpoints, and endpoints pending hot patching.



You can filter vulnerabilities by **Threats** or enter a vulnerability name, tag, or ID in the search box to search for the specific vulnerability. It facilitates accurate locating and O&M management of vulnerabilities.

2. Enabling or disabling hot patching

You can click **Fix** in the **Operation** column of a vulnerability and then enable or disable hot patching for this vulnerability on the displayed page. You can also select multiple vulnerabilities and click **Hot Patch** or **Remove** to enable or disable hot patching for these vulnerabilities at a time.

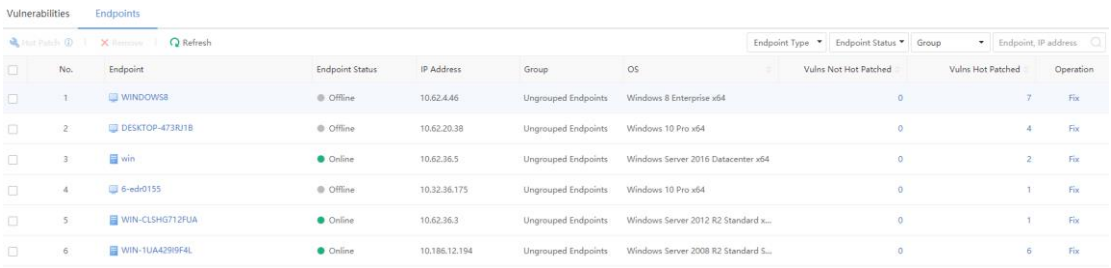
NOTE

Hot patching prevents vulnerabilities from being exploited without disrupting operations or restarting endpoints. When hot patching for high-risk vulnerability is disabled, the protection becomes ineffective. To permanently prevent the vulnerability from being exploited, install a patch.

Endpoints

1. Viewing and managing endpoints

On the **Endpoints** tab page, you can view information, such as the endpoint name, status, IP address, group, operating system, and high-severity vulnerabilities hot patched and not hot patched.



You can filter endpoints by endpoint type, status, and group or enter an endpoint name or IP address in the search box to search for the specific endpoint. It facilitates accurate locating and O&M management of endpoints.

2. Enabling or disabling hot patching

You can click **Fix** in the **Operation** column of a vulnerability and then enable or disable hot patching for this vulnerability on the displayed page. You can also select multiple vulnerabilities and click **Hot Patch** or **Remove** to enable or disable hot patching for these vulnerabilities at a time.

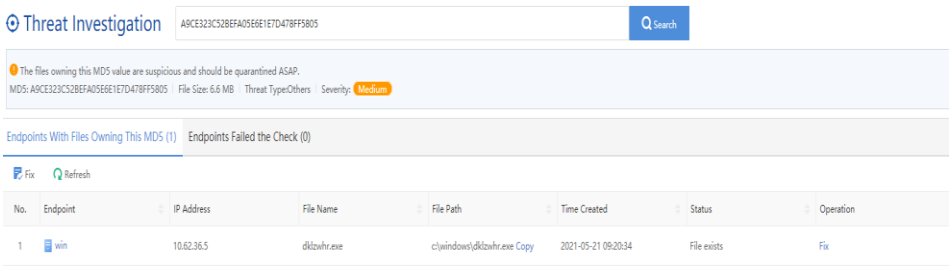
NOTE

Suppose the system does not detect any endpoints that need to be hot patched. In that case, the hot patching function may be disabled or no high-severity vulnerabilities exist in the managed endpoints.

3.6.5 Investigation

Threat investigation can quickly and accurately locate network-wide endpoints infected with the same malicious file or access the same risky domain name by analyzing the file MD5 value or domain name and allowing you to process threats based on locating results.

On the **Investigation** page, you can enter the MD5 value of a malicious file or a risky domain name in the search box and click the search icon to search for the threat. The following figure shows the search result.



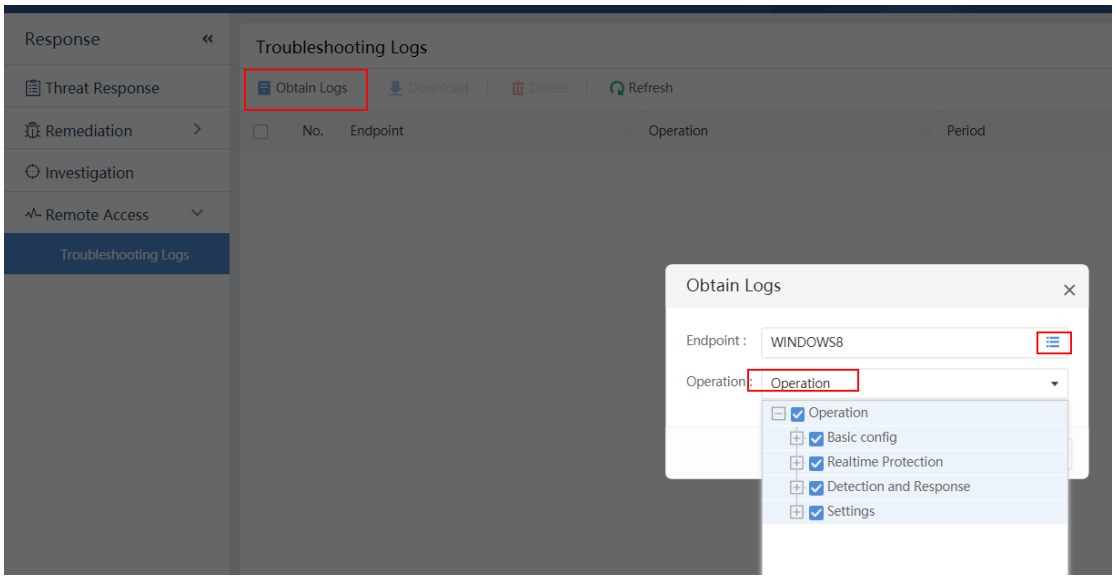
You can view endpoints and processes that access the risky domain name, process file paths, the number of access times, and the total number of process files on the result page. For infected endpoints, you can click **Analyze**, **Fix**, **Trust**, or **Ignore** in the **Operation** column to process the threat for these endpoints.

3.6.6 Remote Access

The remote access function allows you to obtain endpoint troubleshooting logs, which facilitates O&M management.

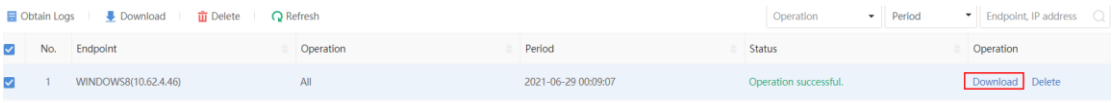
Troubleshooting Logs

1. Choose **Response** > **Remote Access** > **Troubleshooting Logs**, click **Obtain Logs**, and select an endpoint and a log type, as shown in the following figure.



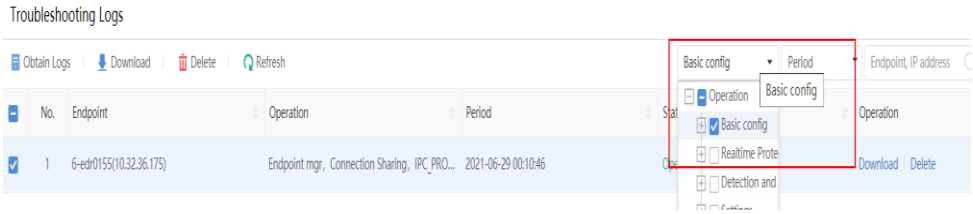
2. Click **OK**. After logs are obtained, click **Download** to download

troubleshooting logs of the endpoint.

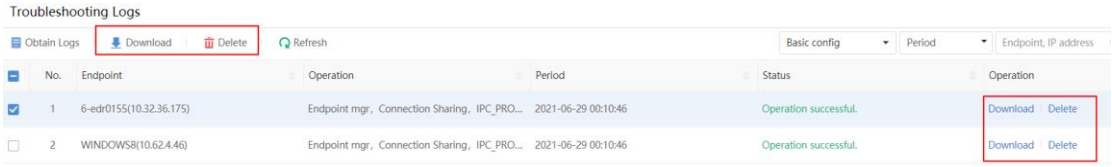


Troubleshooting Log Management

1. On the **Troubleshooting Logs** page, you can view the endpoint name, log type, and status of a log, filter endpoints by log type and task period, and enter an endpoint name or IP address in the search box to search for the specific endpoint.



2. You can select one or more logs and click **Download** or **Delete** to download or delete the logs. You can also click **Download** or **Delete** in the **Operation** column of a log to download or delete the log. The following figure shows the **Troubleshooting Logs** page.

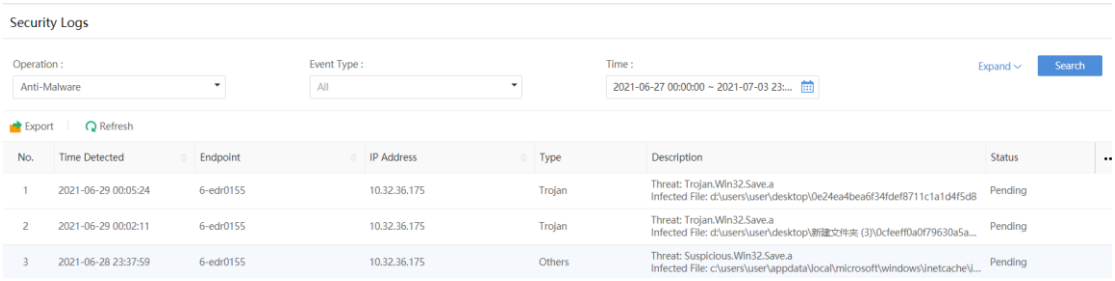


3.7 Logs

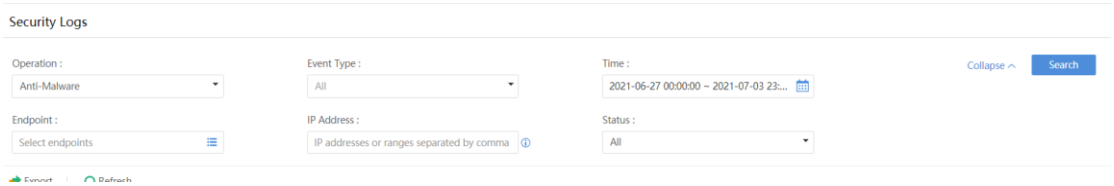
The **Logs** module consists of the **Security Logs**, **Coordinated Action**, **Operation Logs**, **Admin Logs**, and **Reports** nodes.

3.7.1 Security Logs

The **Security Logs** page displays security logs about different security policies, such as anti-malware, vulnerability scan, integrity check, intrusion detection, micro-segmentation, server protection, and USB control. The following figure shows the **Security Logs** page.

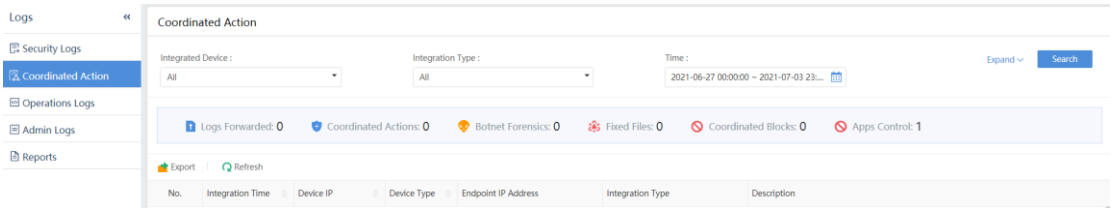


You can filter security logs by log type, statistical period, and time and click **Expand** to further search for security logs by endpoint name and IP address. You can click **Export** to export the search result.



3.7.2 Coordinated Action

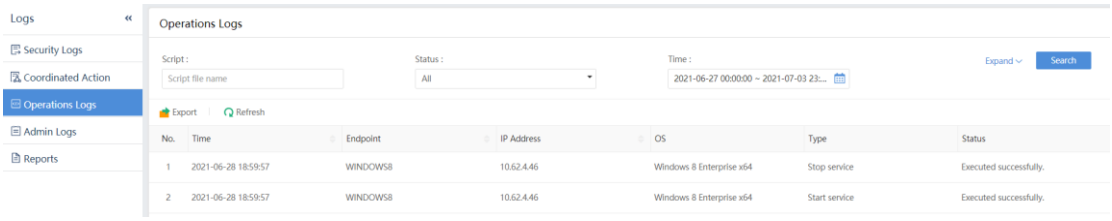
The **Coordinated Action** page displays information about integration between Endpoint Secure and other products, including NGAF, Cyber Command, IAG, Platform-X, and Neutral-X. The information includes the overall integration status, integration time, IP addresses and types of integrated devices, integration type, and integration description. The following figure shows the **Coordinated Action** page.



You can filter integration logs by integrated device, statistical period, and time and click **Expand** to further search for integration logs by endpoint name, IP address, and integration type. You can click **Export** to export the search result.

3.7.3 Operation Logs

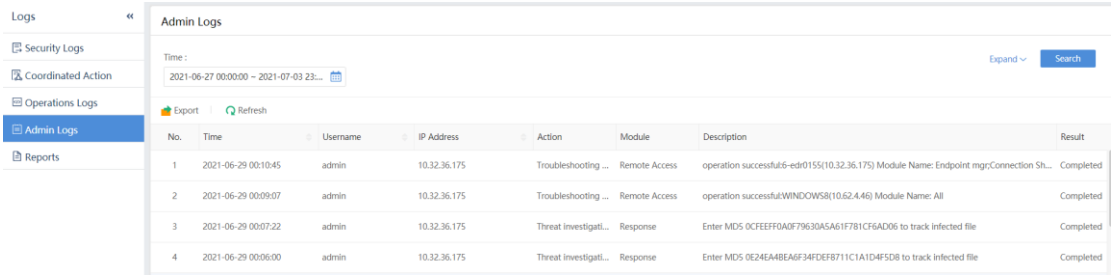
The **Operation Logs** page displays operation logs about remote access, including the operation time, endpoint name, IP address, OS, type, and execution status. The following figure shows the **Operation Logs** page.



You can filter operation logs by script file name, statistical period, and time and click **Expand** to further search for operation logs by endpoint name, IP address, and execution status. You can click **Export** to export the search result.

3.7.4 Admin Logs

The **Admin Logs** page displays logs about administrators' operations on the Endpoint Secure Manager, including the operation time, username, IP address, operation type, object, description, and result. The following figure shows the **Admin Logs** page.

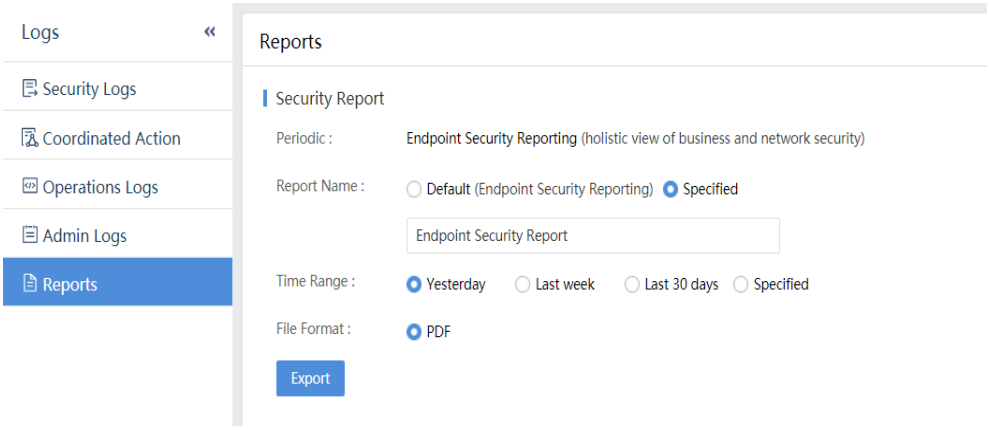


You can filter admin logs by statistical period and time and click **Expand** to further search for admin logs by username, IP address, and execution status. You can click **Export** to export the search result.

3.7.5 Reports

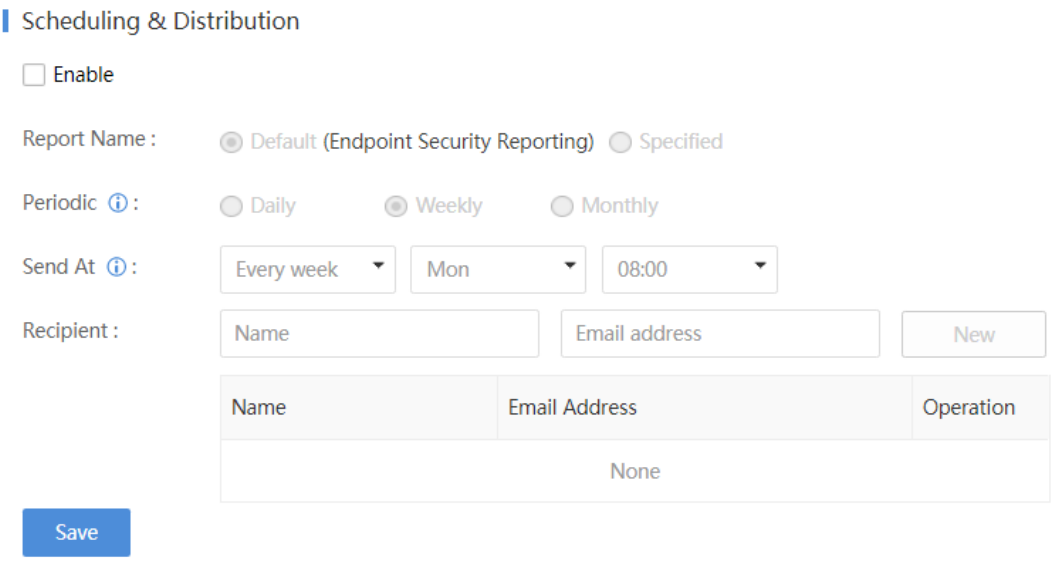
Export

In the **Security Report** area, you can export the endpoint security report. The report analyzes the security status of network-wide endpoints, helping you quickly understand business and network security risks. When exporting the report, you can specify the report name, period, and format. The following figure shows the configuration page.



Scheduling & Distribution

In the **Scheduling & Distribution** area, you can select **Enable** to subscribe to reports and configure the report name, report type, sending time, and recipient. The following figure shows the configuration page.



The parameters are as follows:

- **Periodic**: The options include **Daily**, **Weekly**, and **Monthly**, which indicate reports generated by one calendar day (00:00-24:00), one calendar week (Monday-Sunday), and one calendar month (the first day to the end day of a month), respectively.
- **Send At**: time for sending reports to the recipient.

3.8 System

The **System** module consists of **Agent Deployment**, **System Updates**, **Integrated Devices**, **Branches**, **Administrators**, **Licensing**, and **System** nodes.

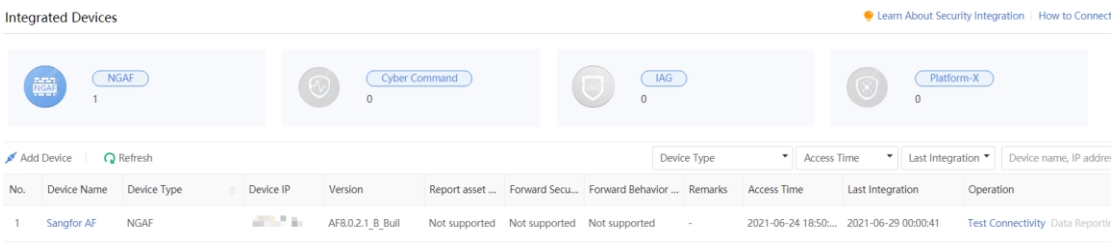
NOTE

For details about Agent deployment, see Installation. For details about system updates, see Product Update.

3.8.1 Integrated Devices

The **Integrated Devices** page manages integration between Endpoint Secure and NGAF, Cyber Command, IAG, Platform-X, and Neural-X. Security integration provides threat detection, scanning, and removal solutions for customers.

The following figure shows the **Integrated Devices** page. You can click **How to Connect** to view configurations for integration between Endpoint Secure and different products.



You can view integrated devices and details about each integrated device on the **Integrated Devices** page, including the device name, type, IP address, version number, access time, and last integration time. You can filter integrated devices

by device type, access time, and previous integration time and enter a device name or an IP address in the search box to search for the specific device.

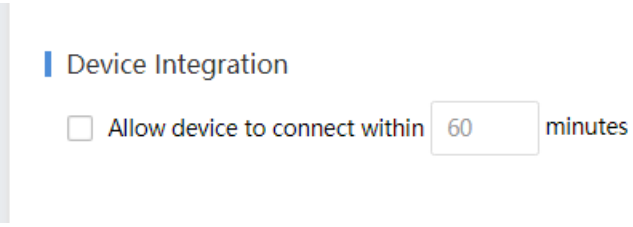
In addition, you can click **Test Connectivity** or **Delete** in the **Operation** column of an integrated device to test connectivity or remote integration for the device.

The following table lists function supported for integration between Endpoint Secure and other products.

Integrated Product	Agent Deployment Redirection	Correlated Block	Log Reporting	Access Control	Correlated Scan	Correlated Malicious File Fixing	Process Forensics	Anti-Proxy
IAG	Yes	No	No	No	Yes	Yes	No	Yes
NGAF	No	No	No	No	Yes	Yes	Yes	Yes
Cyber Command	No	Yes	Yes	Yes	Yes	Yes	Yes	No
Platform-X	No	No	No	No	No	Yes	Yes	No
Neural-X	No	No	Yes	No	Yes	Yes	No	No

Table 6: Functions supported for integration between Endpoint Secure and other products

To integrate Endpoint Secure with any product required to enable **Device Integration** setting. Choose **System** > **System** > **General**, enable **Device Integration**, and set the access time of the integrated device, as shown in the following figure.



NOTE

You should only enable the **Device Integration** option when other Sangfor products are first time connected.

3.8.1.1 Integration with IAG

Integration between Endpoint Secure and IAG ensures Endpoint Secure Agent deployment redirection, coordinated virus scan, and other functions. To integrate Endpoint Secure with IAG, ensure that the following conditions are met:

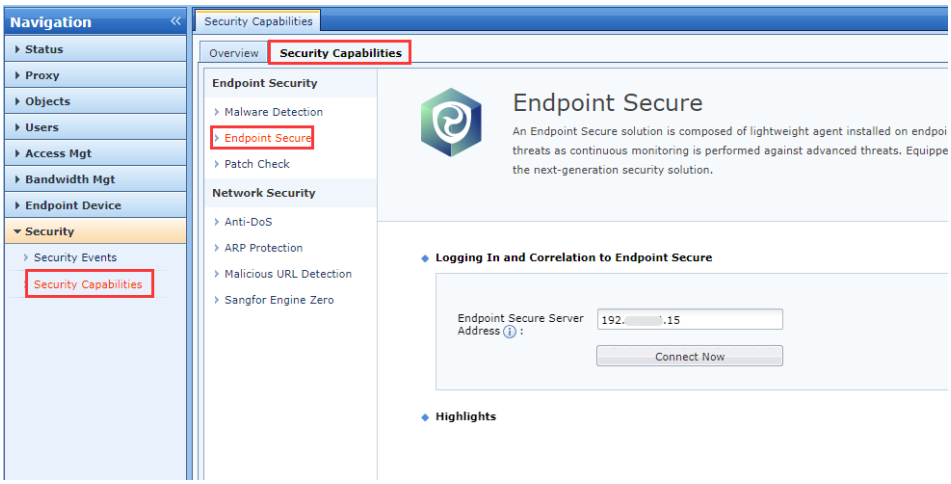
Network connectivity: IAG can communicate with TCP port 443 of Endpoint Secure.

Version: The IAG version is 12.0.16 or later.

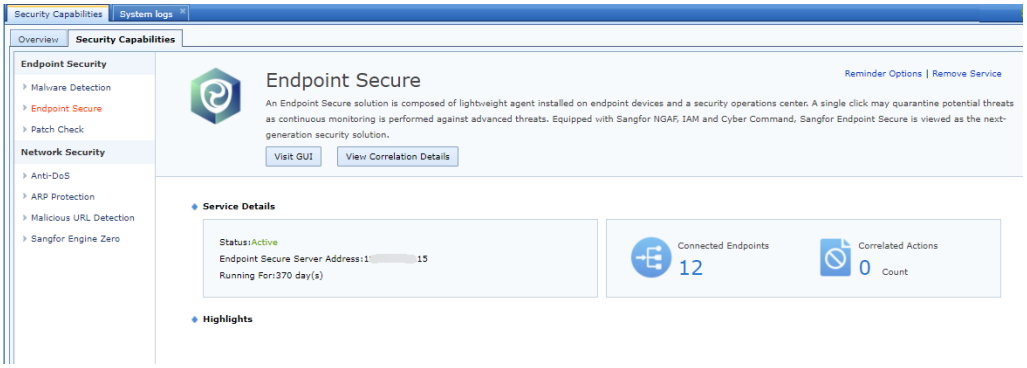
Integration Procedure

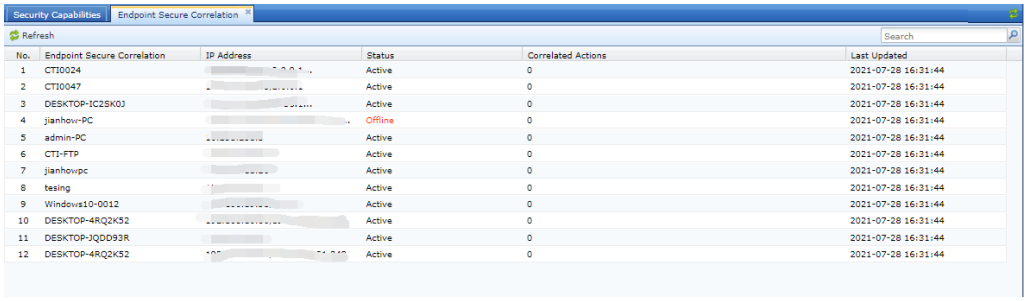
To integrate Endpoint Secure with IAG, you only need to configure data on IAG. The configuration procedure is as follows:

Step 1. Log in to the IAG Manager, choose **Security** > **Security Capabilities** > **Endpoint Secure (ES).** Enter the Endpoint Secure Manager IP address in the **Endpoint Secure Manager IP** text box, and click **Connect Now**. The following figure shows the configuration page.



Step 2. After the integration is successful, Endpoint Secure is in an **Online** state in the **Endpoint Secure Service** area.

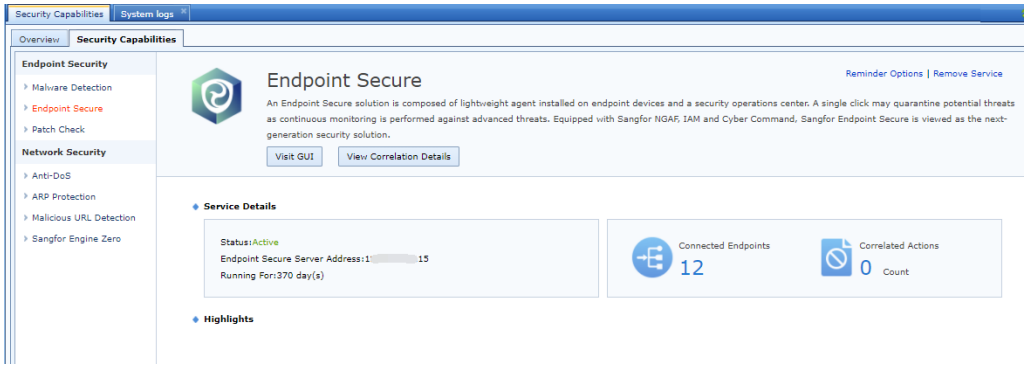


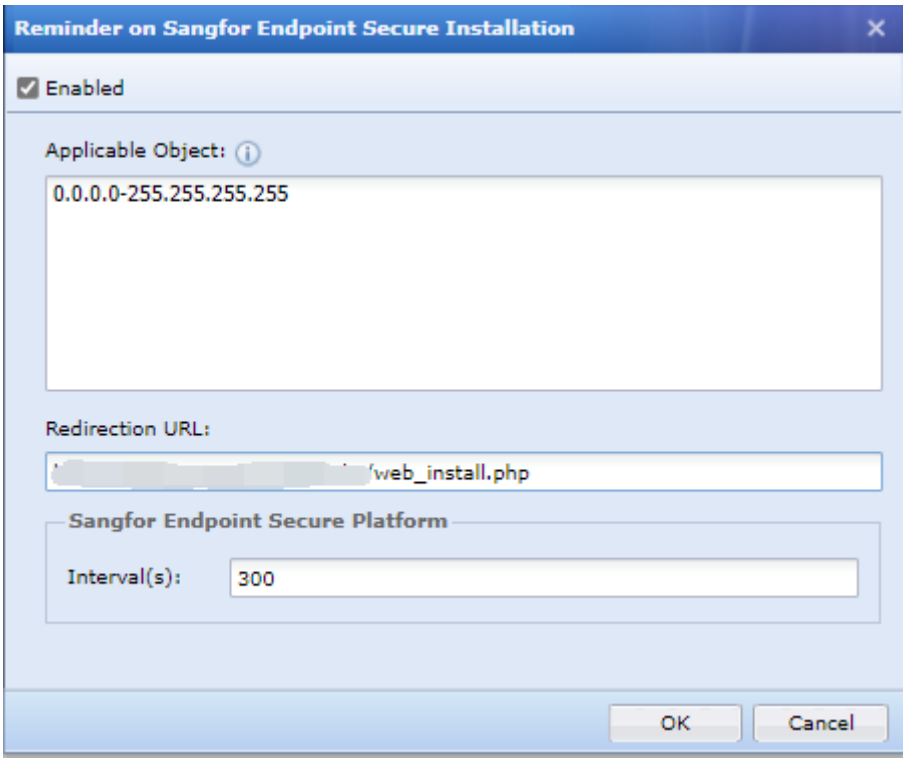


Integration Effect

1. Agent deployment redirection

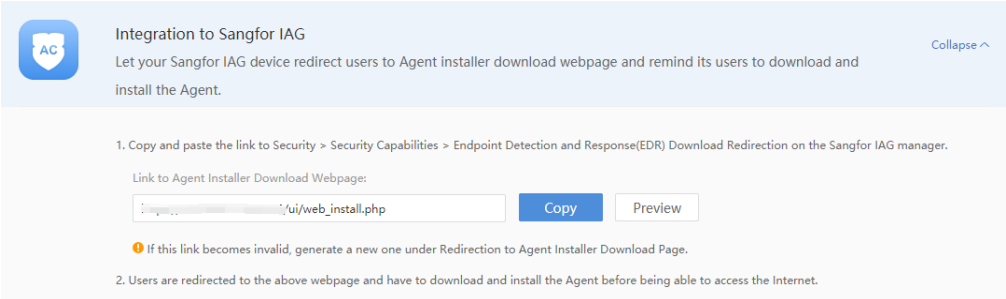
Choose **Security** > **Security Capabilities** > **Endpoint Secure**, click **Reminder Options** and configure the address range for Agent deployment redirection and the address for redirecting to the Agent download page, as shown in the following figure.



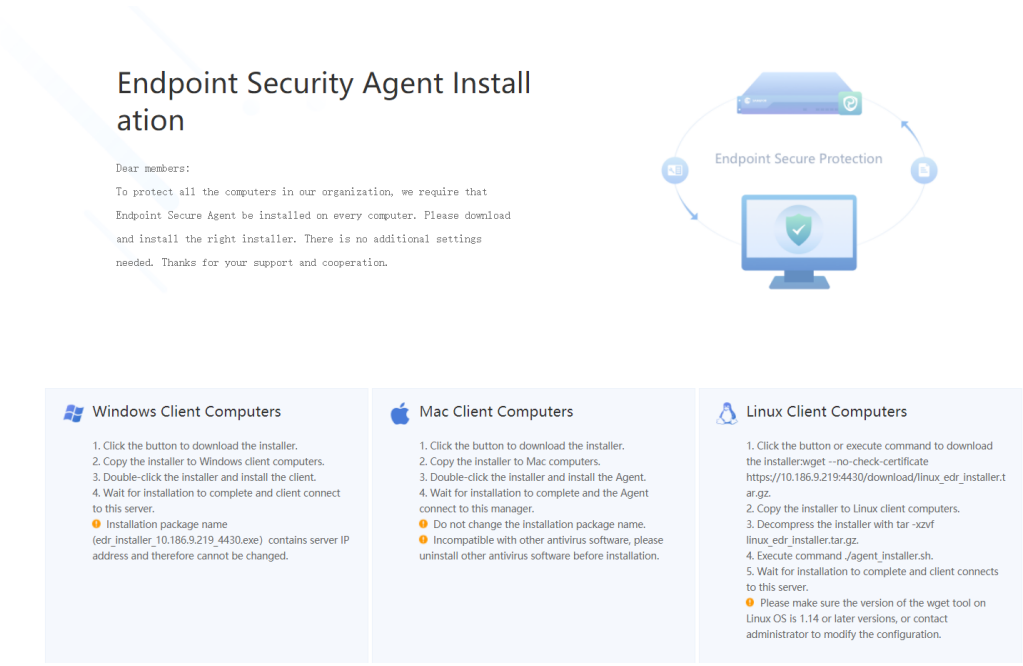


Address Range: Enter the range of intranet IP addresses that require Agent installation.

Redirection Address: Enter the address in **Integration to Sangfor IAG** under **System** > **Agent Deployment** of the Endpoint Secure Manager, as shown in the following figure.

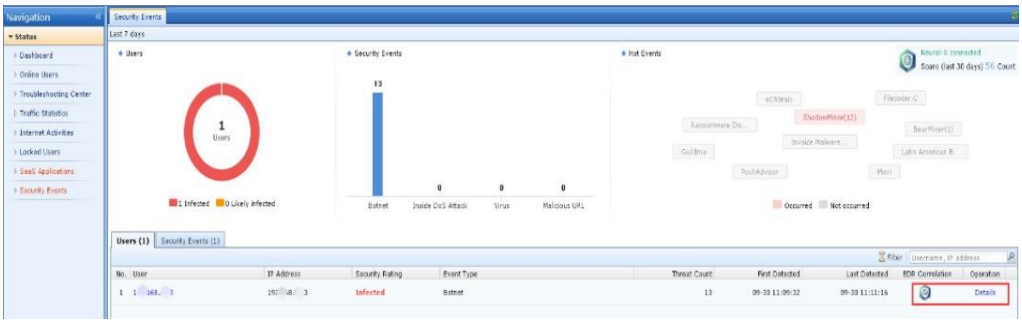


After the configuration is complete, you will be redirected to the Agent deployment notification page when you open a web page. The Agent deployment notification page pops up periodically until you download and install Agent, as shown in the following figure.

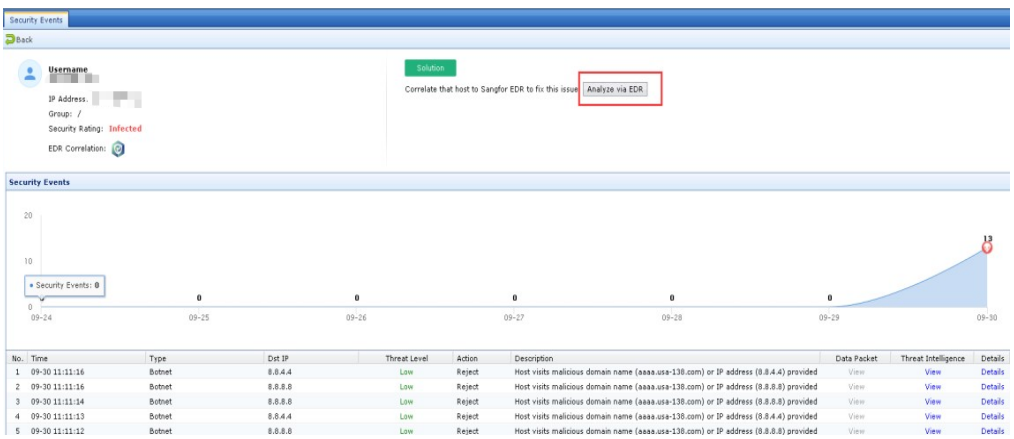


2. Correlated virus scan

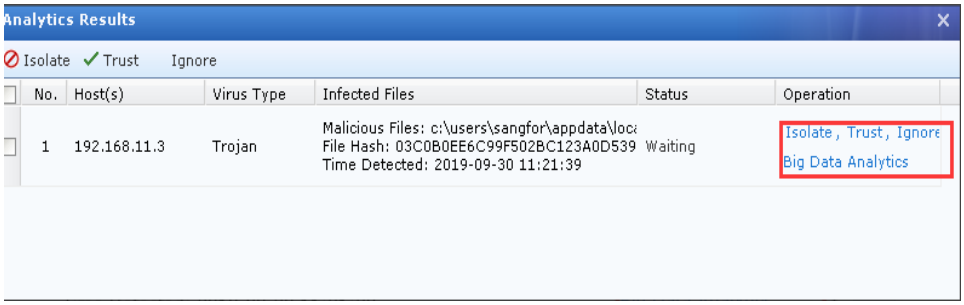
When botnet detection is enabled on IAG and IAG identifies risky endpoints, IAG can correlate with Endpoint Secure for virus scan. On the IAG Manager, choose **Real-Time Status** > **Security Status** and click **Risky Users**, as shown in the following figure.



Click **View Details**, as shown in the following figure.



Click **Integrated Analysis** to perform a virus scan for risky endpoints. The scan result is displayed, as shown in the following figure. You can isolate, trust, or ignore malicious files found after a correlated virus scan is done on the scan result page.



3.8.1.2 Integration with Cyber Command

Integration between Endpoint Secure and Cyber Command enables correlated virus scan, and inbound and outbound traffic isolation for risky endpoints after malicious files or risky endpoints are found by Cyber Command. In addition, security logs generated by Endpoint Secure can be reported to Cyber Command for centralized operations and analysis. To integrate Endpoint Secure with Cyber Command, ensure that the following conditions are met:

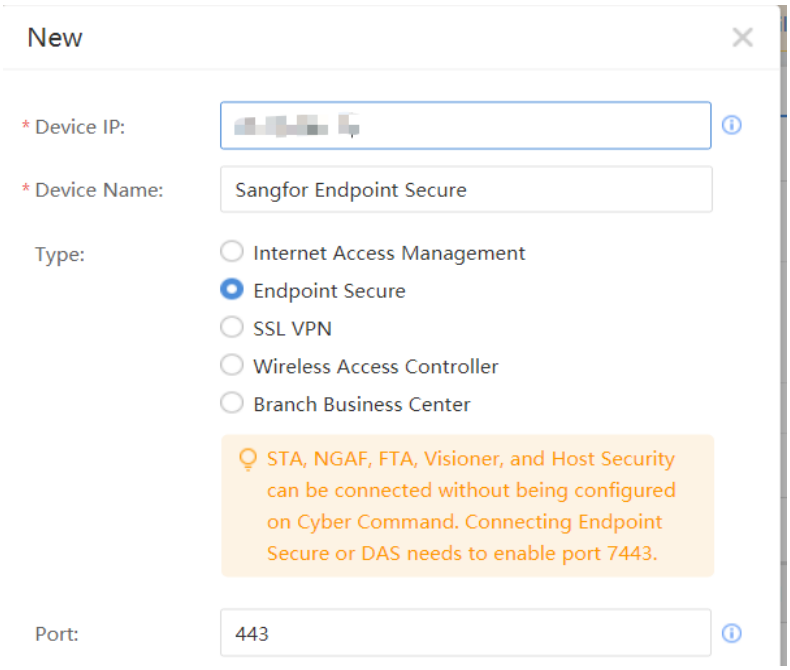
Network connectivity: Cyber Command can communicate with **TCP port 443** of Endpoint Secure, and the Endpoint Secure Manager can communicate with **TCP port 7443** of Cyber Command.

Version: The Cyber Command version is 3.0.49 or later.

To integrate Endpoint Secure with Cyber Command, you only need to configure the Endpoint Secure Manager or Cyber Command Manager.

Integration Procedure on the Cyber Command Manager

Step 1. Log in to the Cyber Command Manager, choose **System** > **Correlated Devices**, and click **New**. On the **Add Device** page, edit the device's IP address, name, and type and click **OK**. The following figure shows the configuration page.



The parameters are as follows:

Device IP: Enter the IP address of the Endpoint Secure Manager.

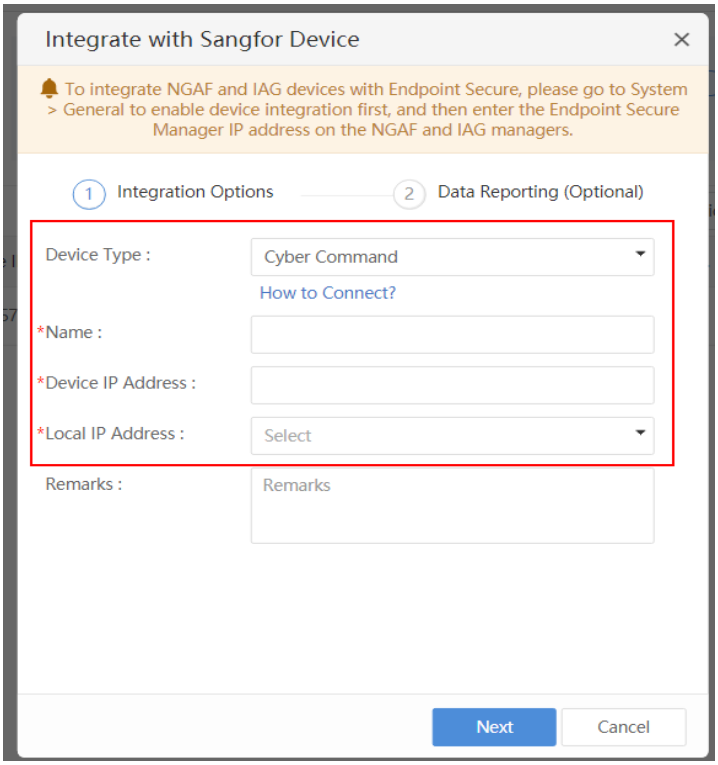
Device Name: Customize a device name that is easy to identify.

Type: Select **Endpoint Secure**.

Step 2. After the integration is successful, the integrated Cyber Command is displayed under **System** > **Integrated Devices** of the Endpoint Secure Manager. You can view details about this Cyber Command and test connectivity.

Integration Procedure on the Endpoint Secure Manager

1. Log in to the Endpoint Secure Manager, choose **System** > **Integrated Devices**, and click **Add Device**. On the **Add Device** page, edit the device type, name, IP address, and correlated localhost IP address and click **Next**. The following figure shows the configuration page. For details, click **How to Connect**.



The parameters are as follows:

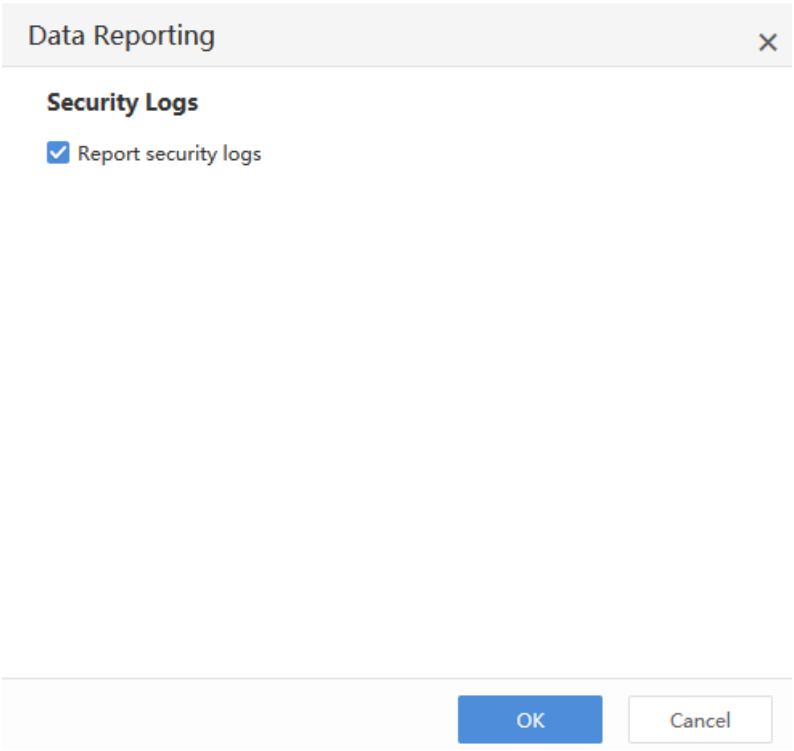
Device Type: Select **Cyber Command**.

Name: Customize a device name that is easy to identify.

Device IP Address: Enter the IP address of the Cyber Command Manager.

Local IP Address: Enter an IP address of the Endpoint Secure Manager that can communicate with Cyber Command.

2. Click **Data Reporting** and select types of logs to be reported, as shown in the following figure.

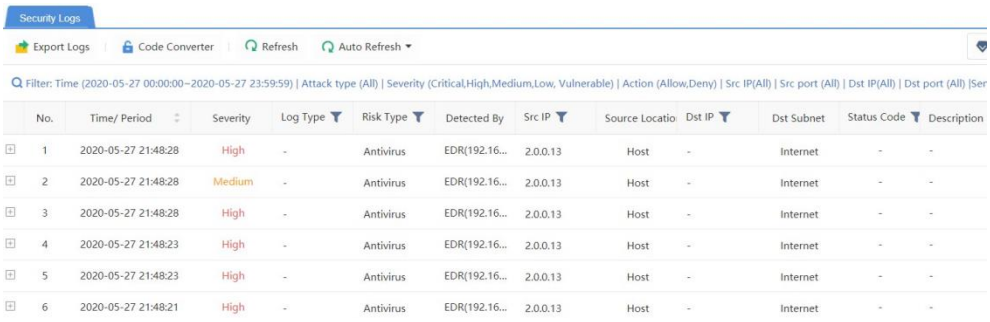


Security Logs: After it is selected, Endpoint Secure will report selected information to the Cyber Command Manager for centralized analysis.

Integration Effect

1. Endpoint Secure security log reporting

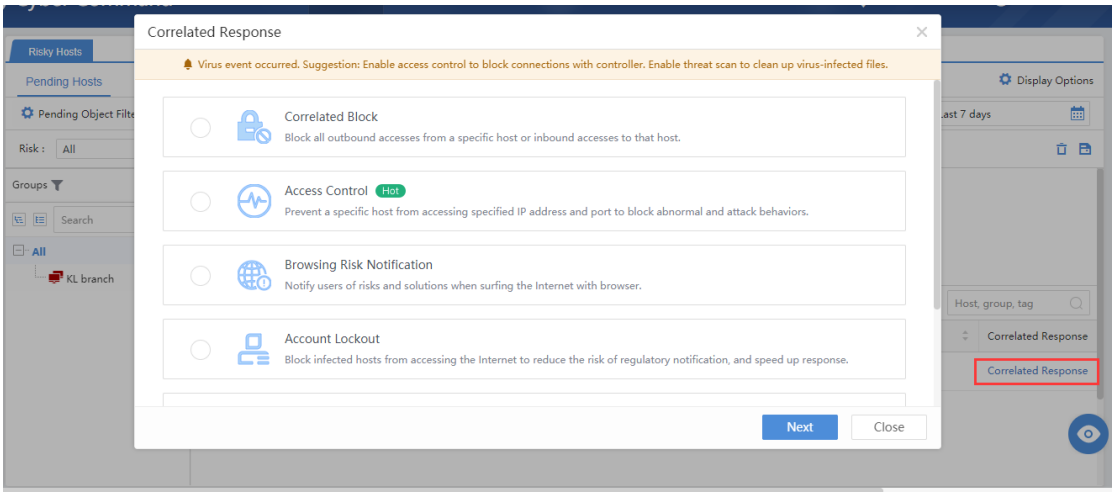
Security logs generated by Endpoint Secure can be automatically reported to the Cyber Command Manager for centralized analysis and operations. On the Cyber Command Manager, you can choose **Analytics > Security Logs** and select Endpoint Secure as the data source to query and analyze security logs reported by Endpoint Secure, as shown in the following figure.



2. Correlated virus scan

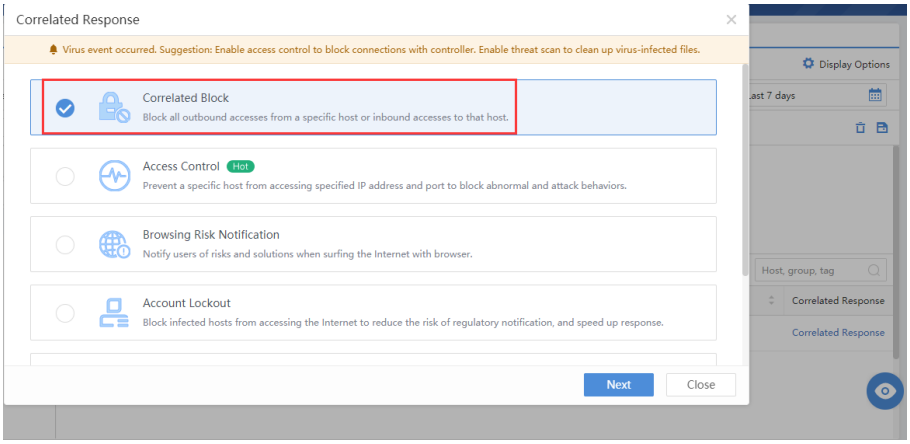
When Cyber Command identifies risky endpoints, it can be correlated with Endpoint Secure for virus scan. Under **Response** > **Risky Hosts** of the Cyber Command Manager, you can correlate Cyber Command with Endpoint Secure

to perform virus scans for identified risky endpoints and isolate, trust, or ignore identified malicious files. The following figure shows the integration page.



3. Risky endpoint isolation

When Cyber Command identifies risky endpoints, it can correlate with Endpoint Secure to isolate risky endpoints. Under **Response** > **Risky Hosts** of the Cyber Command Manager, you can correlate Cyber Command with Endpoint Secure to perform endpoint isolation, outbound isolation, or inbound isolation operations. The following figure shows the integration page.



3.8.1.3 Integration with NGAF

Integration between Endpoint Secure and NGAF enables correlated virus scan and botnet forensics. To integrate Endpoint Secure with NGAF, ensure that the following conditions are met:

Network connectivity: NGAF can communicate with TCP port 443 of Endpoint Secure.

Version: The NGAF version is 8.0.17 or later.

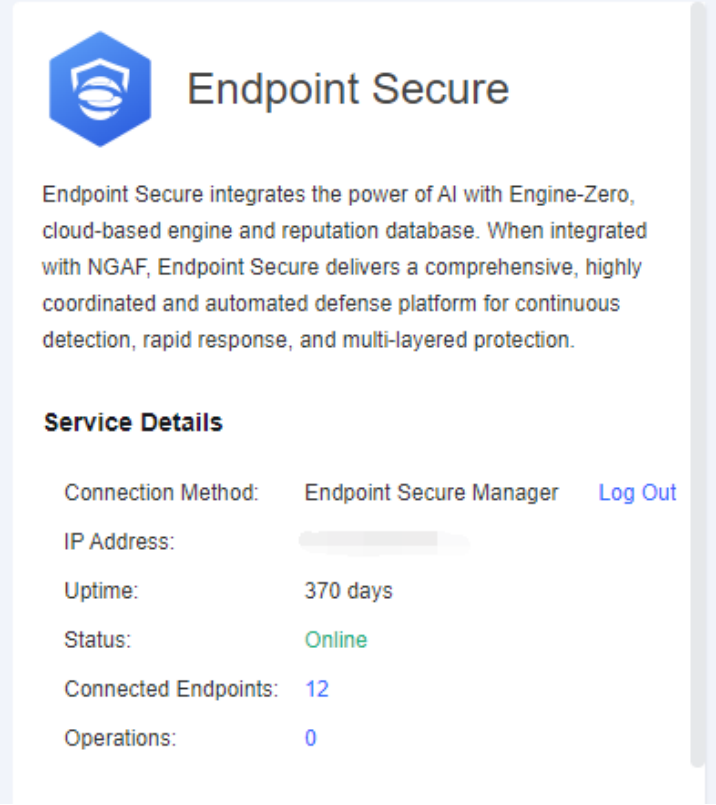
To integrate Endpoint Secure with NGAF, you only need to configure data on the NGAF Manager.

The following procedure and integration effect will be using NGAF v8.0.35 as an example.

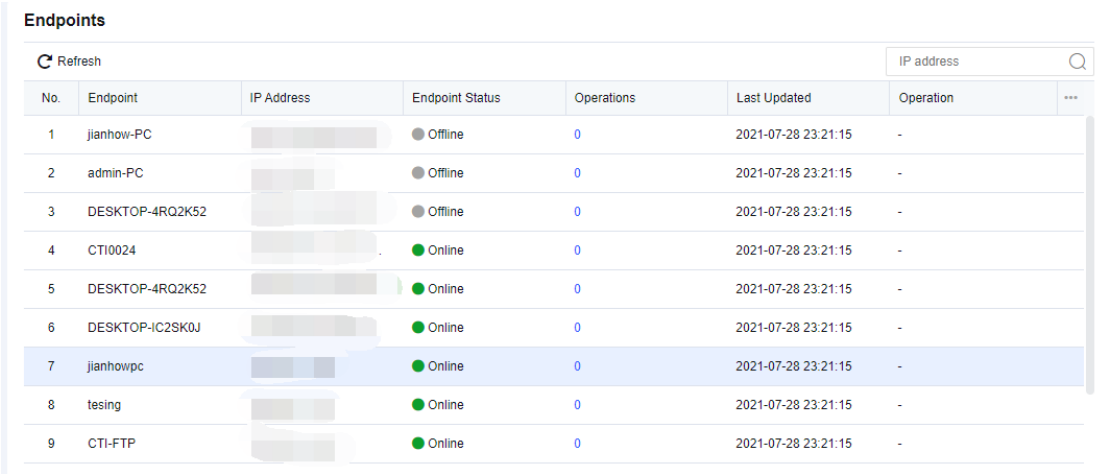
Integration Procedure

Step 1. Log in to the NGAF Manager, choose **SOC > Endpoint Protection > Endpoint Protection options.** Click **Endpoint Secure Manager** and enter the IP address of the Endpoint Secure Manager on the displayed page. Then, click **Connect**. The following figure shows the configuration page.

Step 2. After the integration is successful, Endpoint Secure is in the **Online** state on the above page, as shown in the following figure.



In addition, you can view integrated endpoints and their status under **SOC > Endpoint Protection Options > Endpoint Protection Options**, as shown in the following figure.

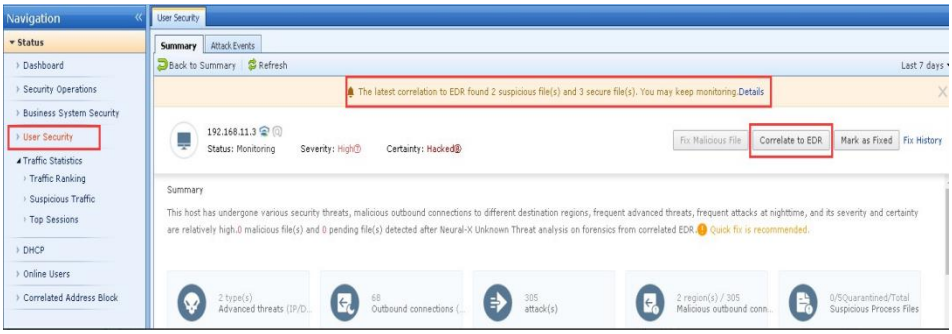


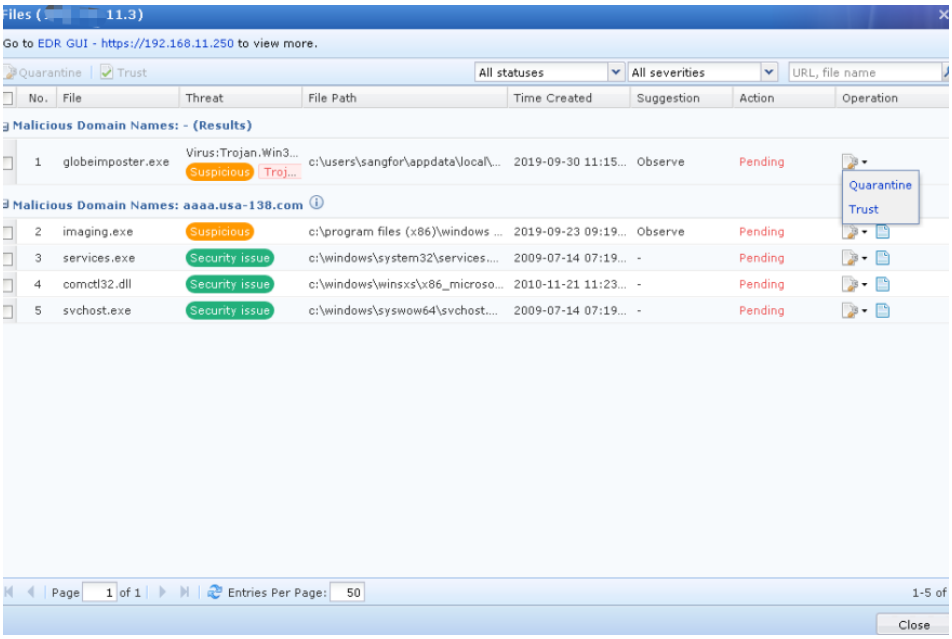
Integration Effect

After the integration is successful, Endpoint Secure can correlate with NGAF for virus scan, botnet forensics, and other operations.

1. Correlated virus scan

When NGAF identifies risky endpoints, it can correlate with Endpoint Secure for virus scan. Under **SOCs** > **User Security** of the NGAF Manager, you can correlate NGAF with Endpoint Secure to perform a virus scan for identified risky endpoints and isolate or trust identified malicious files. The following figure shows the integration page.

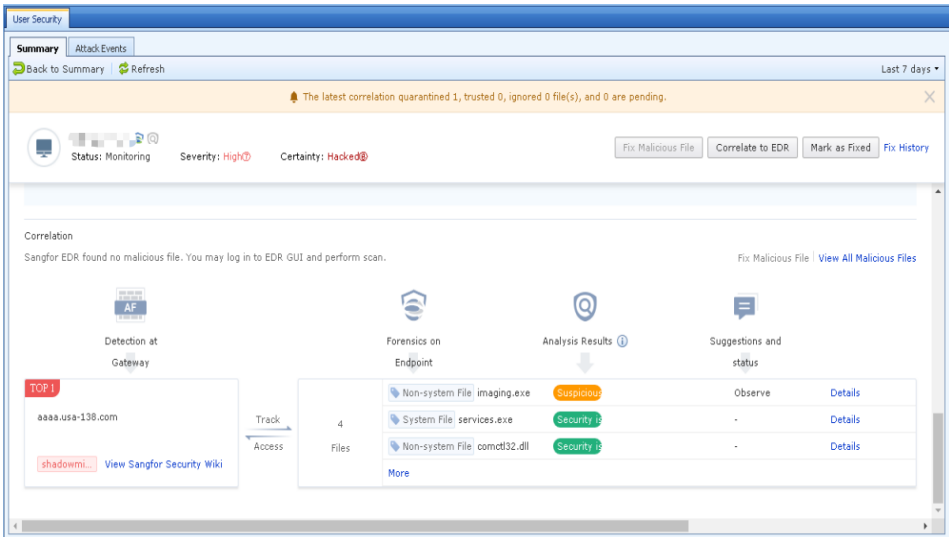




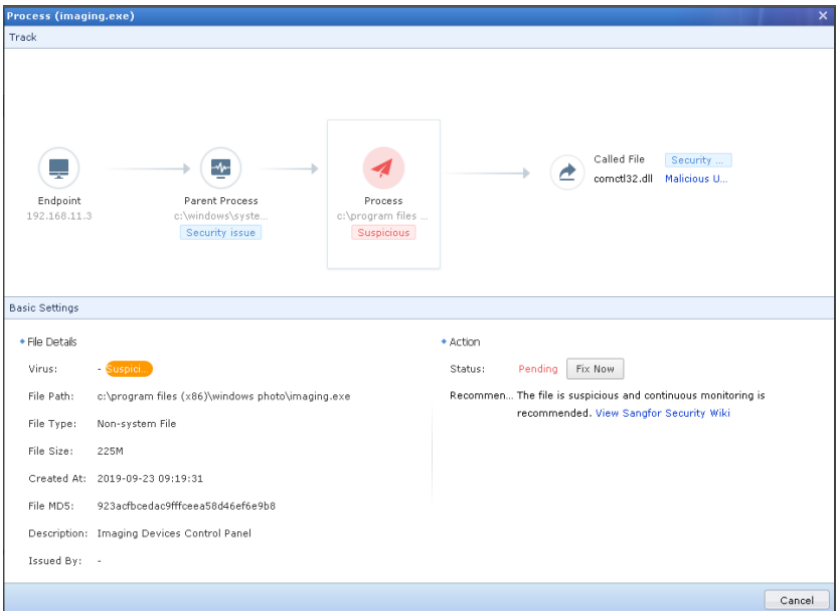
2. Correlated botnet forensics

Endpoint Secure can record domain names accessed by endpoints and processes. When NGAF finds botnet logs, it can correlate with Endpoint Secure for botnet forensics and backtracking to help users identify the processes that access botnet domain names and the process files. Under **SOC > User Security**

of the NGAF Manager, you can view suspicious files of risky endpoints, which are the botnet forensics results, as shown in the following figure.

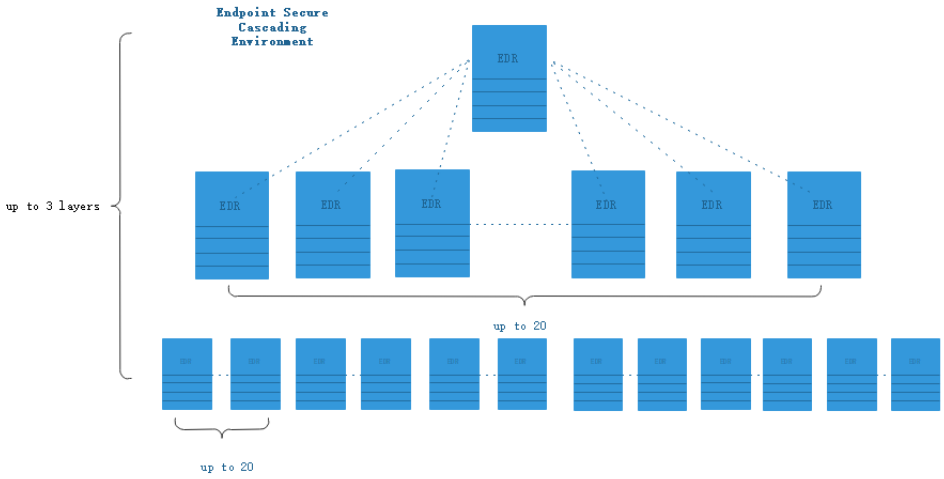


You can click **Details and Operation** to view the backtracking result of malicious domain name access and handle malicious files, as shown in the following figure.

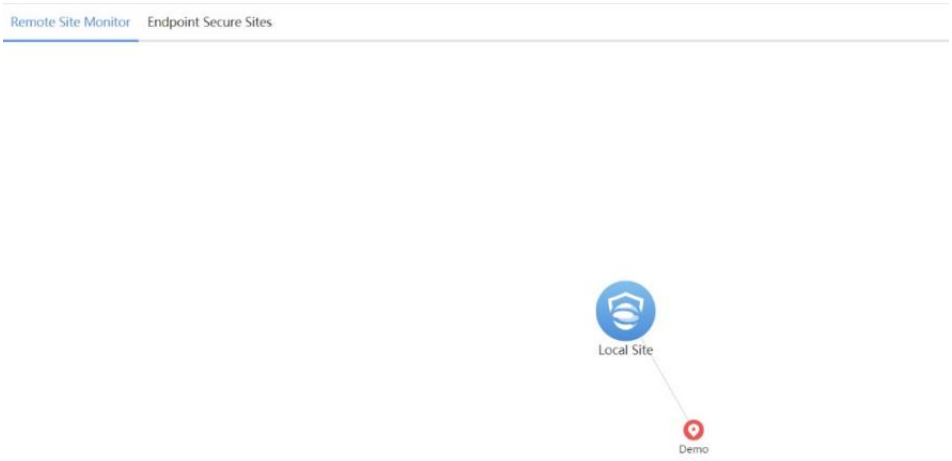


3.8.2 Branches

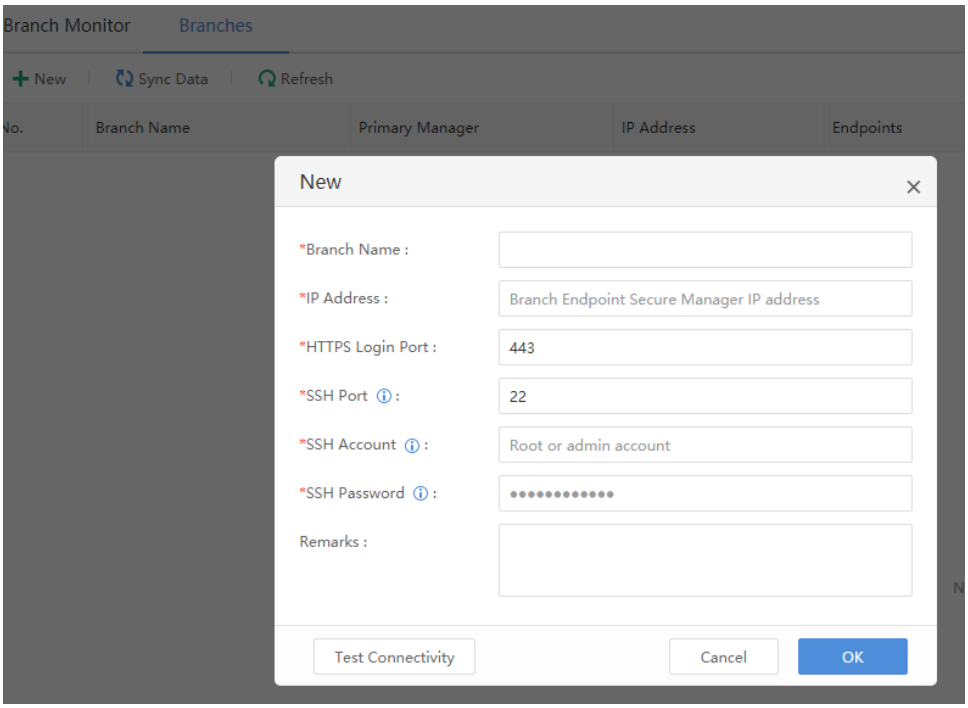
The **Branches** page consists of the **Branch Monitor** and **Branches** tab pages for cascading Endpoint Secure management. Up to three cascading layers are supported, and each Endpoint Secure can be cascaded with up to 20 Endpoint Secure Managers. The following figure shows the Endpoint Secure cascading environment.



On the **Branch Monitor** tab page, you can view the security information of cascaded branches. You can click the icon in the upper right corner to switch between topology and chart formats, as shown in the following figure.



To configure cascaded branches, click **New** on the **Branches** tab page. On the displayed page, edit information about the cascaded Endpoint Secure Manager. Then, click **Test Connectivity**. If network connectivity is normal, click **OK**. The following figure shows the configuration page.



The parameters are as follows:

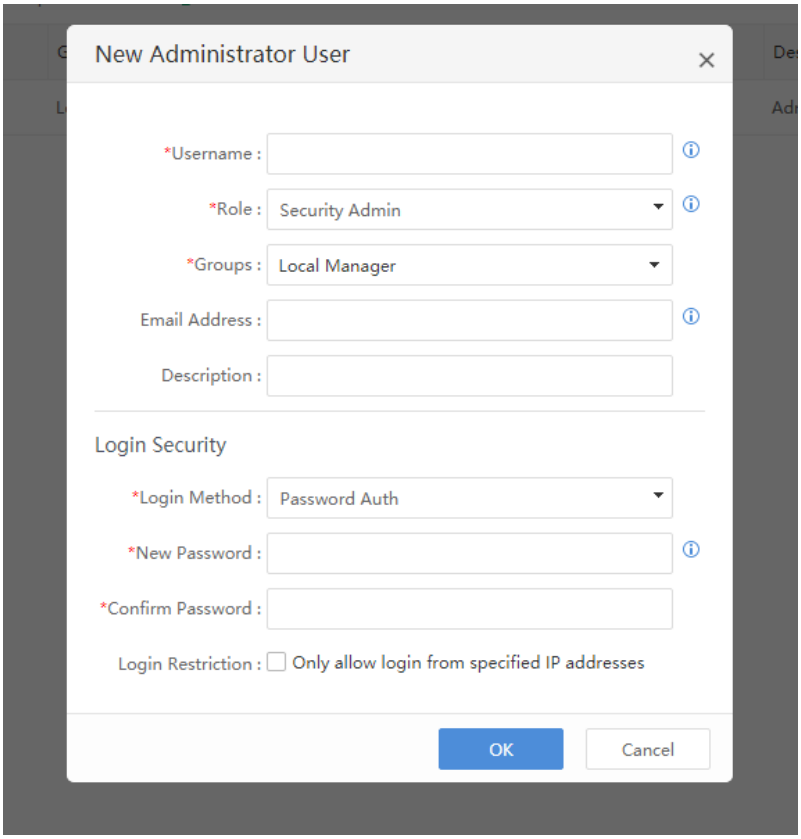
HTTPS Login Port: port used for the HTTPS login page of the Endpoint Secure Manager. The default port is 443. The actual value prevails.

SSH Port, **SSH Account**, and **SSH Password**: The default SSH port is 22. The account is **root**. The password can be entered as required.

3.8.3 Administrators

3.8.3.1 Administrator Permissions

You can perform the following operations to create administrators with different permissions as required: Log in to the Endpoint Secure Manager, choose **System** > **Administrators**, and click **New** to create an administrator user, as shown in the following figure.



For the **Role** parameter, you can select different roles as required.

System Admin: only has permissions to view the home page and configure system settings.

Security Admin: has all permissions except those required to perform operations on the **Micro-Segmentation**, **Integrated Devices**, **Reports**, **Administrators**, **System Updates**, **Licensing**, **Branches**, and **System** modules.

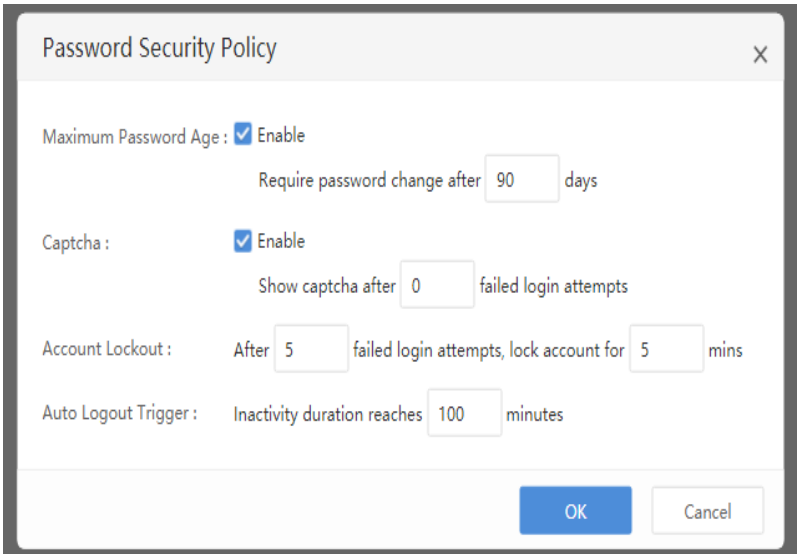
Audit Admin: has permission to view system information but has no permission to edit, add, or delete information.

Different administrators have different operation permissions. It ensures permission-based management of Endpoint Secure Manager accounts.

3.8.3.2 Password Security Policy

You can configure a password security policy for managing the login to the Endpoint Secure Manager based on your installation requirements. To configure a password security policy, perform the following steps: Log in to the Endpoint Secure Manager. Choose **System** > **Administrators**. On the **Administrators** page, select **Password Security Policy** from the **Global Options** drop-down list.

In the **Password Security Policy** dialog box, set parameters as required, as shown in the following figure.

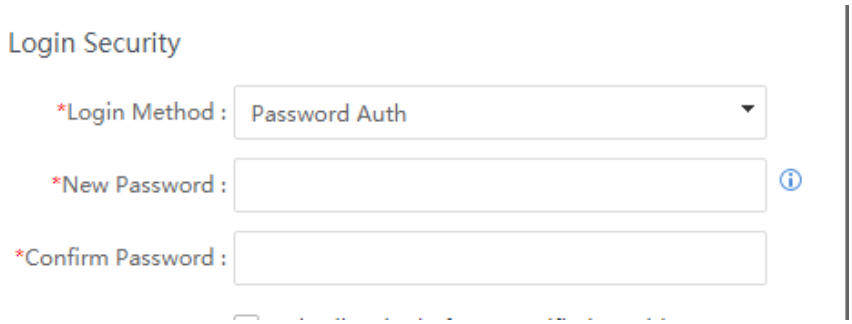


The configuration of a password security policy involves the following parameters:

- **Maximum Password Age**: If you select **Enable** to enable the password validity period, which is disabled by default, you will be forced to change the password during login after the specified period expires (90 days by default, value range: 1-365). If you do not change the password, you will be kicked offline.
- **Captcha**: If you select **Enable** to enable the captcha function, which is enabled by default, a captcha is displayed after the number of consecutive failed login attempts exceeds *N* (0 by default, value range: 0-5).
- **Account Lockout**: When the number of consecutive failed login attempts exceeds *N* (5 by default, value range: 1-5), the login account is locked for *M* minutes (1 minute by default, value range: 1-30).
- **Auto Logout Trigger**: If no operation is performed for *N* minutes (10 minutes by default, value range: 1-120) after login, the login account automatically logs out.

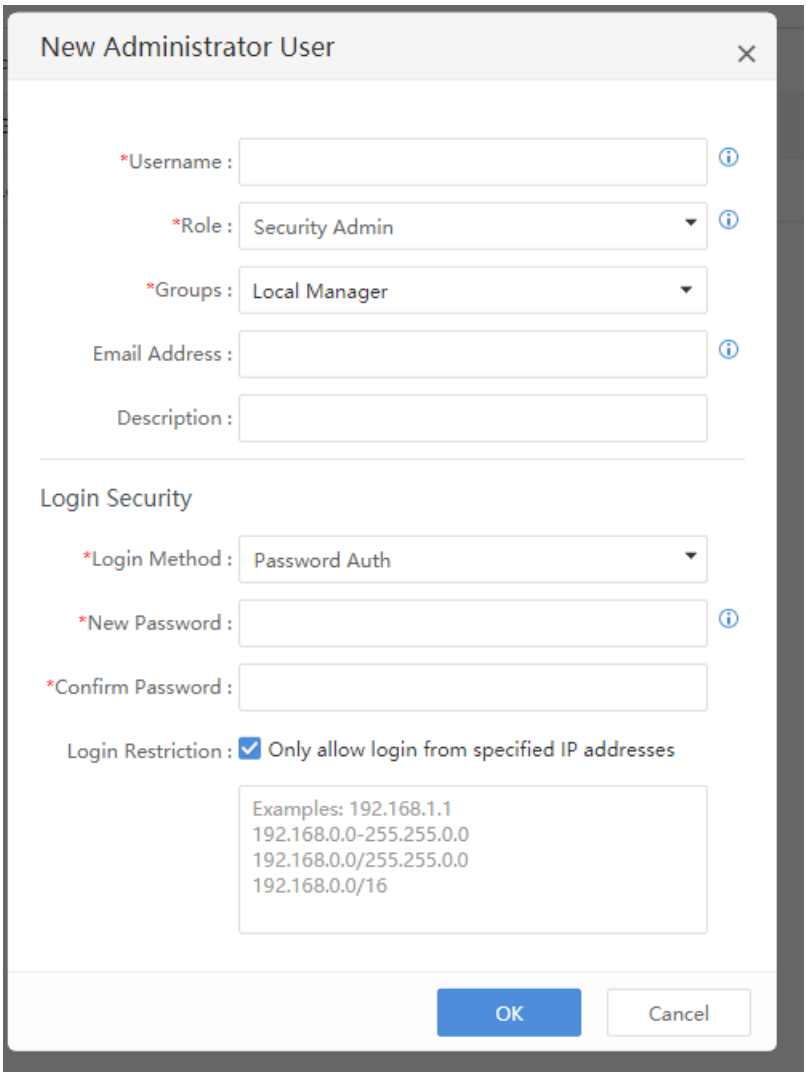
3.8.3.3 Login Account Authentication

The Endpoint Secure Manager provides the **Password Auth** method for authenticating login accounts. To create an administrator user, perform the following steps: Choose **System** > **Administrators**. On the **Administrators** page, click **New** in the upper left corner. In the **New Administrator User** dialog box, create an administrator user, as shown in the following figure.



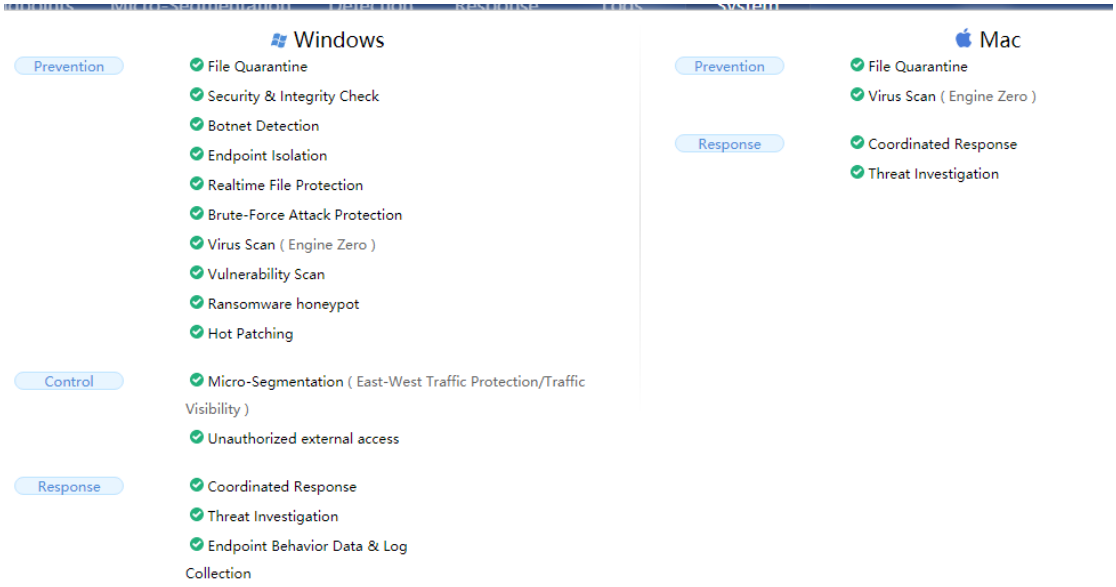
3.8.3.4 Login IP Address Restriction

Endpoint Secure Manager accounts can be used to log in to the Endpoint Secure Manager only from authorized IP addresses. To set the IP addresses from which an account can log in to the Endpoint Secure Manager, select **Only allow login from specified IP addresses** in the **New Administrator User** dialog box when you create the account. Then, enter the required IP addresses, as shown in the following figure.

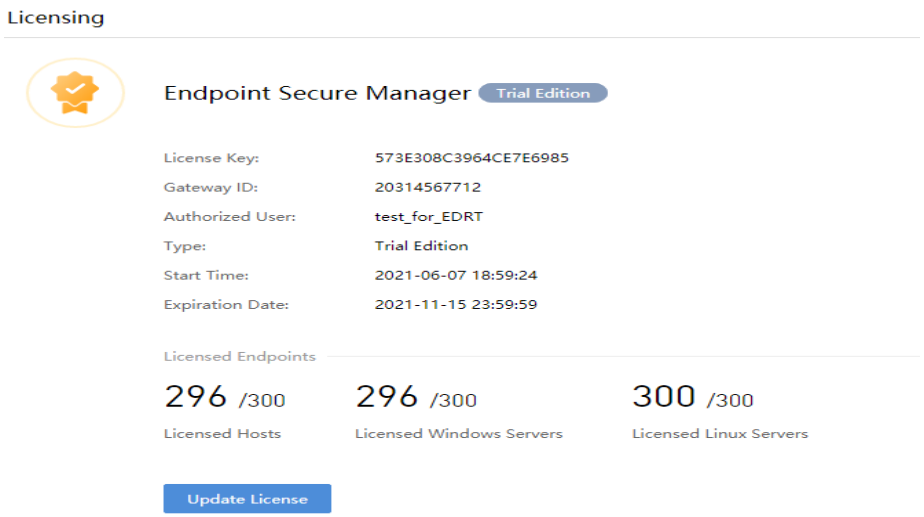

New Administrator User
*Username :
*Role : Security Admin
*Groups : Local Manager
Email Address :
Description :
Login Security
*Login Method : Password Auth
*New Password :
*Confirm Password :
Login Restriction : Only allow login from specified IP addresses
Examples: 192.168.1.1
192.168.0.0-255.255.0.0
192.168.0.0/255.255.0.0
192.168.0.0/16
OK
Cancel

3.8.4 Licensing

Licensing of the Endpoint Secure Manager consists of licenses of the **Prevention**, **Control**, and **Response** modules. The following figure shows complete licensing.



On the **Licensing** page, you can view the licensing status and related information, as shown in the following figure.



NOTE

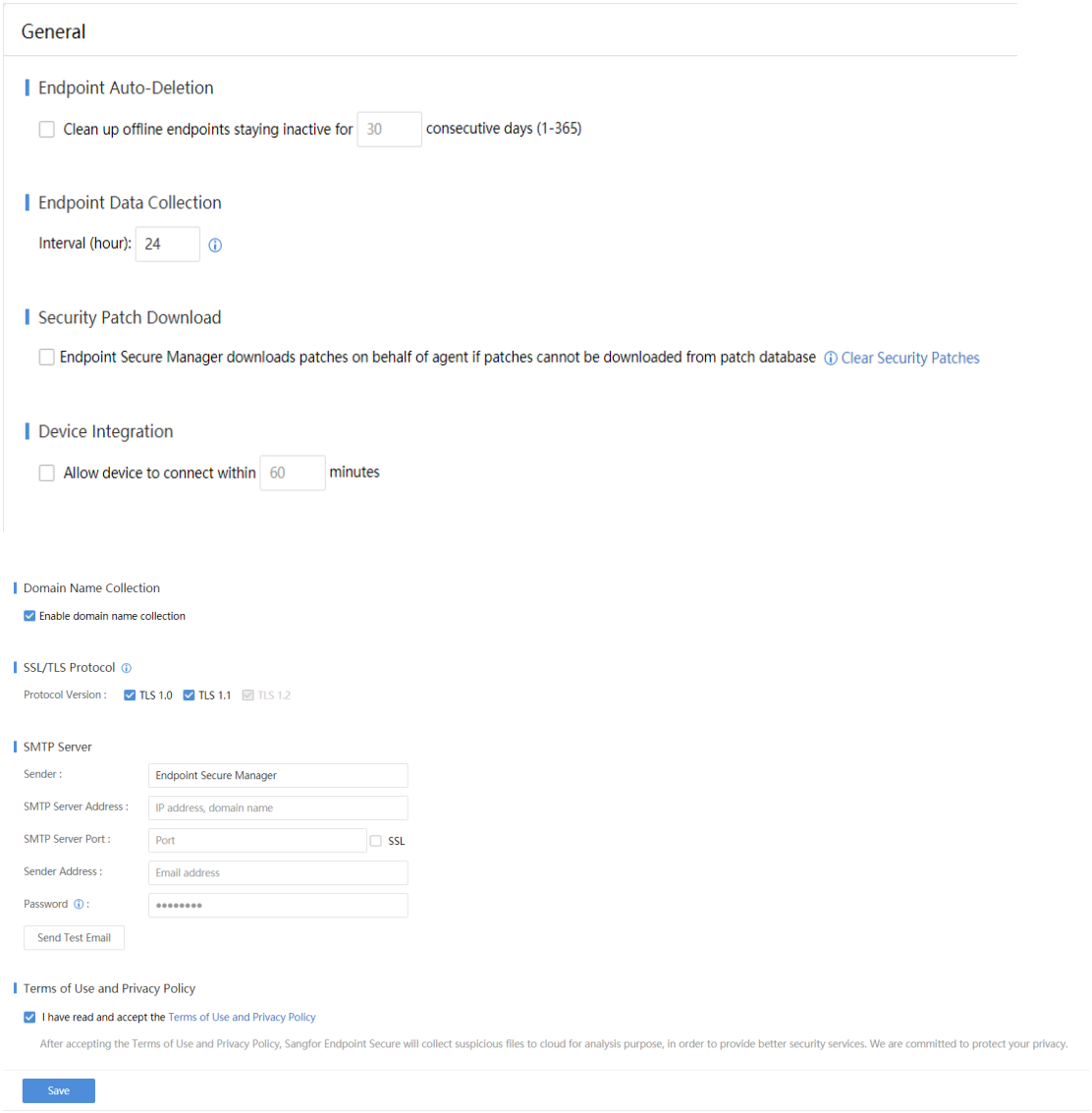
The Endpoint Secure Manager can be used only after it is licensed. For details about the licensing method, see Installation.

3.8.5 System

The **System** module consists of the **General**, **Data Backup**, **Network**, **Logging Options**, **Update Options**, **Alert Options**, and **Tools** nodes.

3.8.5.1 General

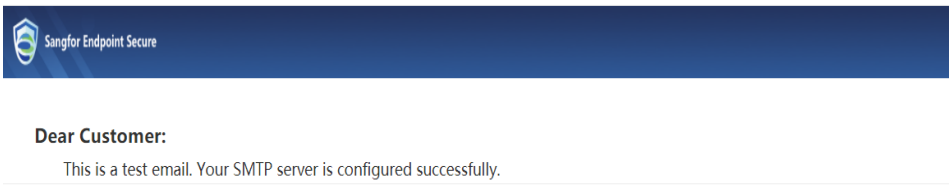
On the **General** page, you can set the date and time, endpoint auto-deletion policy, endpoint data collection interval, security patch download policy, device integration policy, domain name collection policy, SSL/TLS protocol version, Simple Mail Transfer Protocol (SMTP) server, and Terms of Use and Privacy Policy for the Endpoint Secure Manager. The following figure shows the configuration page.



The parameters are as follows:

1. **Date and Time**: Set the date and time of the Endpoint Secure Manager. If you click **Sync with Local PC**, the Endpoint Secure Manager synchronizes the time with the PC used for login. If you click **Obtain System Time**, the motherboard time of the Endpoint Secure Manager server is obtained. If the Endpoint Secure Manager is accessible to the Internet, you can select **Sync time with NTP server periodically**. In this case, the Endpoint Secure Manager synchronizes the time with the NTP server.
2. **Endpoint Auto-Deletion**: Enable automatic deletion of endpoints on the Endpoint Secure Manager that are inactive for a long time to release idle licenses automatically.
3. **Endpoint Data Collection**: Set the interval for collecting endpoint data for endpoint checkup in hours. Enter an integer that ranges from 4 to 168.
4. **Security Patch Download**: If the Agent cannot download security patches due to lack of access to the Internet, the Endpoint Secure Manager can download the security patches on behalf of the Agent. Then, the Agent downloads the security patches from the Endpoint Secure Manager.
5. **Device Integration**: Set the maximum period within which devices integrated with Endpoint Secure are allowed to access the Endpoint Secure Manager. To ensure the access security of integrated devices, such as IAG, NGAF, and Cyber Command, the integrated devices can access the Endpoint Secure Manager only within the specified period when this check box is selected.
6. **Domain Name Collection**: If **Enable domain name collection** is selected, Endpoint Secure can record processes that access malicious domain names. This function is used together with correlated botnet forensics and malicious domain name investigation.
7. **SSL/TLS Protocol**: Protocol versions include TLS1.0, TLS1.1, and TLS1.2. By default, TLS1.2 is enabled because it is more secure than TLS1.0 and TLS1.1. To integrate Endpoint Secure with other devices, you must also select TLS1.0 and TLS1.1.

8. **SMTP Server**: Configure the SMTP server for sending subscription and alert emails. Click **Send Test Email** to check whether the SMTP server is configured. If the configuration is successful, the specified administrator will receive a test email, as shown in the following figure.



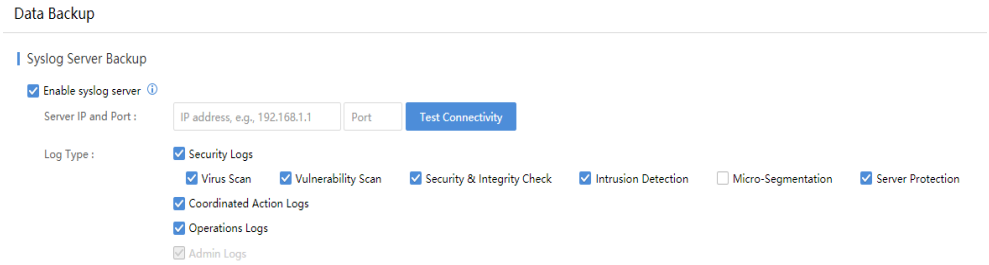
9. **Terms of Use and Privacy Policy**: If **I have read and accept the Terms of Use and Privacy Policy** is selected, Endpoint Secure will collect suspicious files to the cloud for analysis, in order to provide better security services. Make sure that the Endpoint Secure Manager is accessible to https://clt.sangfor.com.

3.8.5.2 Data Backup

The **Data Backup** page consists of the **Syslog Server Backup** and **Policies Backup and Restore** areas.

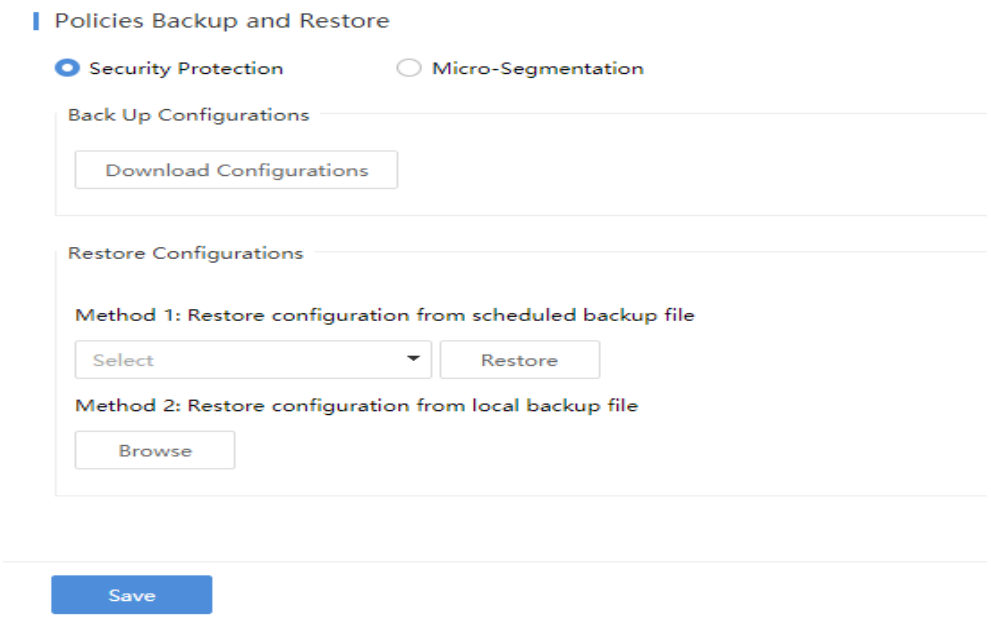
Syslog Server Backup

In the **Syslog Server Backup** area, you can select **Enable syslog server** to send security logs on the Endpoint Secure Manager to the syslog server using the syslog protocol for unified analysis, as shown in the following figure.



Policies Backup and Restore

In the **Policies Backup and Restore** area, you can back up security protection and micro-segmentation configurations. Select the configurations to be backed up and click **Download Configurations** to export the backup data.



Configurations can be restored from a scheduled backup file or local backup file.

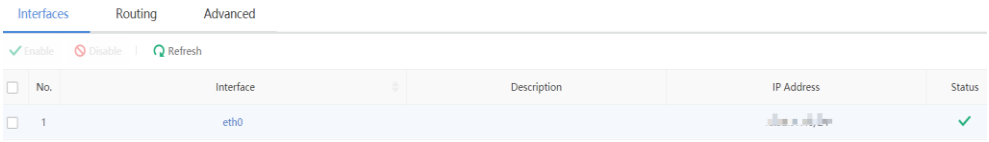
- To restore configurations from a scheduled backup file, select the scheduled backup file, click **Restore**, and then wait until restoration is complete.
- To restore configurations from a local backup file, click **Browse**, select the local backup file, and wait until restoration is complete.

3.8.5.3 Network

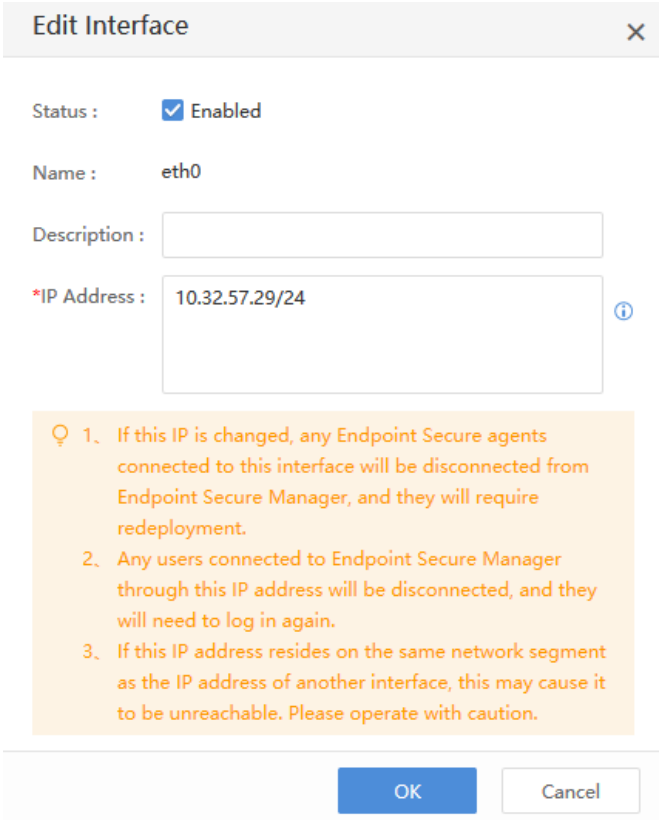
The **Network** page consists of the **Interfaces**, **Routing**, and **Advanced** tabs.

1. **Interfaces**

On the **Interfaces** tab, you can configure IP addresses for network interfaces that are used for communication between the Endpoint Secure Manager and internal endpoints. Endpoints can also use the IP addresses to access the Endpoint Secure Manager. The following figure shows the **Interfaces** tab.



To configure the IP address for a network interface, click the network interface name and enter the IP address in the **Edit Network Interface** dialog box, as shown in the following figure.



WARNING

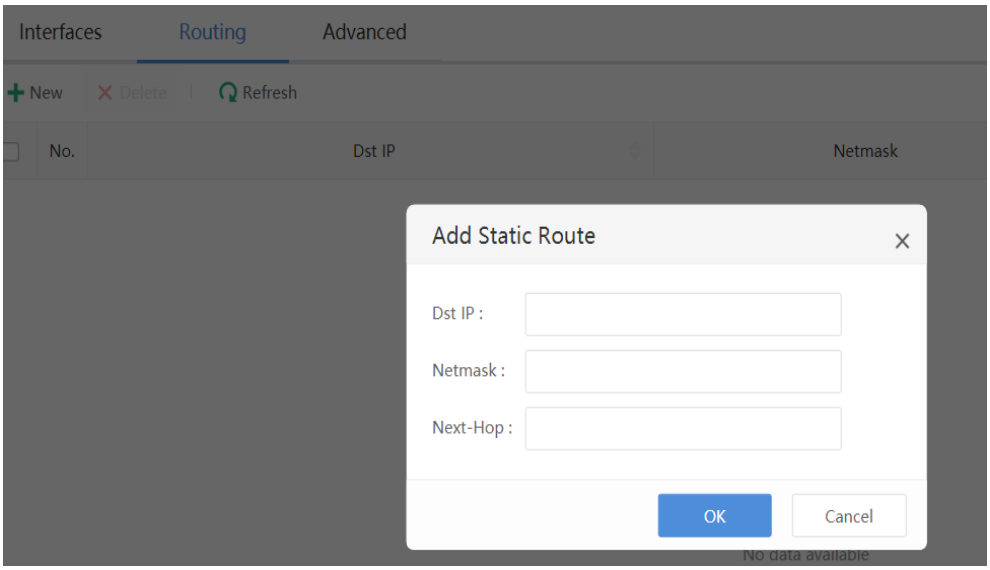
After the IP address is changed, deployed endpoints will be disconnected from the Endpoint Secure Manager and need to be re-deployed. Therefore, exercise caution when you change the IP address.

The **Routing** and **Advanced** tabs are displayed if the Endpoint Secure Manager is installed in ISO or OVA image mode. They are not displayed if the Endpoint Secure Manager is installed in script mode.

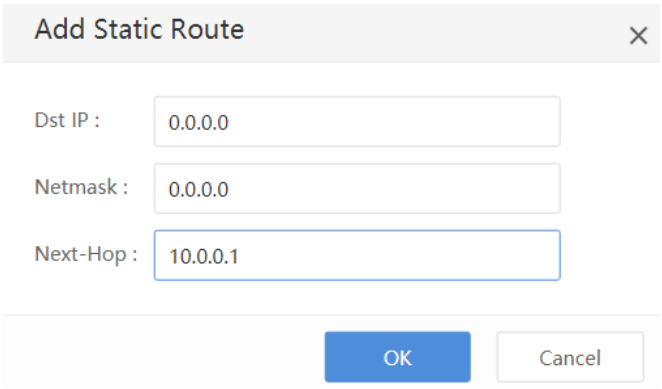
2. **Routing**

The Endpoint Secure Manager needs to connect to and communicate with

endpoints. Therefore, you must configure routes to ensure reachability. To configure a route, choose **System** > **System** > **Network** and click the **Routing** tab, as shown in the following figure.

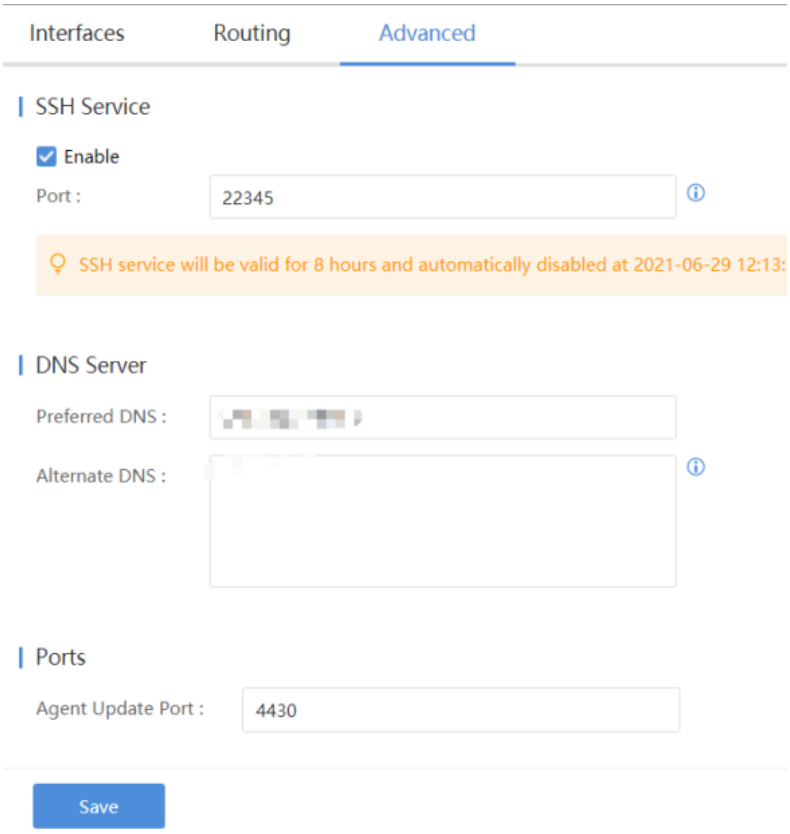


Click **New** and specify the route information.



3. Advanced

The **Advanced** tab consists of the **SSH Service**, **DNS Server**, and **Ports** areas. To go to the **Advanced** tab, choose **System** > **System** > **Network** and click the **Advanced** tab, as shown in the following figure.



The parameters are as follows:

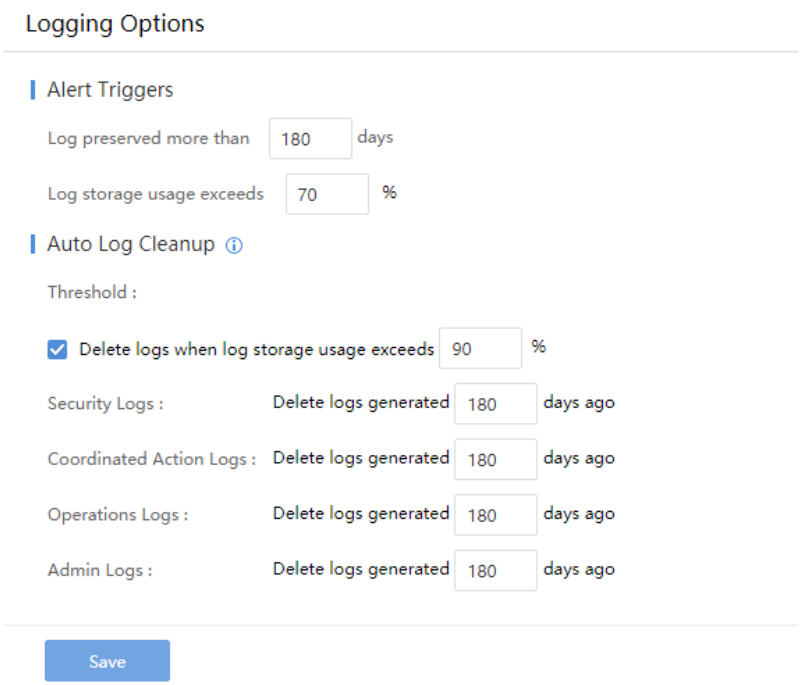
- **SSH Service**: In this area, you can enable or disable the SSH port and change the SSH port of the Endpoint Secure Manager backend. The default port is 22345.
- **DNS Server**: In this area, you can set the DNS server addresses of the Endpoint Secure Manager for domain name resolution when the Endpoint Secure Manager connects to the Internet to update the antivirus database.
- **Ports**: In this area, you can configure the port used to access the Endpoint Secure Manager and the port used for Agent updates.

3.8.5.4 Logging Options

On the **Logging Options** page, you can set the mechanism for automatic log cleanup. Logs that can be automatically deleted include security logs, coordinated action logs, operation logs, and admin logs. You can set the maximum preservation time for logs before they are automatically deleted to 7 to 1095 days. By default, automatic log cleanup is enabled. You can set the expected number of log preservation days and log storage usage for triggering

alerts in the **Alert Triggers** area.

The following figure shows the **Logging Options** page.



Description:

1. When the log storage usage exceeds 70%, a banner notification will be displayed.
2. When the log storage usage exceeds the threshold for deleting logs, logs are automatically deleted. Security logs include logs of Anti-Malware, Vulnerability Scan, Integrity Check, Intrusion Detection (WebShell Detection, Brute-Force Attack Protection, and Fileless Attack), Server Protection, External Access Control, and Suspicious Login.

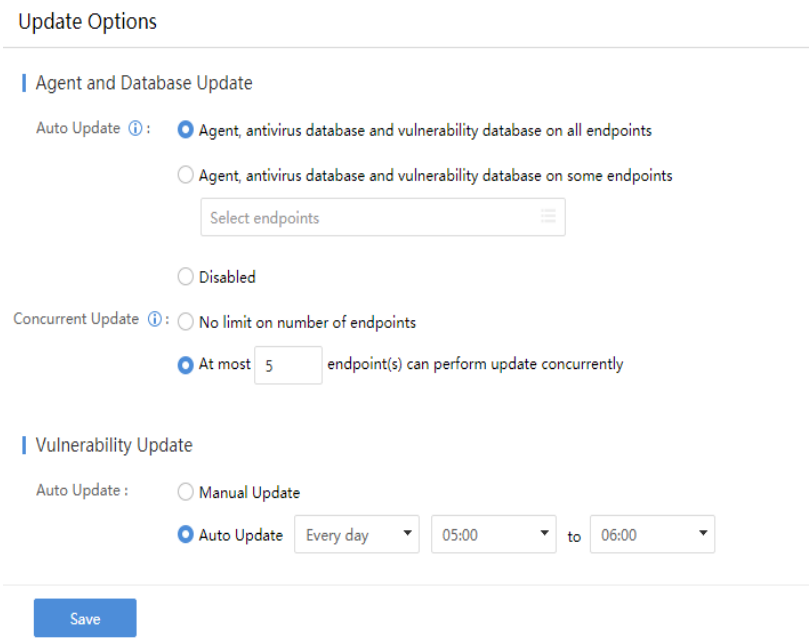
3.8.5.5 Update Options

The Endpoint Secure Manager supports canary updates and staggered updates of the Endpoint Secure Manager and the antivirus and vulnerability databases.

1. Canary update: When Agents on some servers need to be updated, only one Agent is updated first. Other Agents are updated only after it is confirmed that the first updated Agent is normal.
2. Staggered update: To prevent network congestion due to simultaneous

updates of a large number of Agents, you can set the maximum number of endpoints that are concurrently updated to reduce the impact of the update on the network bandwidth.

The following figure shows the **Update Options** page.



Agent and Database Update: Set the endpoint update method and the maximum number of concurrently updated endpoints.

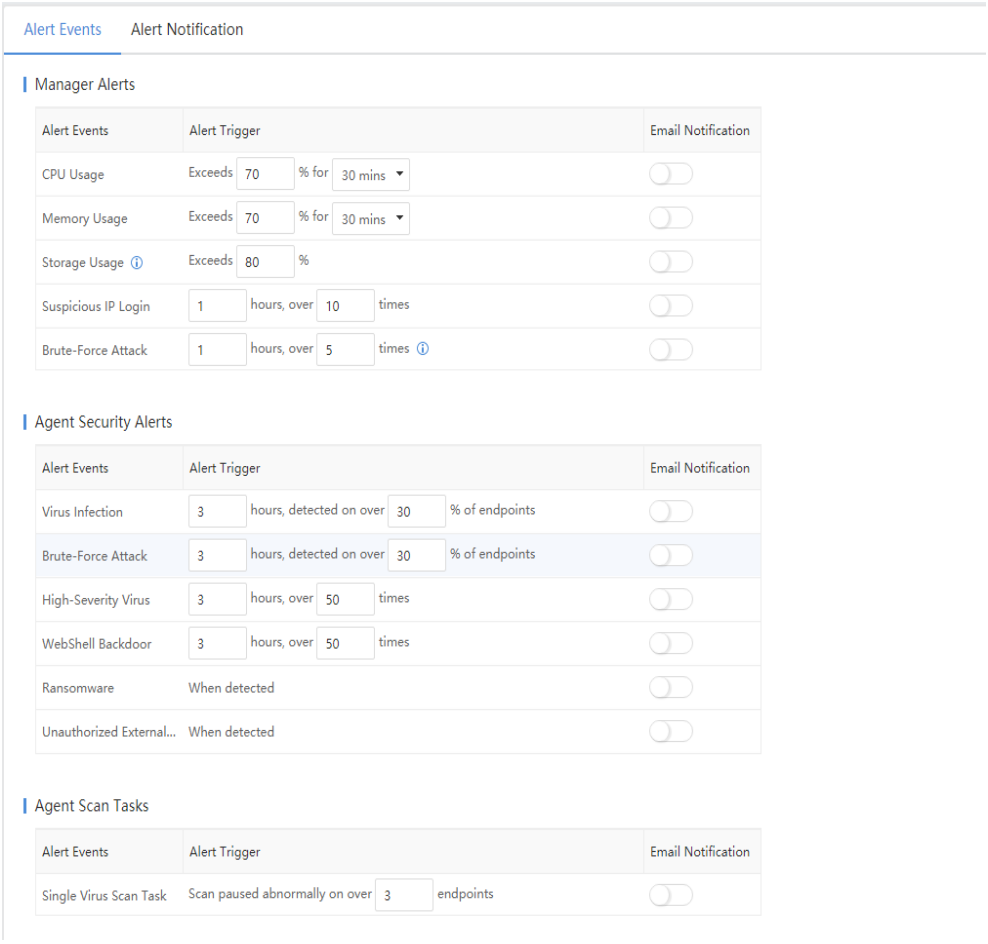
- **Auto Update**: that is, canary update. Select endpoints to be updated.
- **Concurrent Update**: that is, staggered update. Set the maximum number of endpoints that are concurrently updated to reduce the update's impact on the network bandwidth.

Vulnerability Update: Set the automatic update time of the vulnerability database. After auto-update is enabled, the Endpoint Secure Manager automatically updates the vulnerability database at the specified time.

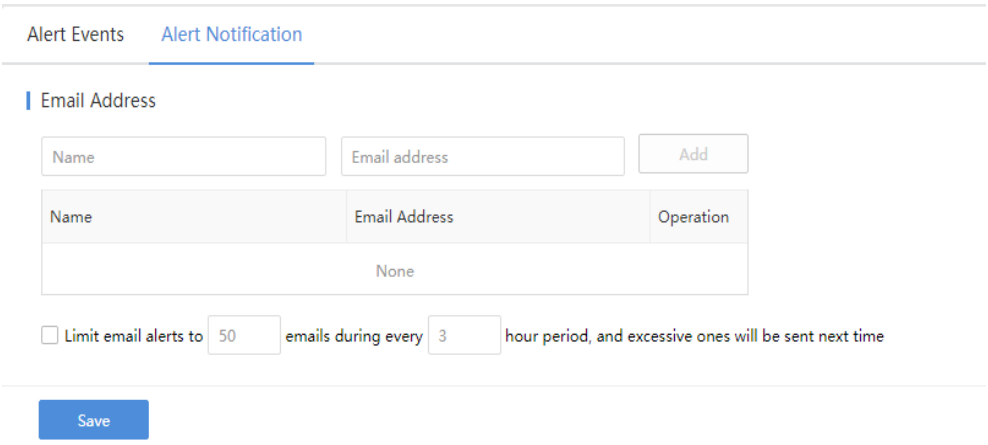
3.8.5.6 Alert Options

The Endpoint Secure Manager can detect the CPU, memory, and hard disk usage. When the usage within the specified time exceeds the threshold, the Endpoint Secure Manager sends an email to the administrator for the administrator to master the Endpoint Secure status and network security in time.

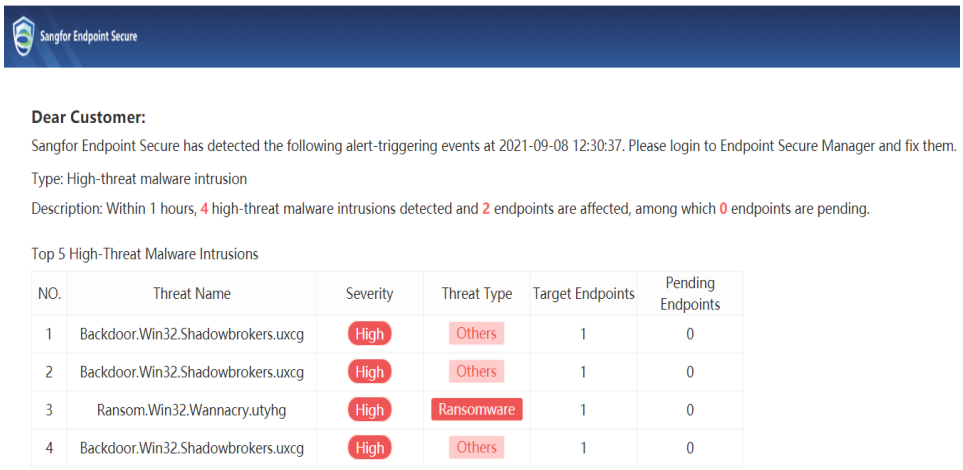
The **Alert Options** page consists of the **Alert Events** and **Alert Notification** tabs. The following figure shows the **Alert Events** tab.



The following figure shows the **Alert Notification** tab.



When an alert event occurs, the administrator will receive an alert email, as shown in the following figure.


Sangfor Endpoint Secure

Dear Customer:

Sangfor Endpoint Secure has detected the following alert-triggering events at 2021-09-08 12:30:37. Please login to Endpoint Secure Manager and fix them.

Type: High-threat malware intrusion

Description: Within 1 hours, 4 high-threat malware intrusions detected and 2 endpoints are affected, among which 0 endpoints are pending.

Top 5 High-Threat Malware Intrusions

NO.	Threat Name	Severity	Threat Type	Target Endpoints	Pending Endpoints
1	Backdoor.Win32.Shadowbrokers.uxcg	High	Others	1	0
2	Backdoor.Win32.Shadowbrokers.uxcg	High	Others	1	0
3	Ransom.Win32.Wannacry.utyhg	High	Ransomware	1	0
4	Backdoor.Win32.Shadowbrokers.uxcg	High	Others	1	0

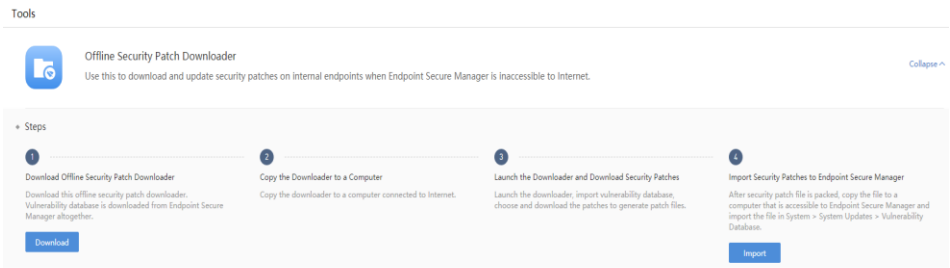
NOTE

To send alert emails, you must first configure the SMTP server on the **General** page.

3.8.5.7 Tools

The **Tools** page provides the Offline Security Patch Downloader, which is used together with the Endpoint Secure Manager's vulnerability scan and patching function. Suppose the Endpoint Secure Manager and all its managed endpoints are not accessible to the Internet. In that case, you can use this tool to download the security patches and import them to the Endpoint Secure Manager to patch endpoint vulnerabilities.

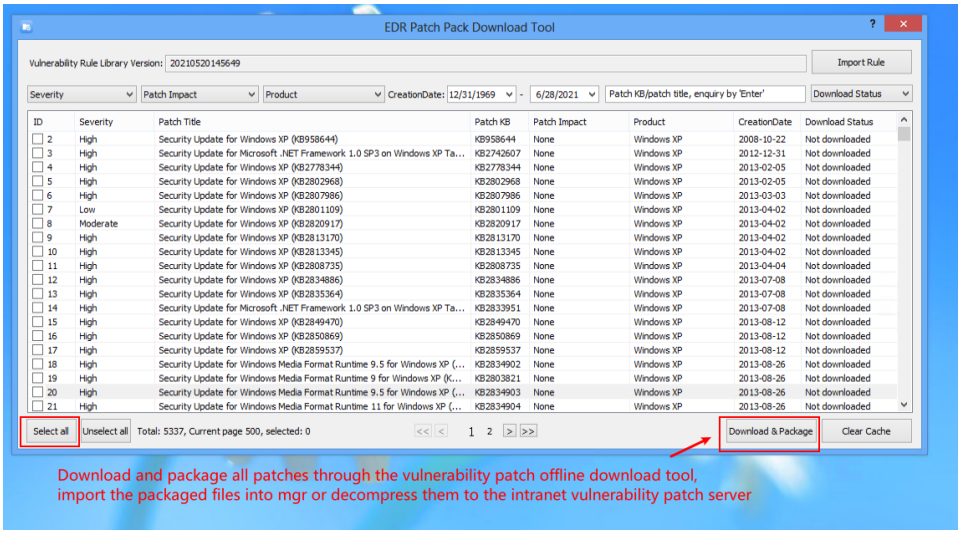
The following figure shows the **Tools** page.



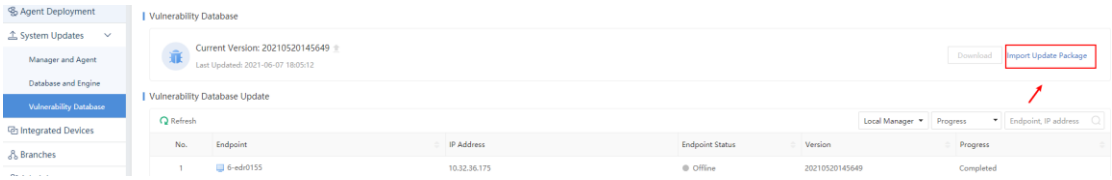
Tool Use

Step 1. Download Offline Security Patch Downloader from the **Tools** page and copy the Downloader to a PC accessible to the Internet.

Step 2. Start the Downloader and download security patches, as shown in the following figure.



Step 3. Import the security patches to the Endpoint Secure Manager, as shown in the following figure.



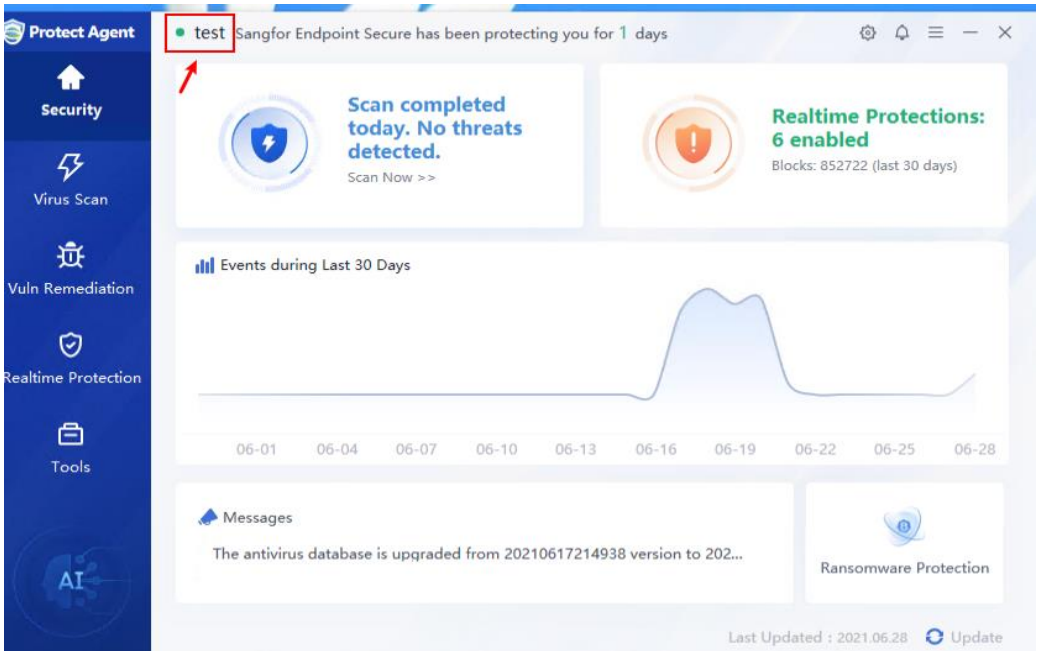
Step 4. Scan and patch endpoint vulnerabilities.

4 Agent

Endpoint users can use the Agent to scan for viruses, view security logs and quarantined or trusted files, and customize settings. Endpoint users can also right-click the Agent icon minimized to the system tray and perform shortcut operations.

4.1 Home Page

After the Agent is deployed, you can view the endpoint protection duration, last scan time, and real-time protection trend on the home page, as shown in the following figure.



4.2 Security

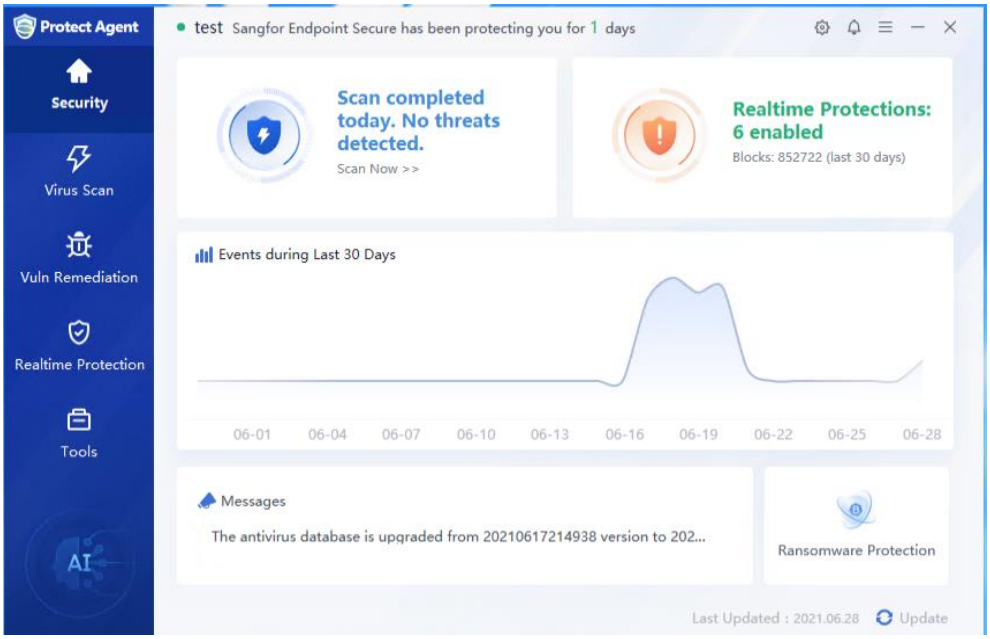
On the **Security** page, the endpoint protection duration and the connection status between the Agent and the Endpoint Secure Manager are on the top.

- If in the upper left corner is green, the Agent properly connects to the Endpoint Secure Manager.
- If the icon is gray, the connection between the Agent and the Endpoint Secure Manager is abnormal.

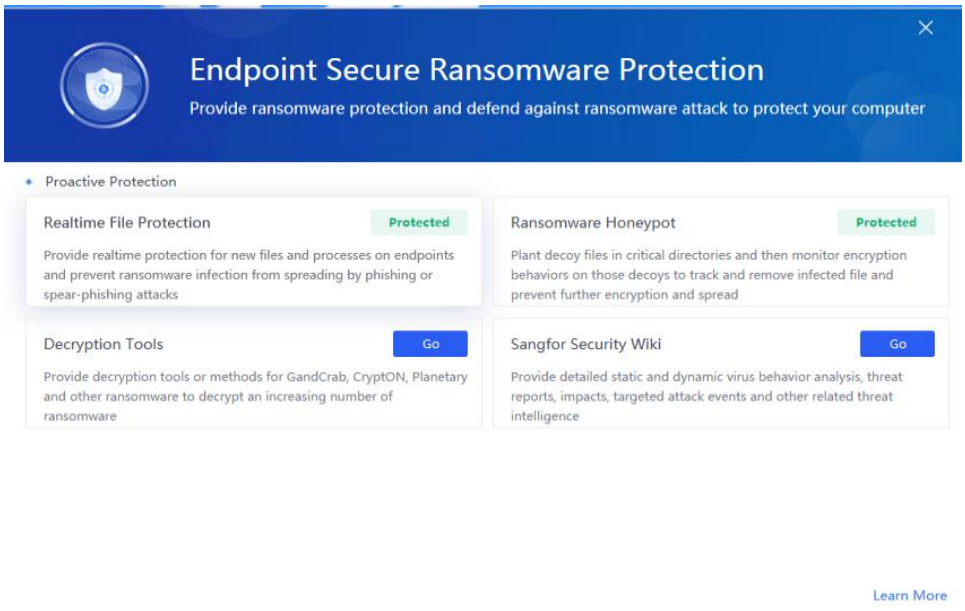
The **Security** page provides quick entrances to **Anti-Malware** and **Realtime**

Protection and displays the protection trend in the last 30 days.

The **Notification** area displays the latest messages, such as antivirus database version update, software version update, and notifications sent by the administrator.

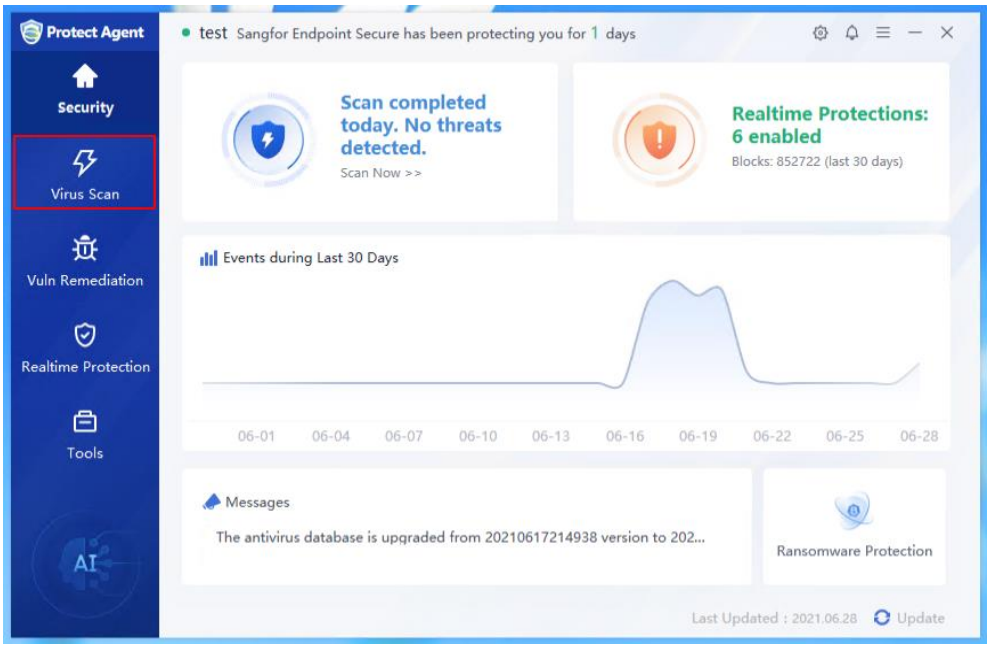


in the lower right corner displays the ransomware protection mechanisms in the prevention, protection, detection, and response phases, as shown in the following figure.



4.3 Anti-Malware

On the **Anti-Malware** page, you can perform a quick scan, full scan, or custom scan for the endpoint and view scan logs.



Quick Scan: Scan critical Windows system directories, for example, **/windows**, **/windows/system32**, and **/windows/system32/drivers** and its subdirectories.

Full Scan: Scan all Windows system directories.

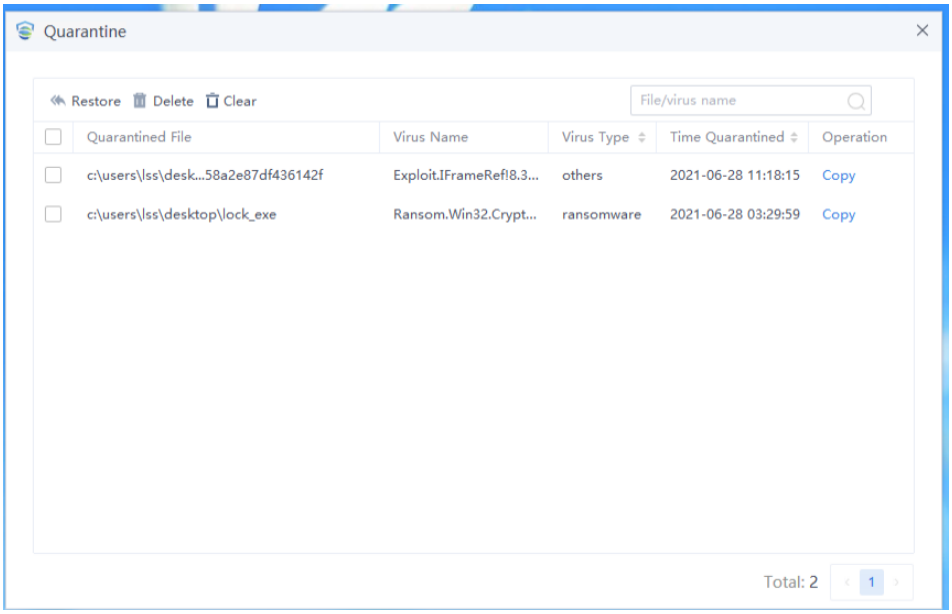
Custom Scan: Scan specified files or directories.

In the lower-left corner of the **Anti-Malware** page, you can view the scan engines. A blue icon indicates that an engine is enabled, and a gray icon indicates that an engine is disabled. You can move the cursor to the engine icon to view detailed engine information.

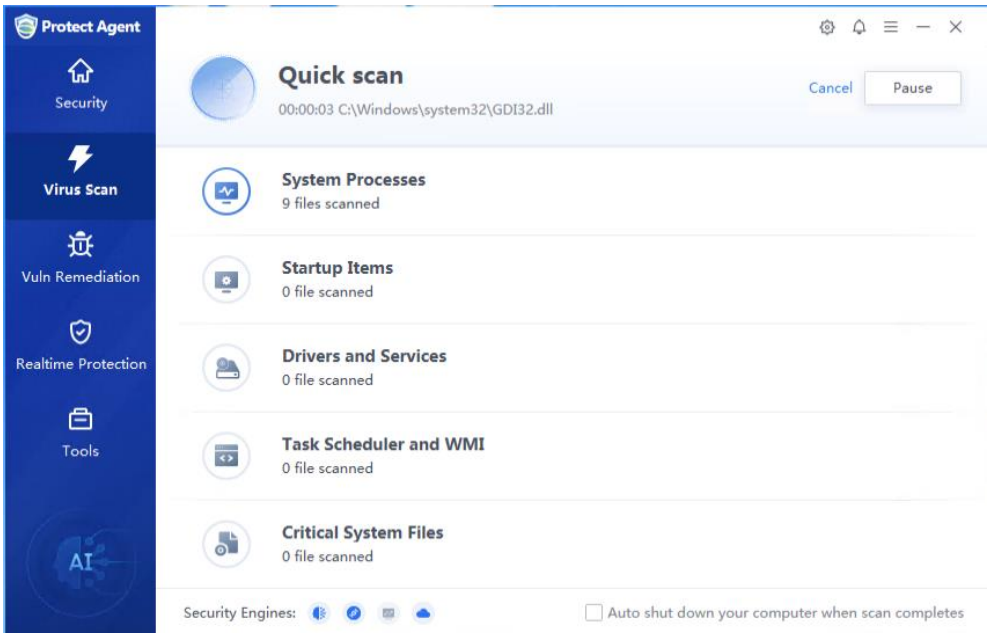
Icon	Engine	Description
	Sangfor Engine Zero	It is a Sangfor-developed AI engine proficient in ransomware scan and removal, auto-learning, and identification of various virus variants. It helps improve the capability to detect unknown viruses.
	Gene Analysis Engine	It is a traditional virus scan and removal engine and is good at locating viruses with family features.

	Behavioral Analysis Engine	It uses virtual execution to find viruses and is good at identifying new unknown virus variants.
	Cloud-Based Engine	It owns abundant antivirus databases and can correlate with other engines for virus scan and removal. It has a powerful virus identification capability.

You can view quarantined and trusted files and virus scan logs in the lower right corner of the **Anti-Malware** page. You can click **Quarantine**, and then restore, delete, or clear quarantined files with one click, as shown in the following figure.

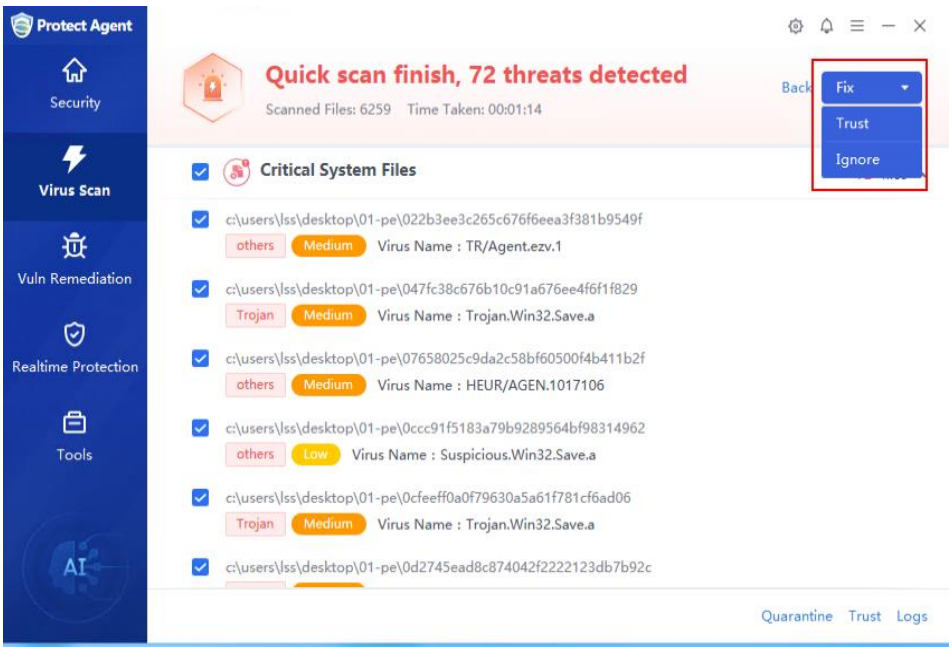


For example, click **Quick Scan** to trigger scanning of critical system directories, as shown in the following figure.



If you enable a virus scan before the end of the day and require that the PC automatically shuts down after scanning is complete, select **Auto shut down your computer when scan completes** in the lower right corner.

For malicious files found during the virus scan, you can fix, trust, or ignore these malicious files and view the file details, as shown in the following figure.



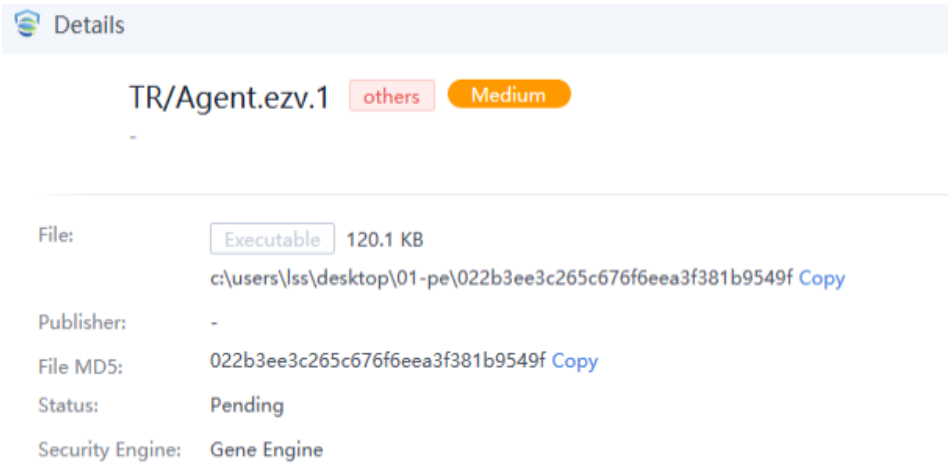
Fix: Quarantine found malicious files. For a macro virus or infectious malicious files, the ES agent will try to fix them first. Quarantined files can be

viewed in the **Quarantine** area.

Trust: Define false-positive malicious files as trusted after manual analysis. Trusted files can be viewed in the **Trust** area.

Ignore: Ignore the file check result.

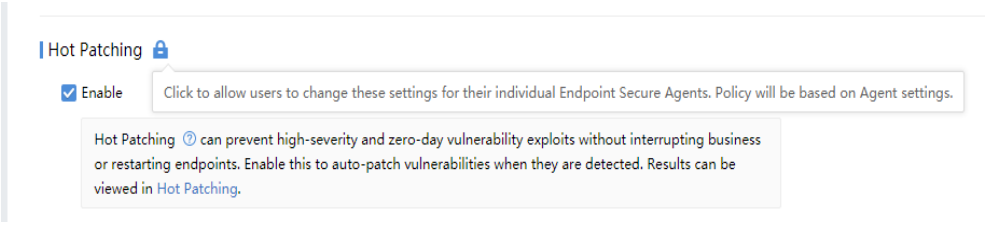
Details: View detailed information about a malicious file, as shown in the following figure.



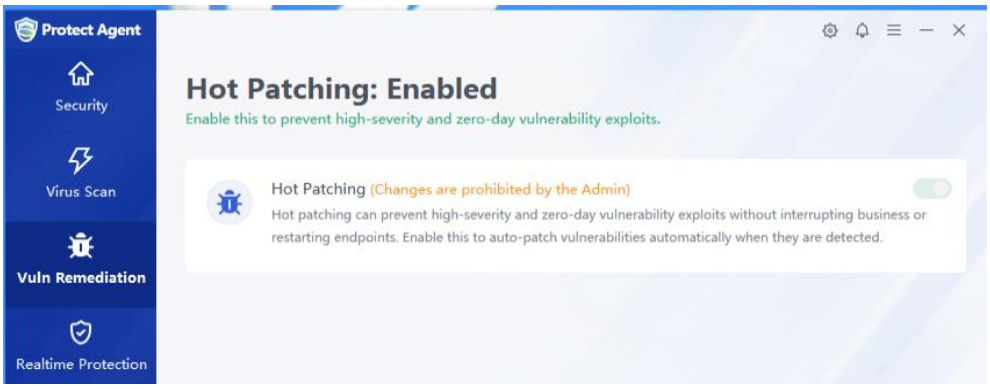
4.4 Vulnerability Scan

Suppose you enable and lock **Hot Patching** on the **Vuln Remediation** tab under **Endpoints > Security Protection** on the Endpoint Secure Manager. In that case, hot patching is enabled on the Agent by default, as shown in the following figure.

Display on the Endpoint Secure Manager.

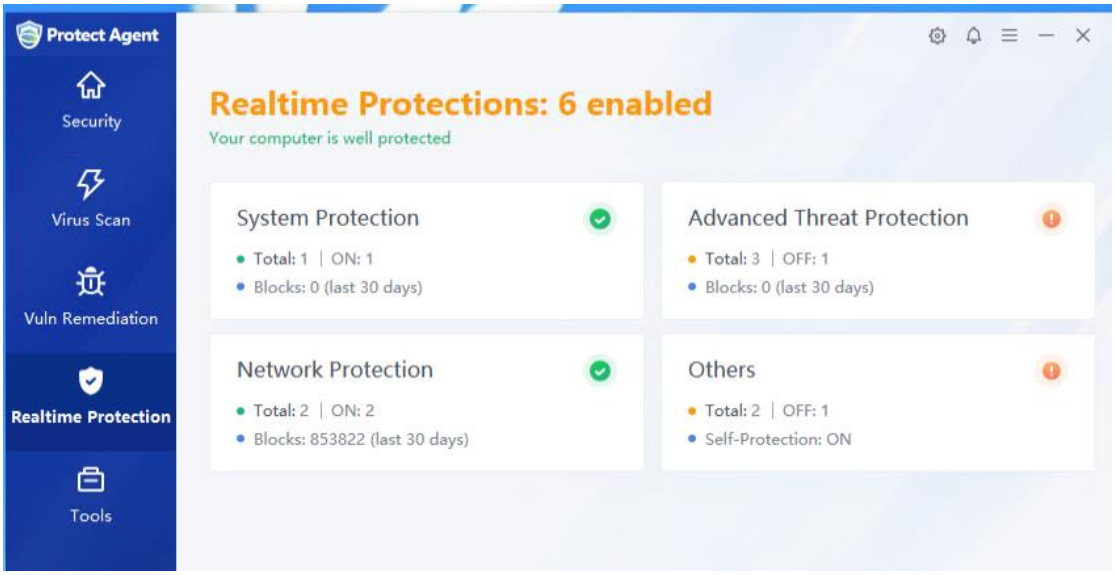


Display on the Endpoint Secure Agent.

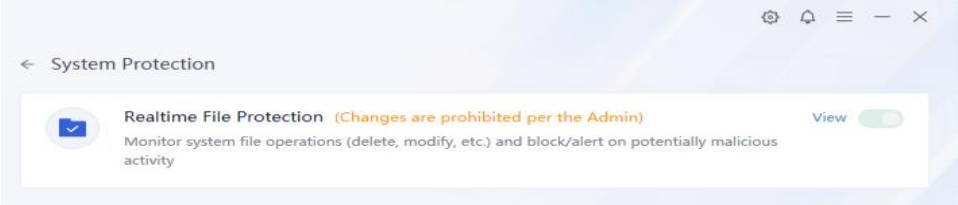


4.5 Realtime Protection

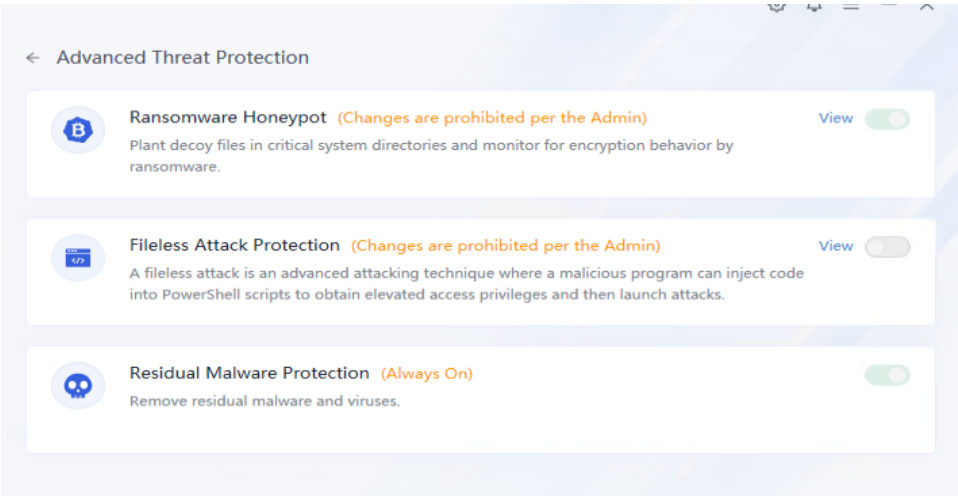
Realtime protection provides the following types of protection: System Protection, Advanced Threat Protection, Network Protection, and Others. The **Realtime Protection** page displays the statuses of different protection types, as shown in the following figure.



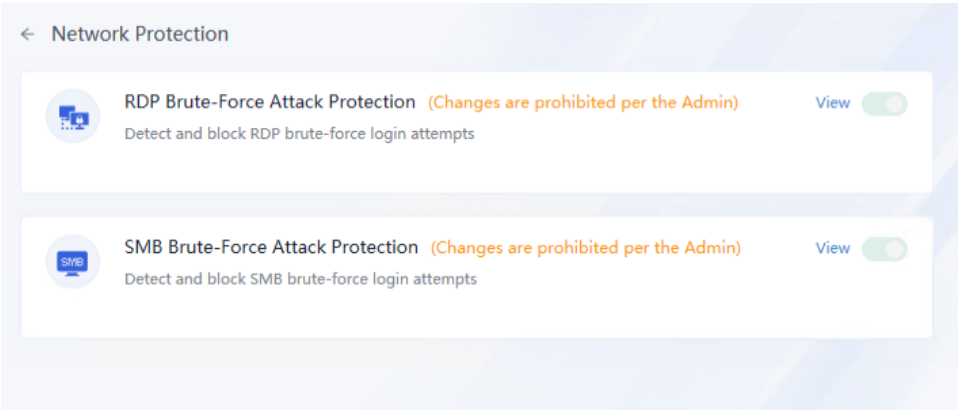
Click **System Protection** to go to the **System Protection** page, where **Realtime File Protection** is provided. The administrator can revoke the configuration permissions from endpoint users. Suppose the administrator does not allow endpoint users to modify the configurations. In that case, the "Changes are prohibited by the admin" message is displayed on the Agent, as shown in the following figure.



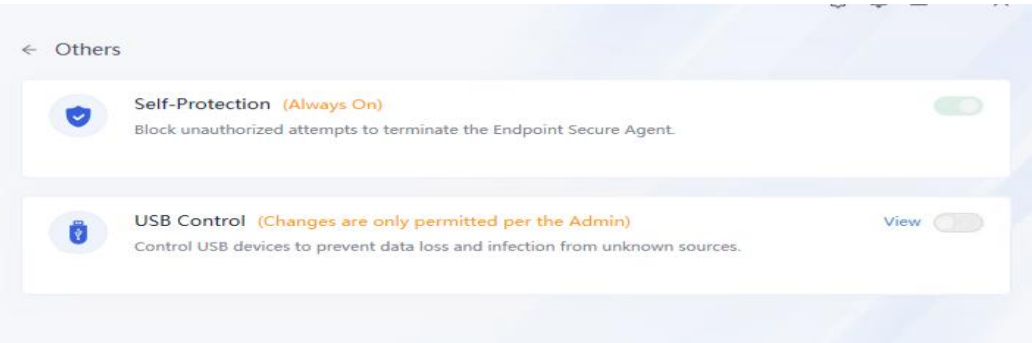
Click **Advanced Threat Protection** to go to the **Advanced Threat Protection** page, where **Ransomware Honeypot**, **Fileless Attack Protection**, and **Residual Malware Protection** are provided, as shown in the following figure.



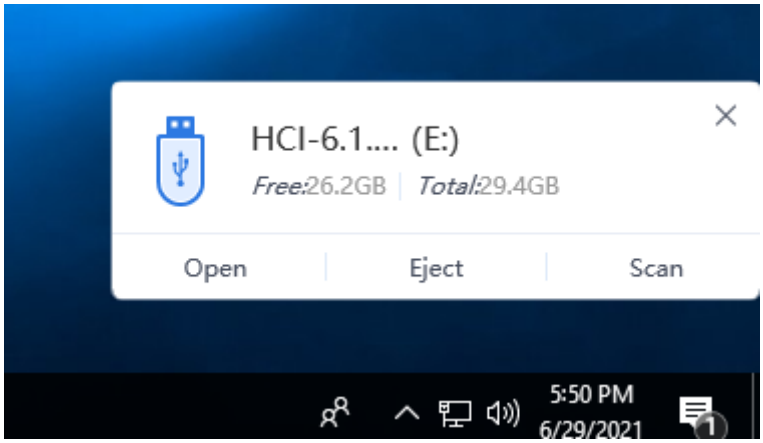
Click **Network Protection** to go to the **Network Protection** page, where **RDP Brute-Force Attack Protection** and **SMB Brute-Force Attack Protection** are provided, as shown in the following figure.



Click **Others** to go to the **Others** page, where **Self-Protection** and **USB Control** are provided, as shown in the following figure.



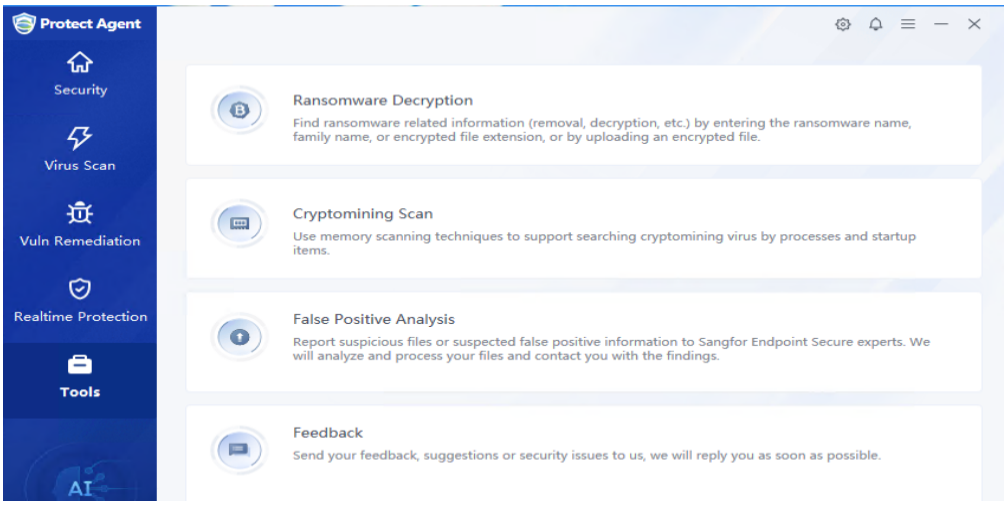
USB Control is enabled by default. When a USB flash drive is inserted into the endpoint, a shortcut menu is displayed in the lower right corner. You can open, remove, or perform a virus scan for the USB flash drive, as shown in the following figure.



If you click **Eject**, the inserted USB flash drive automatically exits.

4.6 Tools

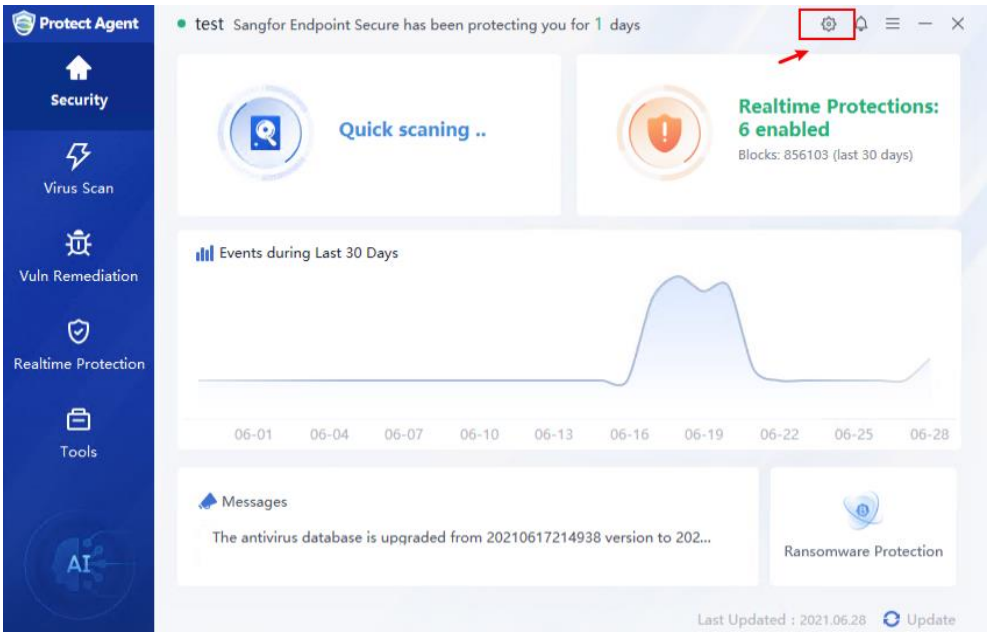
The **Tools** page consists of the **Ransomware Decryption**, **Cryptomining Scan**, **False Positive Analysis**, and **Feedback** parts.



Ransomware Decryption: When the server is attacked by ransomware, you can query ransomware information and whether decryption is available using the ransomware decryption tool based on ransomware features, such as the encrypted file extension and ransom information.

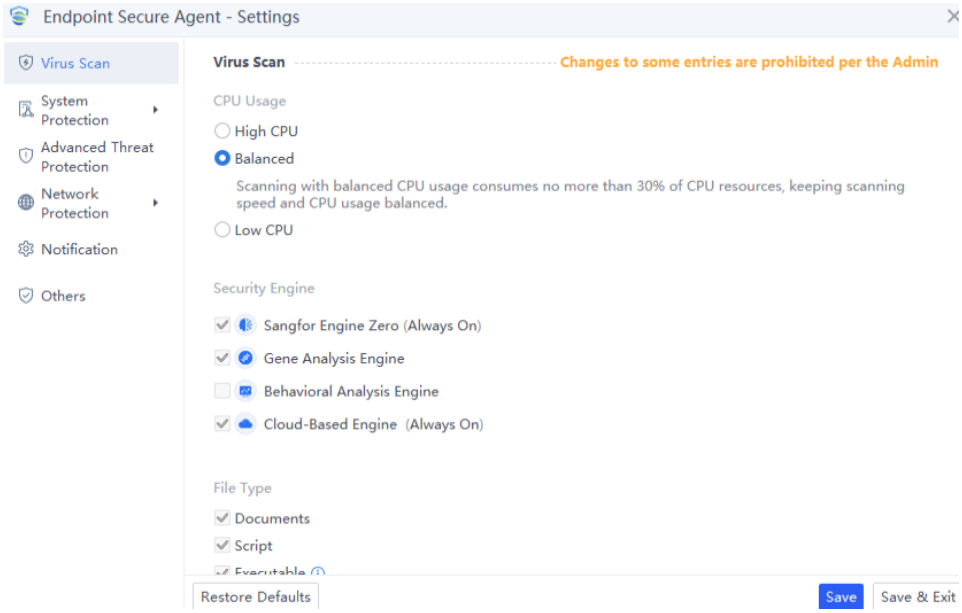
4.7 Endpoint Secure Agent - Settings

Click in the upper right corner of the Agent to go to the **Endpoint Secure Agent - Settings** page, as shown in the following figure.



The **Endpoint Secure Agent - Settings** module consists of the **Virus Scan**, **System Protection**, **Advanced Threat Protection**, **Network Protection**, and **Notification** nodes. Each function has corresponding configuration items on

the Endpoint Secure Manager. The administrator can revoke the configuration permissions from endpoint users. In the **Security Protection** module of the Endpoint Secure Manager, a lock icon is displayed next to each policy. When the lock icon next to a policy is on, the administrator does not allow endpoint users to configure the policy. The "Changes are prohibited by the admin" message is displayed on the Agent, as shown in the following figure.



Virus Scan: On the **Virus Scan** page, you can configure the scan mode, scan engine, scan options, and action to take.

Scan modes include **High CPU**, **Balanced**, and **Low CPU**.

- **High CPU**: Scan is performed at full speed, and the CPU usage of the scanning is not limited.
- **Balanced**: A balance is reached between the scan speed and CPU usage, and the CPU usage cannot exceed 30%.
- **Low CPU**: Less CPU resources are occupied during scanning, and the CPU usage cannot exceed 10%.

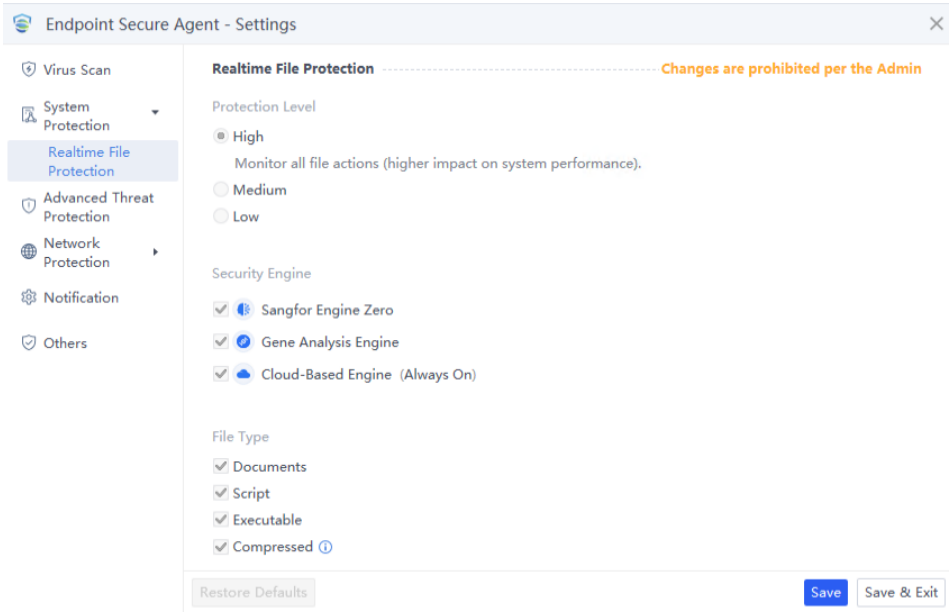
Scan Options: Set the maximum size and a maximum number of compression layers of a file to scan. The scan software can scan compressed files up to 10 layers deep.

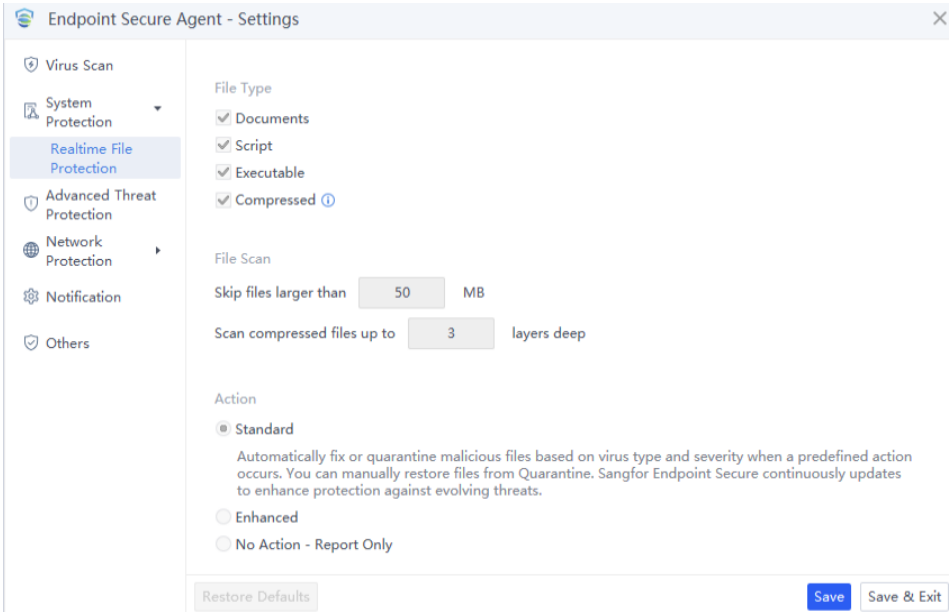
Action: When malicious files are found, the actions that can be performed include **Standard**, **Enhanced**, and **No Action - Report Only**.

- **Standard**: Quarantine malicious files in the blacklist and report detection logs for threat files not in the blacklist. **Standard** is selected by default.
- **Enhanced**: Quarantine all detected threat files. This option is suitable for strict protection scenarios.
- **No Action - Report Only**: Report security logs for all threat files without quarantining the files. This option is suitable for scenarios in which an on-duty security professional is responsible for fixing threats.

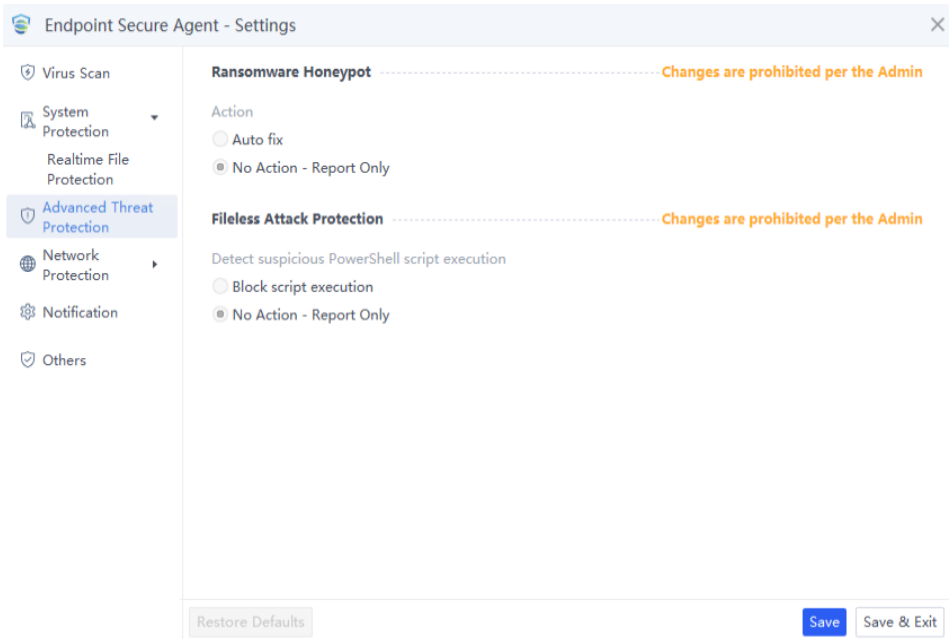
Click **Save** to save the page configurations and switch to other pages for configuration.

Click **Save & Exit** to save the page configurations and close the **Endpoint Secure Agent - Settings** page.

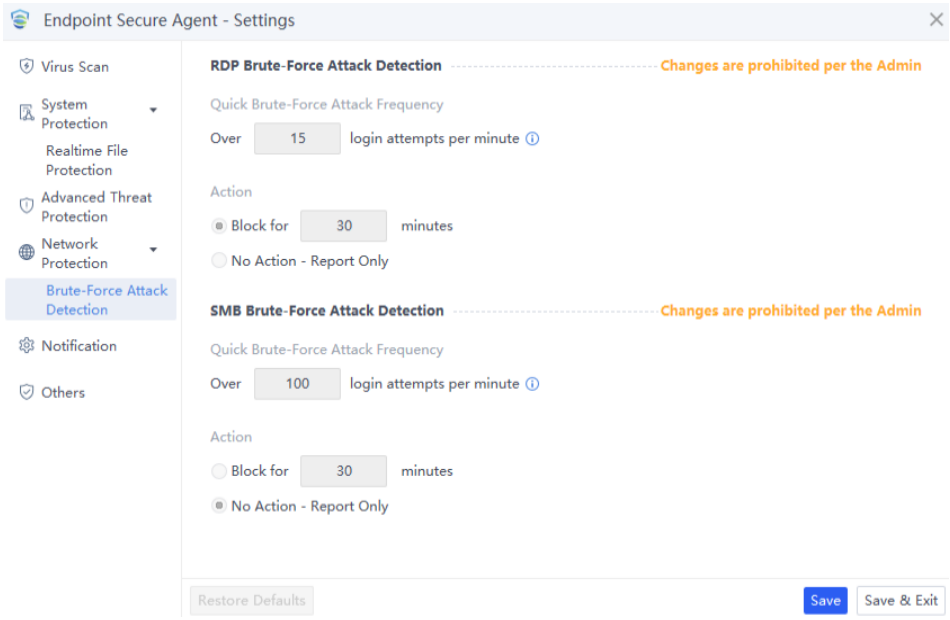




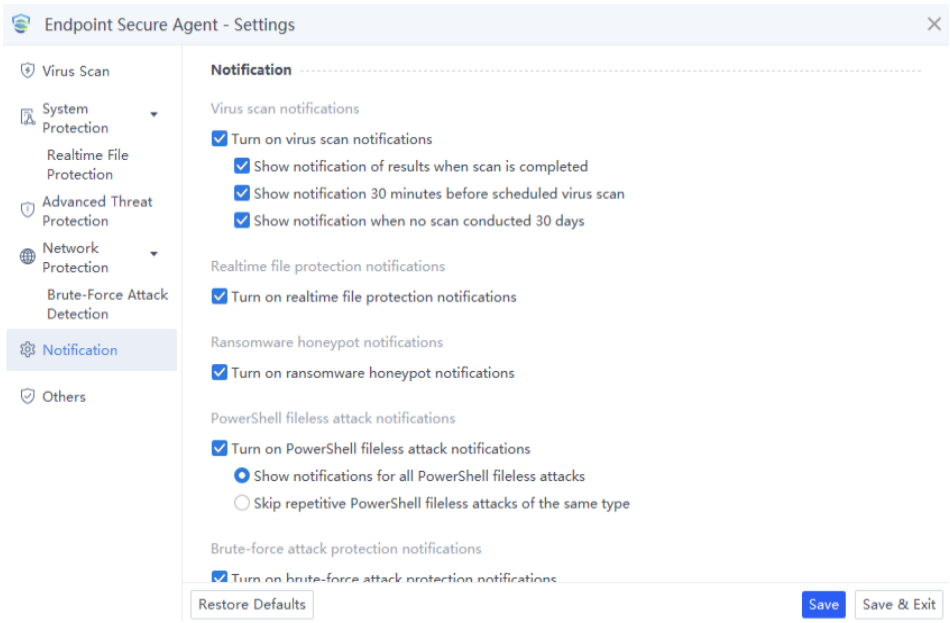
System Protection: On the **System Protection** page, you can set the protection level, scan engine, file type, scan options, and action for real-time file protection. The parameter settings are the same as those in the **Realtime File Protection** area on the **Realtime Protection** tab under **Endpoints** > **Security Protection** on the Endpoint Secure Manager. For details, see Realtime Protection.



Advanced Threat Protection: You can configure **Ransomware Protection** and **Fileless Attack Protection**. The parameter settings are the same as those in the **Ransomware Protection** and **Fileless Attack Protection** areas on the **Realtime Protection** tab page under **Endpoints** > **Security Protection** on the Endpoint Secure Manager. For details, see Realtime Protection.



Network Protection: You can configure **RDP Brute-Force Attack Protection** and **SMB Brute-Force Attack Protection**. The parameter settings are the same as those in the **Brute-Force Attack Protection** area on the **Realtime Protection** tab page under **Endpoints** > **Security Protection** on the Endpoint Secure Manager. For details, see Realtime Protection.

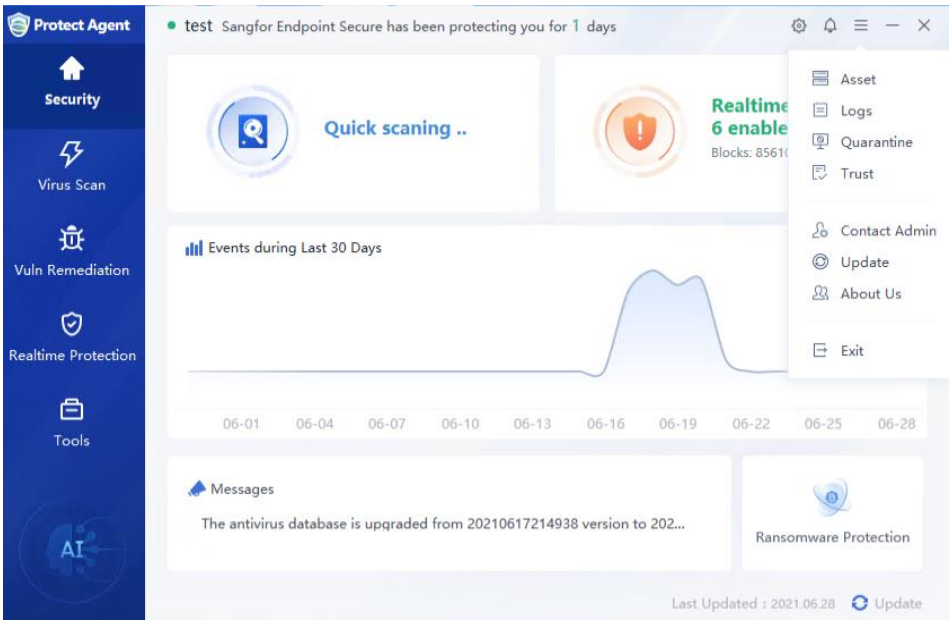


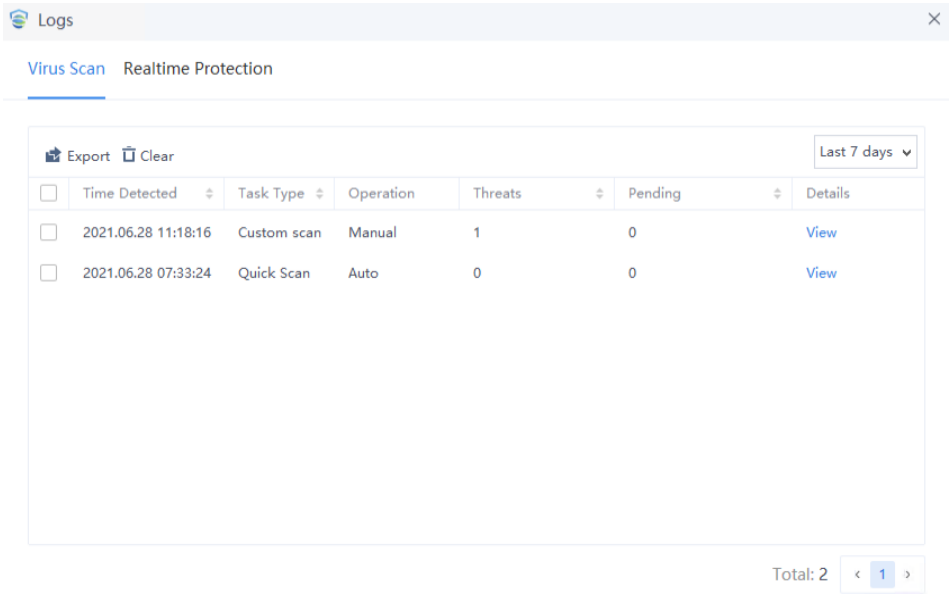
Notification Settings: You can configure the virus scan notification and alert notifications for real-time file protection, ransomware protection, and fileless attack protection. You can determine whether to enable a notification based on actual requirements. If the administrator has disabled notifications on the Endpoint Secure Manager or **Do Not Disturb** is enabled on the Agent, the

options on this page are dimmed and cannot be modified.

4.8 Security Logs

Click ☰ in the upper right corner of the Agent and choose **Security Logs** to open the **Security Logs** page, as shown in the following figure.



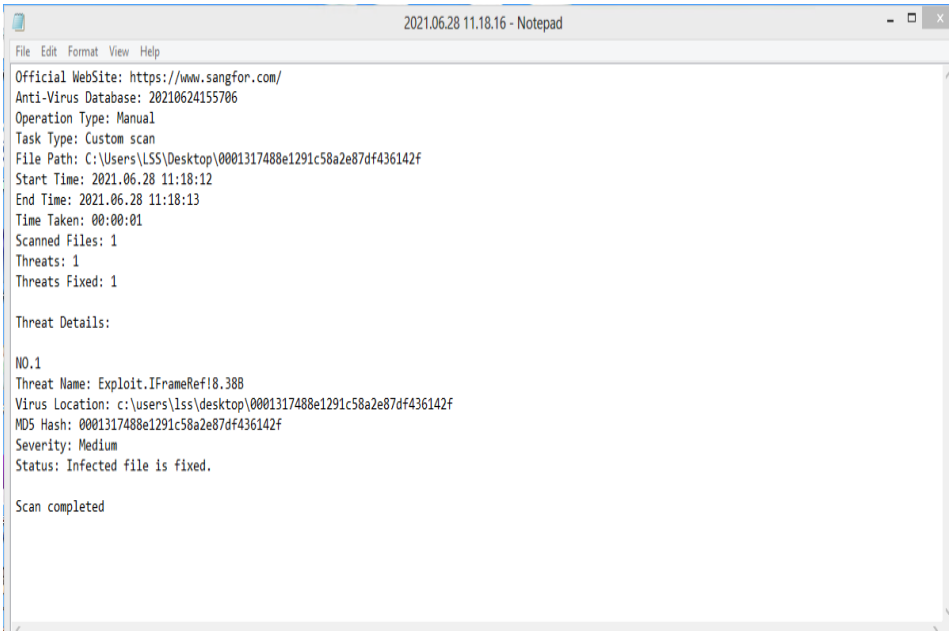


Security logs include real-time protection logs and anti-malware logs.

Realtime protection logs are security logs generated for detected malicious files after real-time file protection is enabled.

Anti-malware logs are operation logs about virus scans. You can click **Details** to

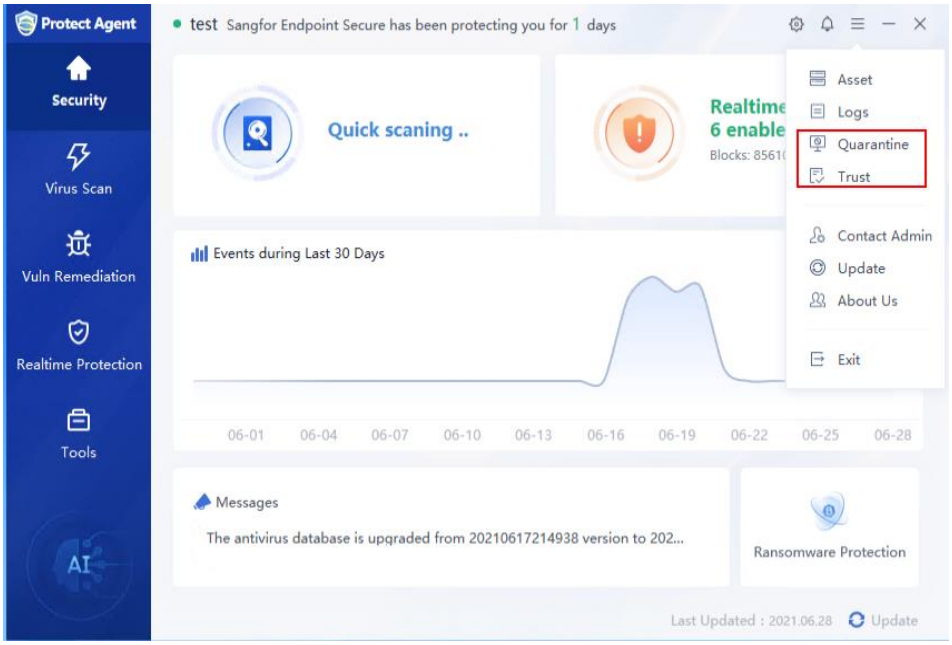
view the anti-malware details, as shown in the following figure.



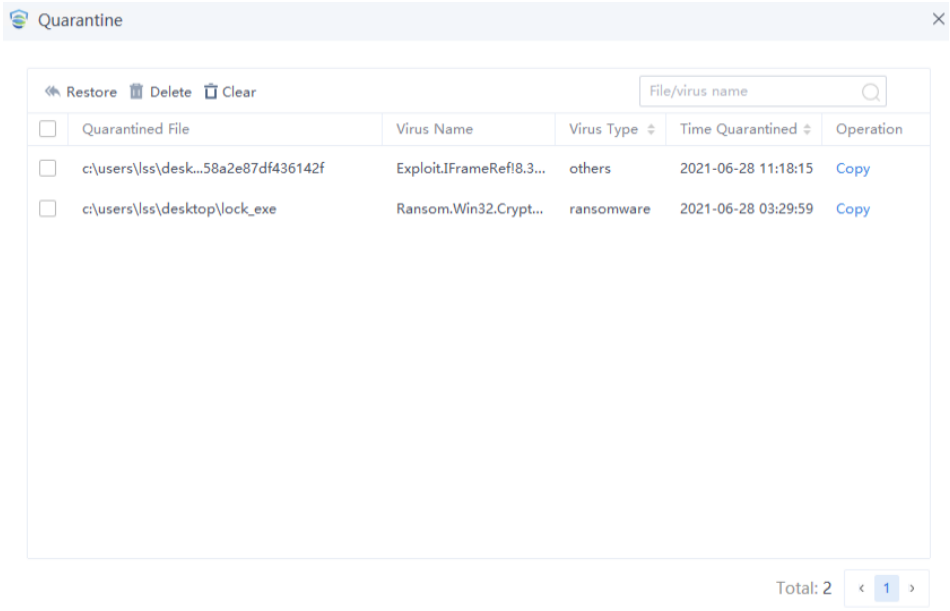
4.9 Quarantine and Trust Areas

When Endpoint Secure isolates detected malicious files, the files are moved to the **Quarantine** area. False-positive files or processes are added to the **Trust** area. Files in the **Trust** area are automatically skipped during virus scans and real-time file protection.

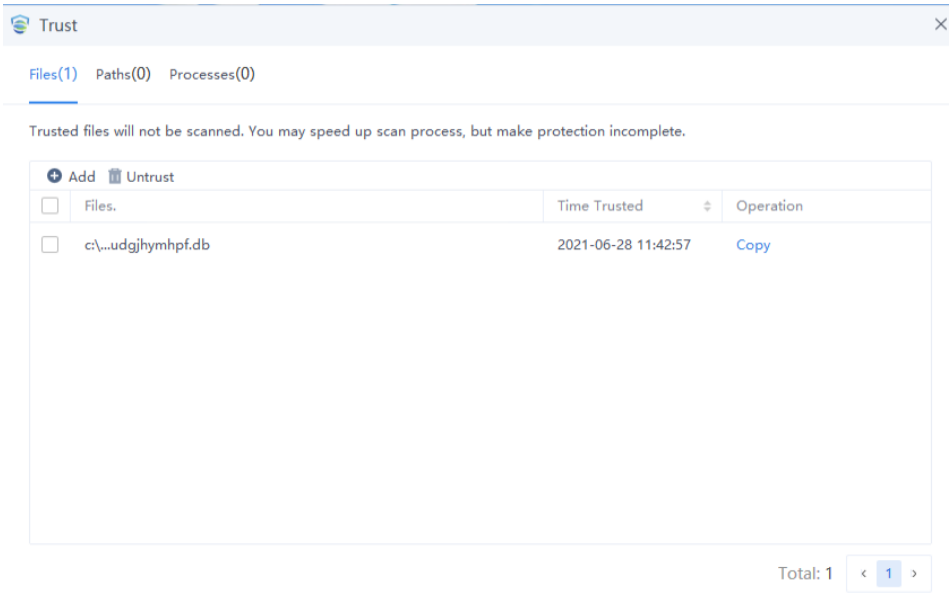
Click ☰ in the upper right corner of the Agent and choose **Quarantine** or **Trust** to open the **Quarantine** or **Trust** page, as shown in the following figure.



You can restore, delete, and clear isolated files on the **Quarantine** page with one click, as shown in the following figure.

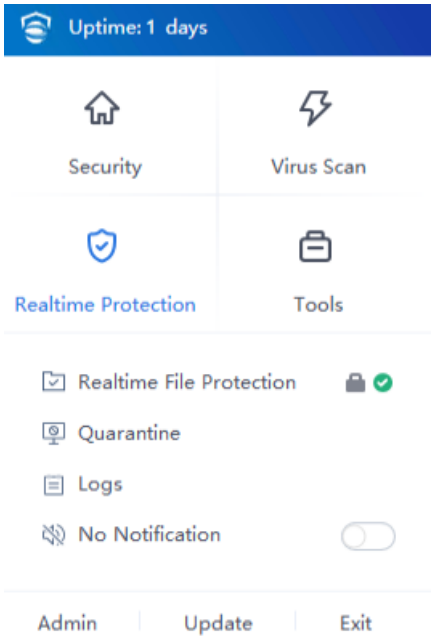


You can add files, directories, and processes as trusted on the **Trust** page, as shown in the following figure.



4.10 System Tray

The Endpoint Secure Agent minimized to the system tray in the lower right corner supports some shortcut operations. When you right-click the Agent icon, the shortcut menu shown in the following figure is displayed.

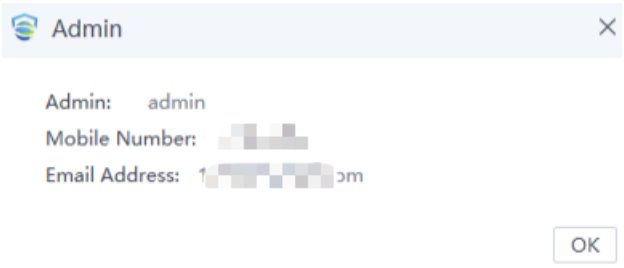


Endpoint Secure has protected your computer for *X* days: shows how long that Endpoint Secure has protected your computer.

Security Center, **Quick Scan**, **Realtime Protection**, **Tools**, **Realtime File Protection**, **Quarantine**, and **Security Logs**: shortcuts provided by Endpoint Secure.

Do Not Disturb: If it is enabled, Endpoint Secure will not alert when malicious files are detected. This function can be configured on the Agent or delivered by the administrator from the Manager.

Administrator: When you click **Administrator**, the administrator information is displayed, as shown in the following figure. If you encounter any issues when using the Endpoint Secure Agent, you can contact the administrator.



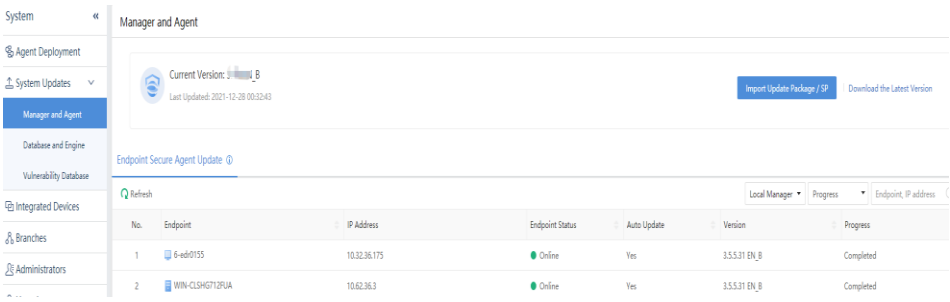
5 Product Update

Endpoint Secure updates include the Manager and Agent update, antivirus database and engine update, vulnerability database and patch package update.

5.1 Manager Update

To update the Manager, perform the following steps:

1. Visit https://community.sangfor.com/plugin.php?id=service:download, download the update package of the corresponding version, and verify the MD5 value.
2. Log in to the Endpoint Secure Manager, choose **System** > **System Updates** > **Manager and Agent**, and click **Import Update Package/SP**, as shown in the following figure.



3. The update takes about 5 minutes and does not require a server restart. After the update is complete, log in to the Manager and check whether the displayed version is the target version. If yes, the update is successful.

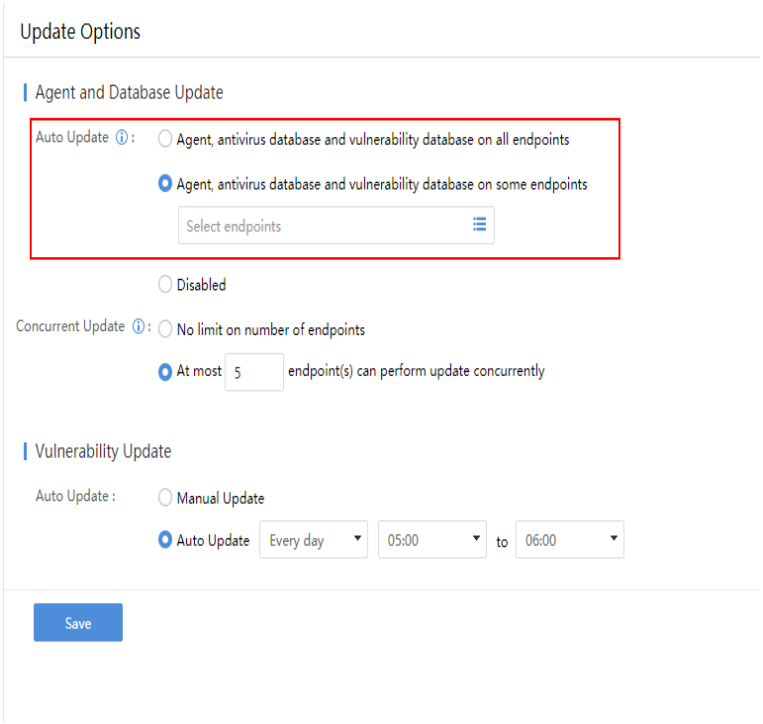
5.2 Agent Update

When the Agent detects that the Manager is updated, the Agent automatically triggers an update. After the update is successful, the update status and version number are displayed in the **Endpoint Secure Agent Update** area on the **Manager and Agent** page under **System** > **System Updates**. To ensure stable and efficient Agent update, you are advised to use both grayscale updates and staggered updates.

5.2.1 Grayscale Update

On the Manager, you can enable auto-update only for some endpoints after the Manager is updated. After these endpoints are successfully updated, select **Agent, antivirus database and vulnerability database on all endpoints** to enable the update for all endpoints. It ensures smooth update and system stability.

To configure canary update, choose **System** > **System** > **Update Options**, select **Agent, antivirus database and vulnerability database on some endpoints** for **Auto Update** in the **Agent and Database Update** area, as shown in the following figure.

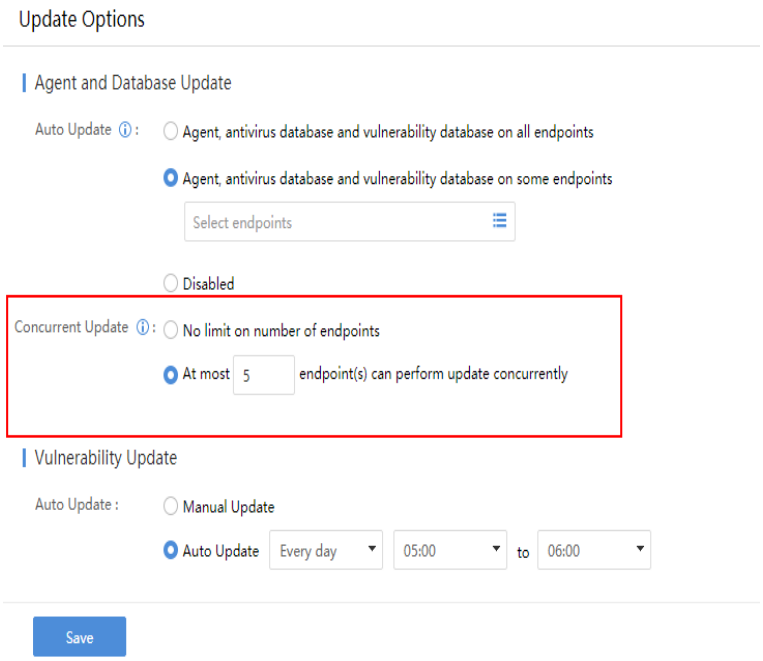


5.2.2 Staggered Update

To prevent network congestion caused by the update of a large number of Agents, set the number of concurrently updated Agents on the Manager. You are advised to set the maximum number of concurrently updated endpoints to 5 or less if the network bandwidth is 100 Mbit/s and 30 or less if the network bandwidth is 1000 Mbit/s.

To configure the number of concurrently updated Agents, choose **System** > **System** > **Update Options**, and set the number of concurrently updated Agents

in the **Concurrent Update** area.



5.3 Antivirus Database and Engine Update

The antivirus database and engine can be updated in automatic online update and manual offline update modes.

5.3.1 Automatic Online Update

By default, the antivirus database and engine are automatically updated online if the Manager can access the Internet.

5.3.2 Manual Offline Update

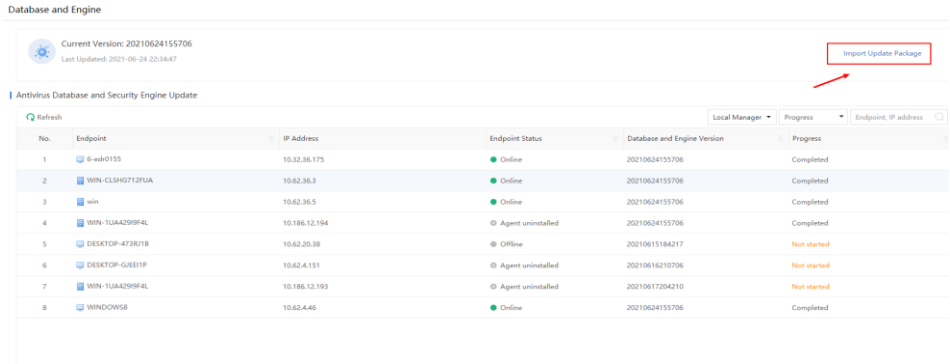
If the Manager is in an isolated network environment, it cannot access the Internet. Therefore, you need to use the manual offline update mode. The update procedure is as follows:

1. Download the offline antivirus database or engine and verify the MD5 value.

   To download the antivirus database, visit https://community.sangfor.com and choose **Self-Service** > **Software Download** > **Endpoint Secure** > **Antivirus Database**.

2. Log in to the Manager, choose **System** > **System Updates** > **Database and**

Engine, click **Import Update Package**, and select the antivirus database or engine downloaded in step 1. After the import is successful, the Agent automatically updates the antivirus database or engine, as shown in the following figure.



5.4 Vulnerability Database and Patch Package Update

The vulnerability database and patch package can be updated in automatic online update and manual offline update modes.

5.4.1 Automatic Online Update

By default, the vulnerability database and patch package are automatically updated online if the Manager can access the Internet.

5.4.2 Manual Offline Update

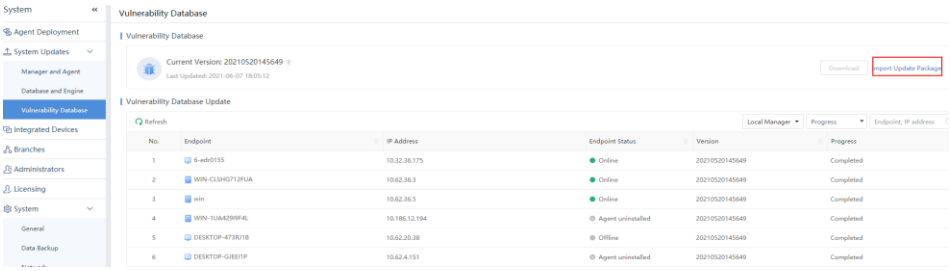
If the Manager is in an isolated network environment, it cannot access the Internet. Therefore, you need to use the manual offline update mode. The update procedure is as follows:

1. Download the vulnerability database or patch package and verify the MD5 value.

   To download the vulnerability database, visit https://community.sangfor.com and choose **Self-Service** > **Software Download** > **Endpoint Secure** > **Vulnerability Database**.

2. Log in to the Manager, choose **System** > **System Updates** > **Vulnerability Database**, click **Import Update Package**, and select the vulnerability

database or patch package downloaded in step 1. After the import is successful, the Agent automatically updates the vulnerability database or patch package, as shown in the following figure.



6 Routine Maintenance

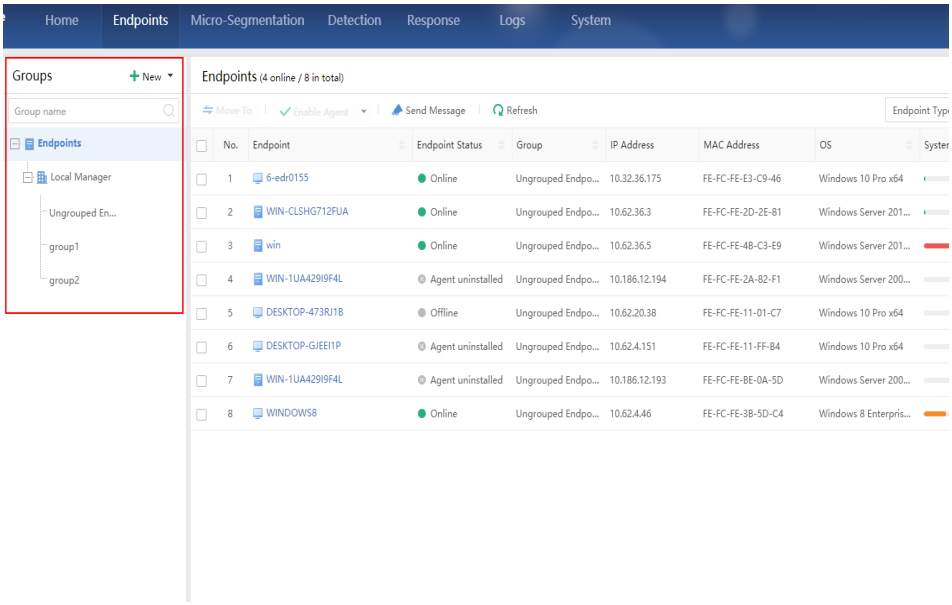
6.1 Endpoints

6.1.1 Groups

In scenarios where multiple departments or branches exist, you are advised to group endpoints by organizational structure. When new endpoints are connected to the Endpoint Secure Manager, the endpoints are automatically grouped based on the IP addresses. In addition, you are advised to set an administrator for each organization or branch. The detailed operations are as follows:

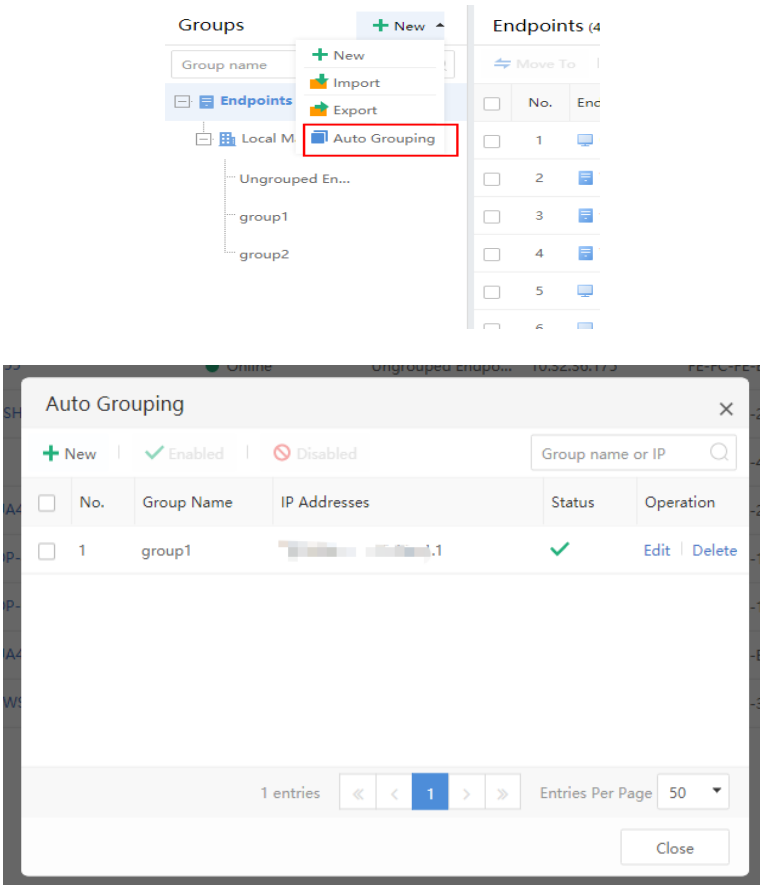
1. **Creating Groups by Organizational Structure**

Choose **Endpoints** > **Groups** and create groups by organizational structure, as shown in the following figure.



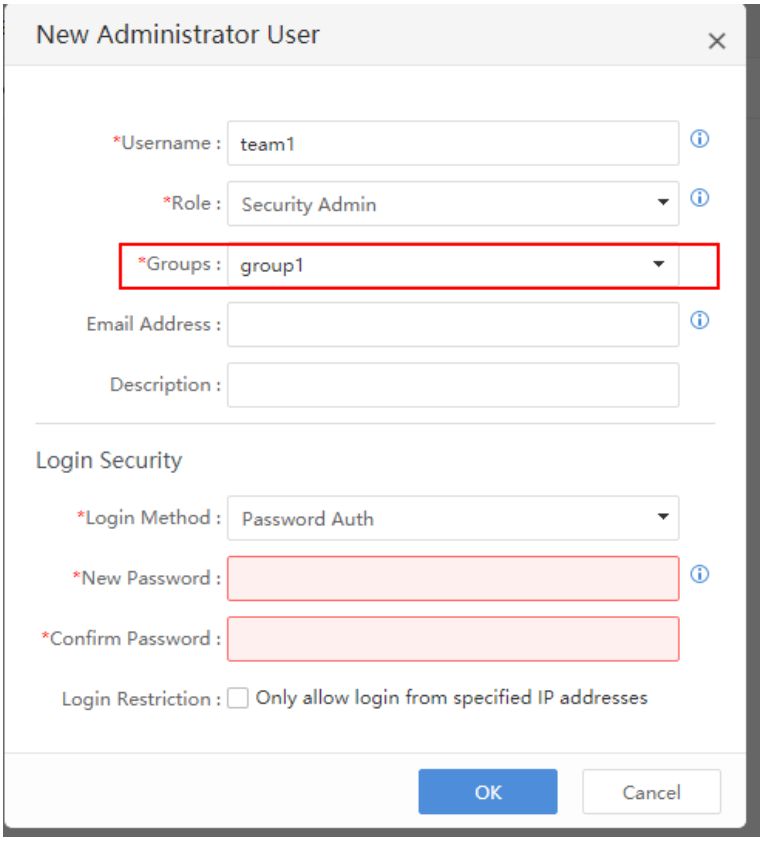
2. **Grouping Endpoints by IP Addresses**

Choose **Endpoints** > **Groups**, click the drop-down list icon next to **New** and choose **Auto Grouping** to open the **Auto Grouping** page, as shown in the following figure. Configure auto grouping of new endpoints by IP addresses.



3. **Setting an Administrator for Each Organization**

Choose **System** > **Administrators** and create an administrator for each organization for independent management, as shown in the following figure.

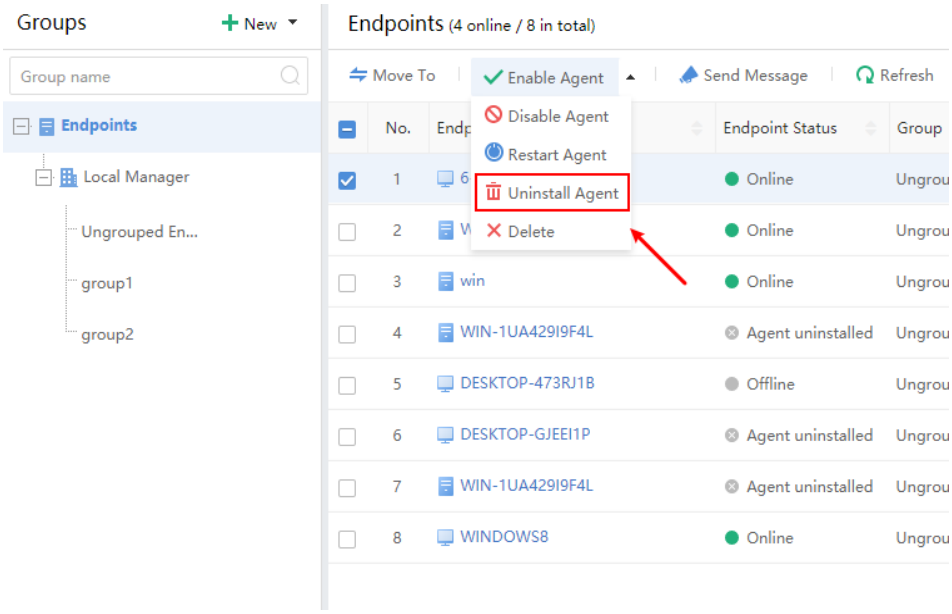


6.2 Licenses

The administrator must periodically delete endpoints offline for a long time or have the Agent uninstalled to release licenses and ensure that there are sufficient licenses for new endpoints connected to the Manager. Licenses can be automatically or manually released.

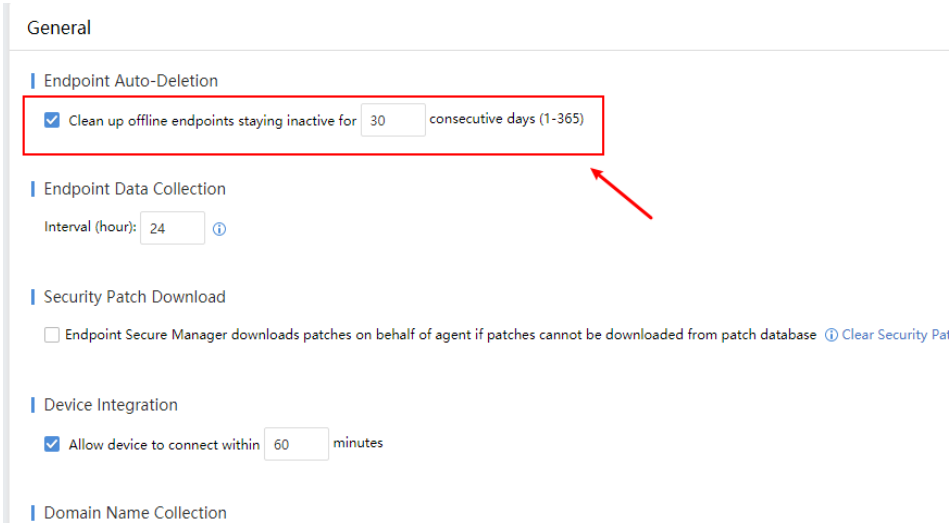
1. **Periodical Manual Release Agent License**

Choose **Endpoints** > **Groups**, select the endpoints that have the Agent uninstalled or are offline for a long time, and delete them to release licenses, as shown in the following figure.



2. Automatic Release

Choose **System** > **System** > **General**, select **Endpoint Auto-Detection**, and set the inactive duration of offline endpoints to be deleted, as shown in the following figure. Offline endpoints whose inactive duration exceeds the set value will be automatically deleted to release licenses.



6.3 Server Protection

The administrator must check security policies periodically to identify security risks and perform server protection. Server protection measures include version and database check, change of the exit and uninstall passwords, Manager account and password management, change of the remote access protection password, Manager login IP address restriction, endpoint security and integrity check, vulnerability scan, and policy optimization.

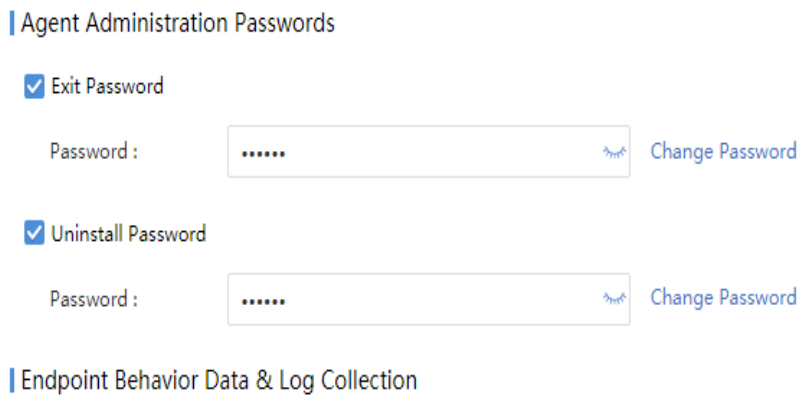
6.3.1 Version and Database Check

The administrator must check the product version and antivirus database version periodically. You are advised to use the latest product version and the latest antivirus database version. To obtain the latest product version and antivirus database version, visit http://bbs.sangfor.com and choose **Self-Service** > **Software Download** > **Endpoint Secure**.

6.3.2 Exit and Uninstall Passwords

The administrator must periodically change the exit and uninstall passwords. The passwords must be strong passwords that contain digits and letters.

To change the exit password or uninstall password, choose **Endpoints** > **Security Protection** > **Basic Config** and set the exit password or uninstall password in the **Agent Administration Passwords** area, as shown in the following figure.



6.3.3 Manager Accounts and Passwords

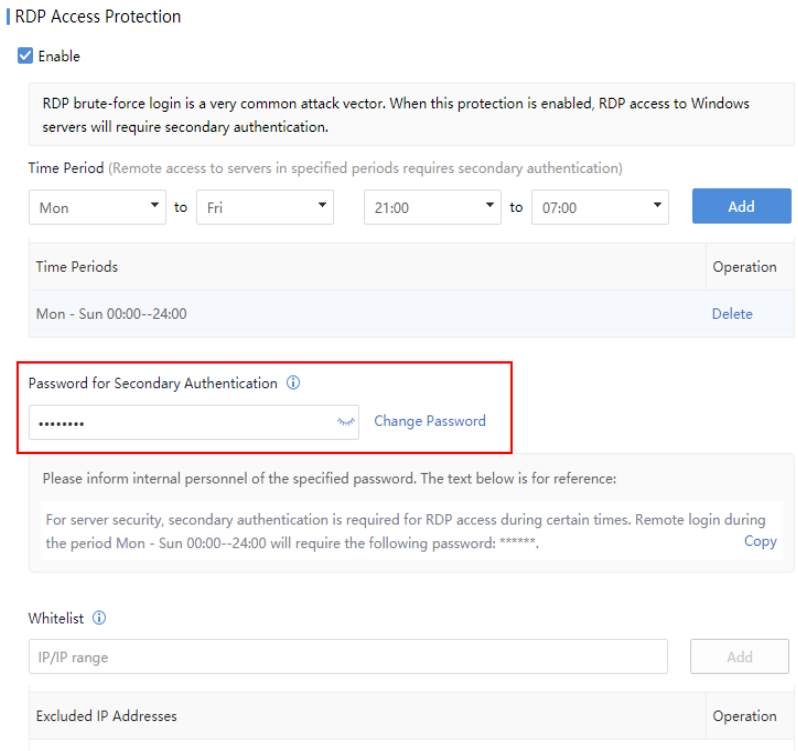
The administrator must periodically check Manager accounts and passwords as follows:

1. Check whether invalid Manager accounts exist. If yes, delete them.
2. Periodically change passwords of Manager accounts and ensure that strong passwords are used.

6.3.4 Remote Access Protection Password

The administrator must periodically change the remote access protection password based on the password complexity requirements.

To change the remote access protection password, choose **Endpoints** > **Security Protection** > **Server Protection** and enter the password in the **Password for Secondary Authentication** text box, as shown in the following figure.

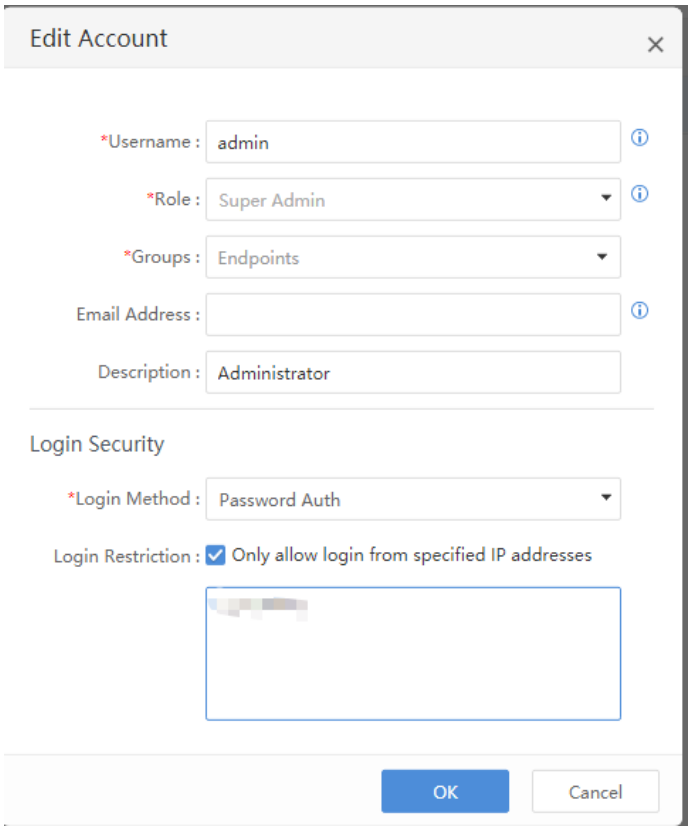


6.3.5 Manager Login IP Address Restriction

You are advised to restrict the IP addresses from which Manager accounts can

log in to the Manager. This way, Manager accounts can log in only through authorized computers.

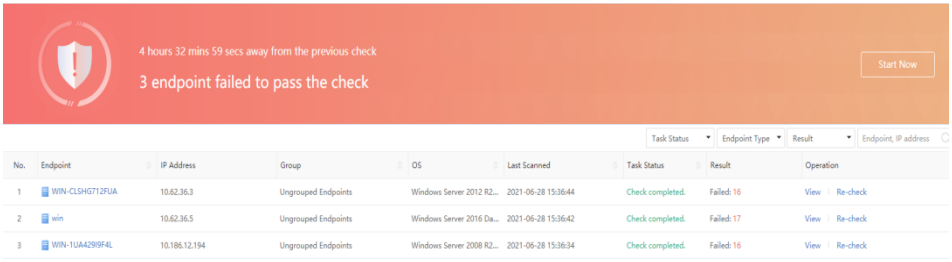
To restrict login IP addresses, choose **System** > **Administrators**, click **Edit** in the **Operation** column of an account, select **Only allow login from specified IP addresses**, and enter the IP addresses, as shown in the following figure.



6.3.6 Security and Integrity Check

The administrator must periodically check security and integrity for internal endpoints and perform protection for check items that do not meet requirements based on the protection guide.

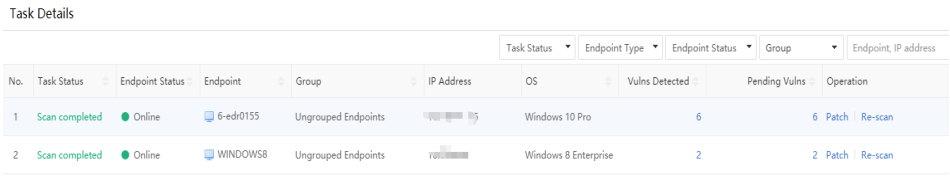
To perform **Security and Integrity Check**, choose **Detection** > **Security & Integrity Check**, as shown in the following figure.



6.3.7 Vulnerability Scan

The administrator must scan internal endpoints for system vulnerabilities and install patches periodically.

To scan internal Windows endpoints for system vulnerabilities and install patches, choose **Detection** > **Vulnerability Scan**, as shown in the following figure.



6.3.8 Policy Optimization

The administrator must check and optimize internal security policies periodically. The following table describes the recommended configurations for different security policies.

Policy	Status	Recommended Configuration
Anti-malware	Enabled by default	Retain the default configuration and enable scheduled scan.
Realtime file protection	Enabled by default	Retain the default configuration.
Brute-force attack protection	Enabled by default	Retain the default configuration.
Ransomware protection	Enabled by default	Retain the default configuration.
WebShell detection	Enabled by default	Retain the default configuration.
Fileless attack protection	Enabled by default	If scripts or programs that run PowerShell commands exist in the internal network, disable fileless attack protection. If not, retain the default configuration.
Trusted server	Enabled as	Configure it as needed.

process protection	needed	
Remote access protection	Enabled by default	Retain the default configuration.
Trusted files	Enabled as needed	Configure it as needed.
Micro-segmentation	Enabled as needed	Configure it as needed.
Alert policy	Enabled as needed	Enable the email alert policy to notify the administrator of threats found in the internal network.

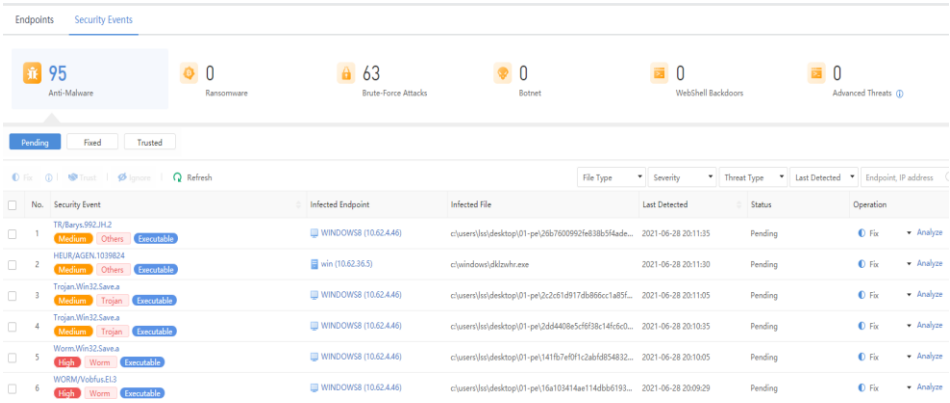
Table 7: Policy optimization

6.4 Security Event Handling

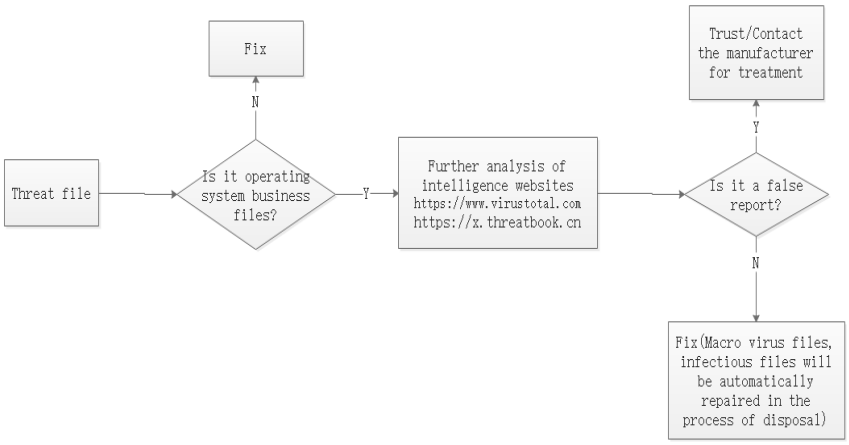
6.4.1 Rules

The administrator must check whether pending security events exist on the Manager and handle them periodically.

To view security events, choose **Response** > **Threat Response** and click the **Security Events** tab, as shown in the following figure.



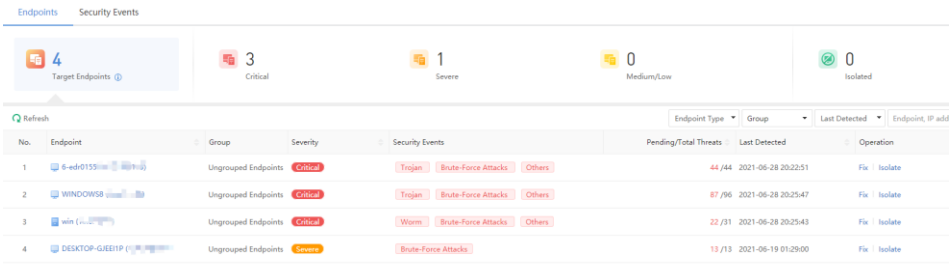
Security events must be handled for critical, severe, and medium or low endpoints in sequence.



6.4.2 Case

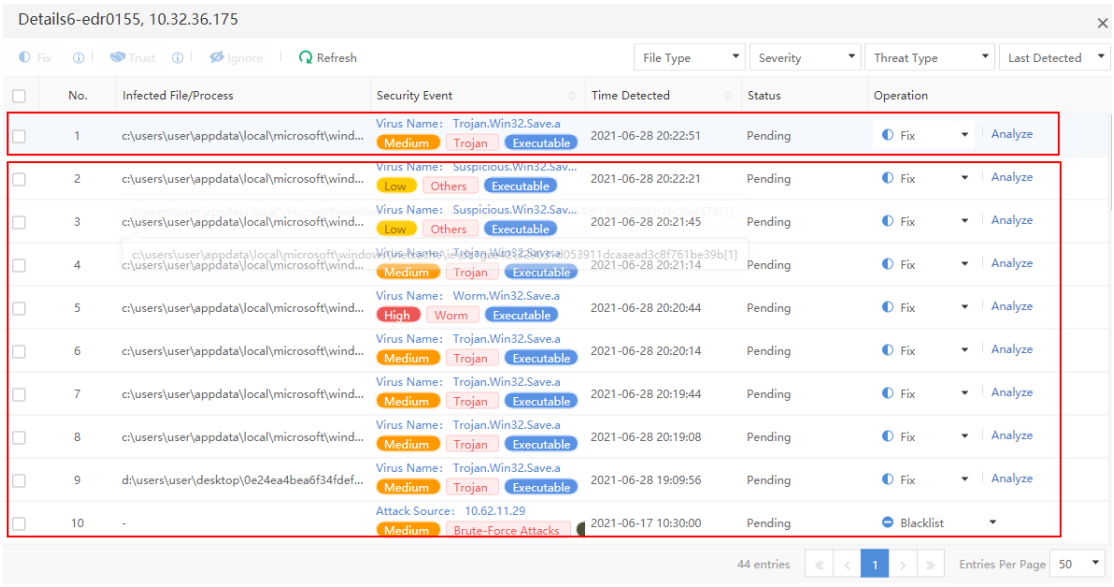
This section uses a case to describe how to handle malicious files.

Files that are not automatically isolated will be reported to the **Response** > **Threat Response** page, as shown in the following figure. Security events must be handled for critical, severe, and medium/low endpoints in sequence.



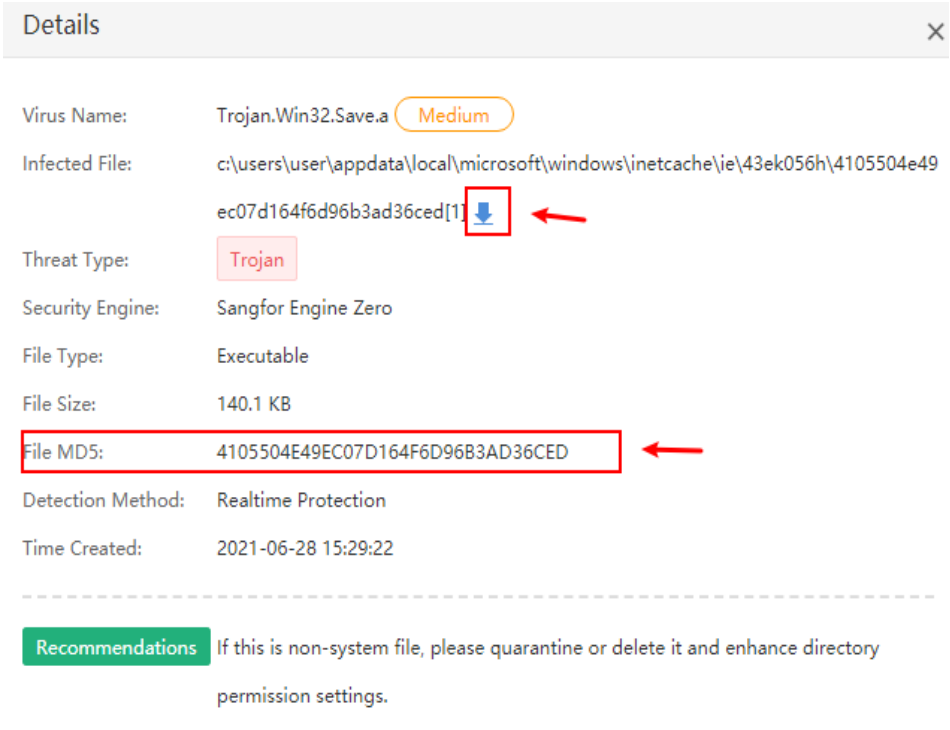
Step 1. Determine whether a malicious file is a business file.

The following figure shows malicious files found on an endpoint. The second to seventh malicious files are in the recycle bin and are not business files. They can be handled with one click. The first file is suspicious and needs further analysis.



Step 2. Obtain the suspicious file for further analysis.

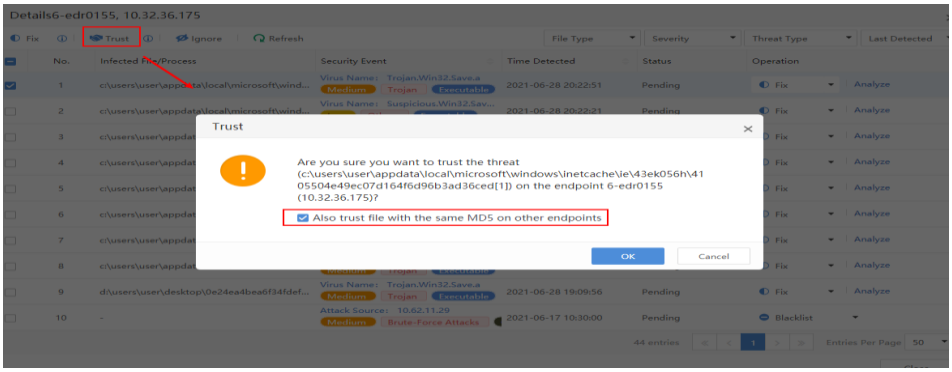
View the suspicious file details, download the suspicious file sample, and upload it to an intelligence website (such as https://www.virustotal.com/gui/home) for further analysis.



Step 3. Based on the threat analysis result can further process the file.

According to the analysis result of ThreatBook Cloud Sandbox, the file is secure

and needs to be added as a trusted file.



7 High-risk Operations

The following table describes high-risk operations that need to be avoided during the use of Endpoint Secure. Improper implementation of these operations will affect services and even cause service interruption.

Module	Level-1 Menu	Level-2 Menu	Risky Operation	Description	Severity	Solution
Endpoints	Security Protection	Anti-Malware	Set the action for detected malicious files to **Enhanced**.	The customer's business files may be isolated due to false positives, resulting in business exceptions.	High	Set the action for detected malicious files to **Standard**.
Endpoints	Security Protection	Anti-Malware	Enable heuristic scanning during normal use.	Heuristic scanning can improve the virus detection rate but will increase false positives. It needs to be enabled only when the virus detection rate is tested.	High	Disable heuristic scanning during normal use.
Endpoints	Security	Realtime	Set the action	The	High	Set the

	Protection	Protection	for detected malicious files in the **Realtime File Protection** area to **Enhanced**.	customer's business files may be isolated due to false positives, resulting in business exceptions.		action for detected malicious files to **Standard**.
Detection	Virus Scan	CPU Usage	Select **High CPU** when the server resources are insufficient.	In **High CPU** mode, more CPU resources will be consumed. If the server resources are insufficient, services will be affected. You are advised to use the **Balanced** mode.	High	When the server resources are insufficient, select **Low CPU** or **Balanced** for **CPU Usage**.
Response	Threat Response	Endpoints	Isolate endpoints.	Isolated endpoints can only connect to the Endpoint Secure Manager and cannot access any	High	Choose **Response** > **Threat Response**, click **Isolated** on the **Endpoints** tab, and

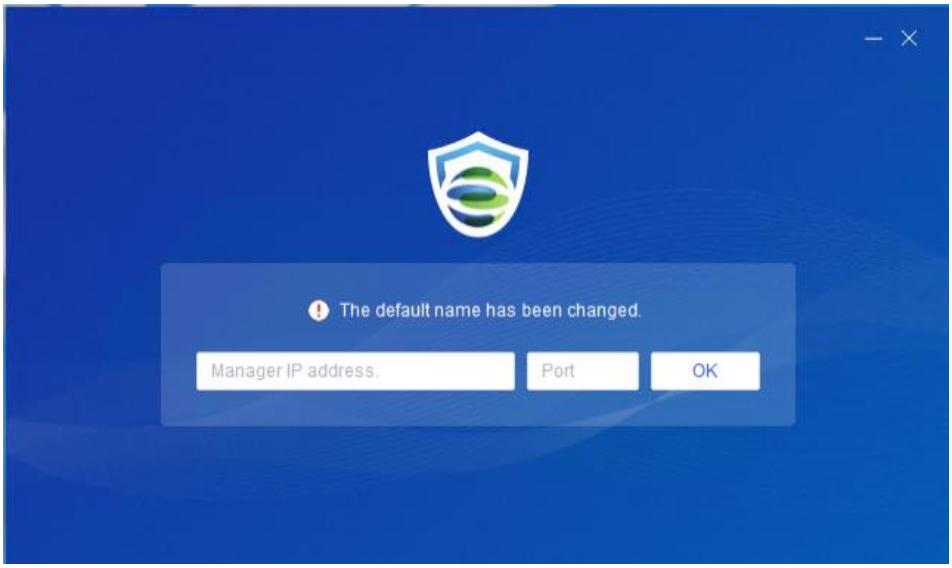
				other networks. If a server is isolated, services will be affected.		remove isolated endpoints.
Response	Remediation	Patching	Enable automatic server restart for vulnerability fixing.	Server restart causes service interruption.	High	Do not enable server restart for vulnerability fixing. Restart a server manually at a specific time when services are not affected.
Endpoints	Security Protection	Server Protection	Enable server protection or critical directory protection but do not add service processes of the server to the trusted processes.	Key services of the server do not run, resulting in service interruption.	High	Add service processes of the server to trusted processes.

Table 8: High-risky operations

8 FAQ

8.1 Installation

1. What can I do if the message in the following figure is shown during installation?



Solution:

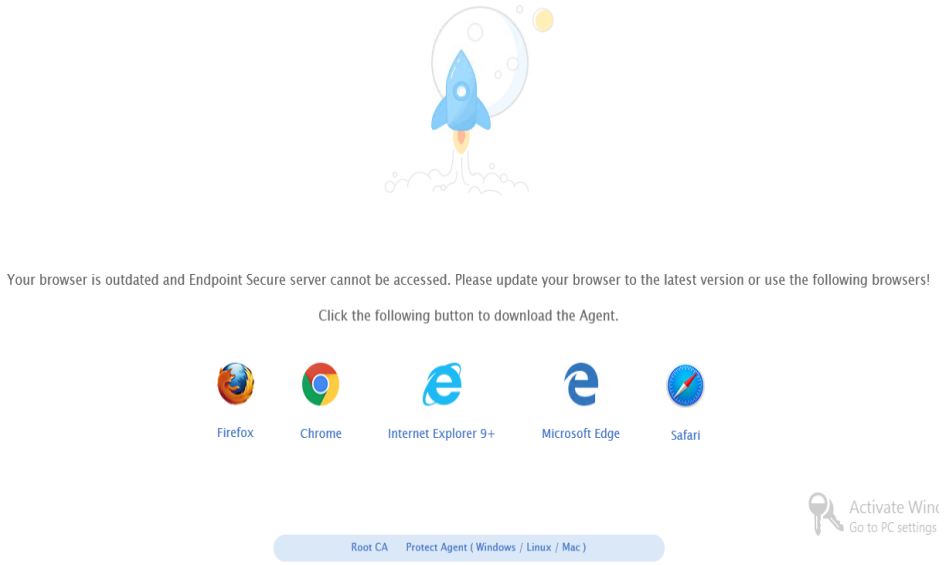
The message is shown because the installer file name is modified. Enter the IP address of the Endpoint Secure Manager and port 443 in the dialog box to complete installation. Alternatively, download the installer without modifying the file name and use it to install the Manager.

2. What can I do if "It is detected that you have installed other security software, which may conflict with the Endpoint Secure Agent" is shown during installation?

Solution:

Uninstall other security software on the computer and install the Endpoint Secure Agent.

3. What can I do if I failed to log in to the Endpoint Secure Manager through Internet Explorer and a message in the following figure is shown?



Solution:

The message is displayed because your Internet Explorer is not the latest version. Use Internet Explorer 11 or another browser to log in to the Endpoint Secure Manager.

4. What can I do if the antivirus database does not automatically update?

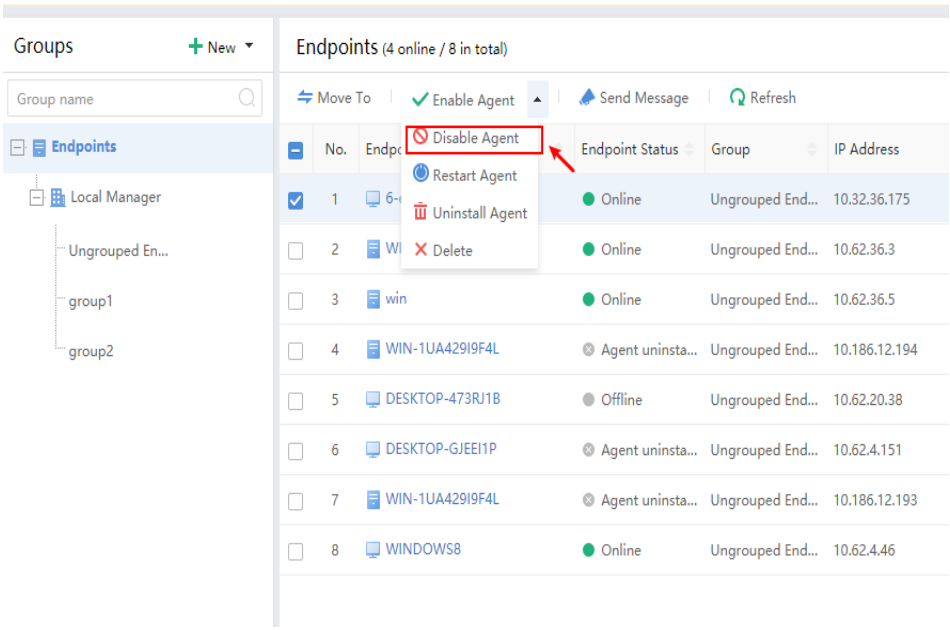
Solution:

Ensure that the Manager IP address, gateway, and DNS are correctly configured, and the environment where the Manager resides can visit download.sangfor.com.cn.

5. What can I do if the computer is abnormal after the Endpoint Secure Agent is installed?

Solution:

Log in to the Endpoint Secure Manager, choose **Endpoints** > **Groups**, disable the Agent for the abnormal computer, as shown in the following figure. If the fault is rectified, contact the service provider for further processing.



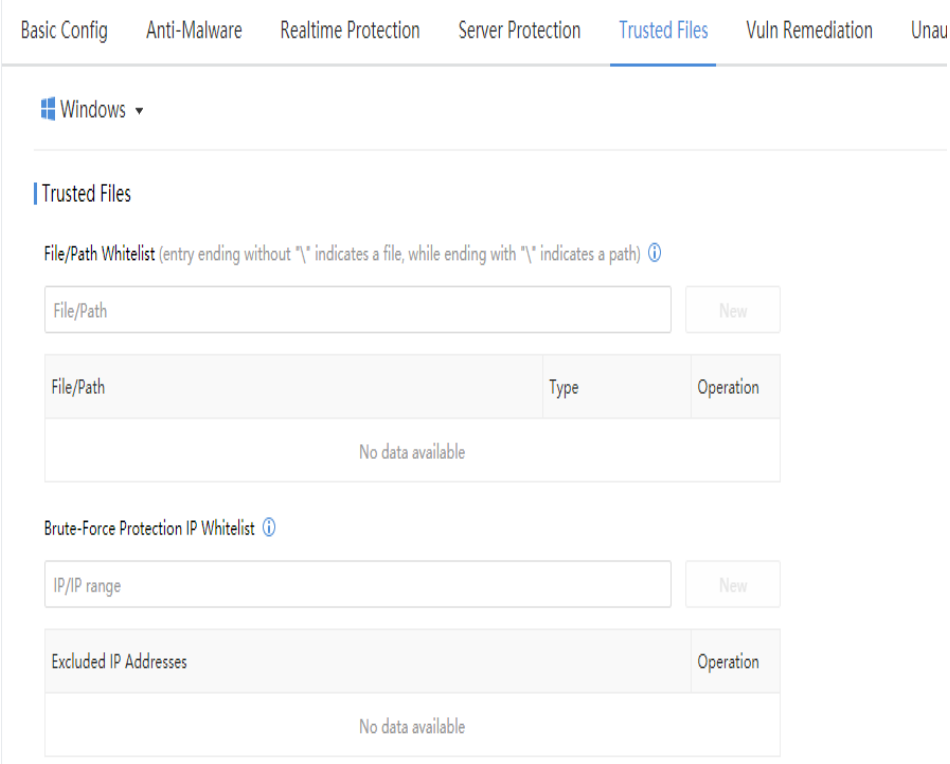
8.2 Anti-Malware

1. What can I do if a business file is mistakenly regarded as a malicious file by an anti-malware task?

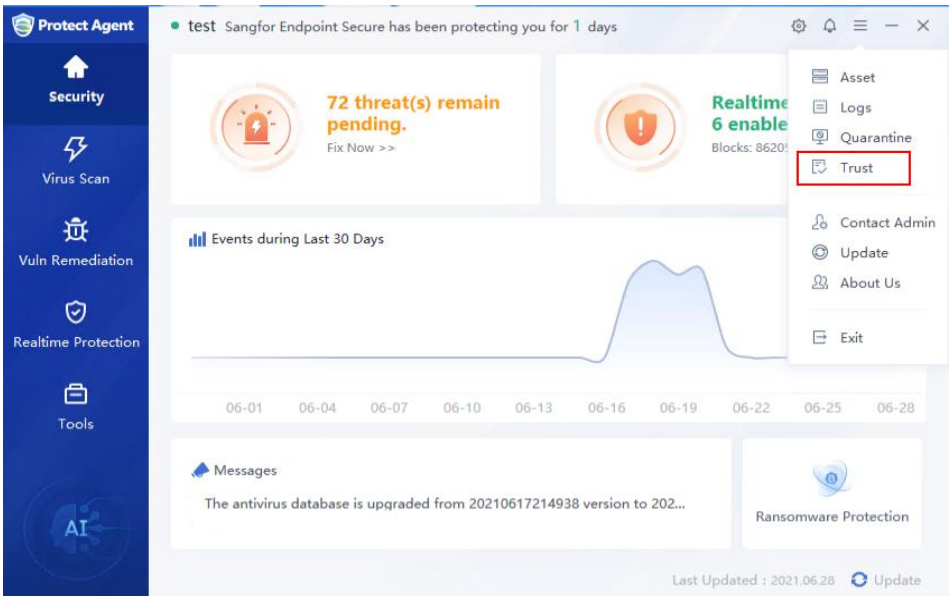
Solution:

Use either of the following methods to add the business file to the trusted files.

- On the Endpoint Secure Manager, choose **Endpoints** > **Security Protection** > **Trusted Files**, click **New** in the **Trusted Files** area, and select the business file, as shown in the following figure.



- On the Endpoint Secure Agent, adds the business file to the **Trust** area, as shown in the following figure.



2. Does Endpoint Secure support virus scan for files in USB flash drives and network sharing paths?

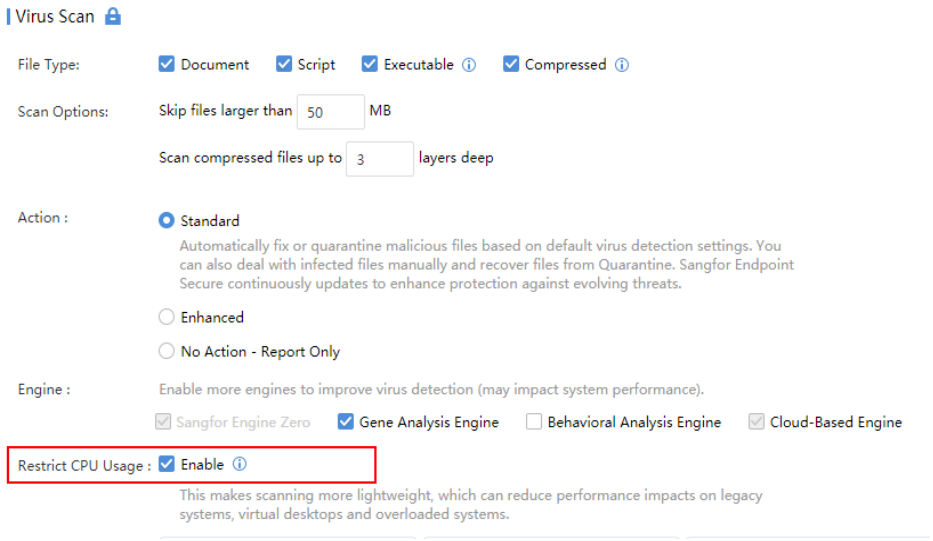
Solution:

Endpoint Secure supports virus scan for files in USB flash drives but not for files in network sharing paths.

3. What can I do if the CPU usage on a low-performance computer is high when Endpoint Secure delivers an anti-malware task?

Solution:

On the Endpoint Secure Manager, choose **Endpoints** > **Security Protection** > **Anti-Malware**, and enable **Restrict CPU Usage**, as shown in the following figure.



4. What can I do if a message indicating that the isolated area is full and malicious files cannot be isolated shown when I isolate malicious files?

Solution:

On Windows endpoints, the isolated area is 4 GB by default, and the path of the isolated area is **C:\ProgramData\Sangfor\EDR\SAV**. When files in the path exceed 4 GB, no more malicious files can be isolated. Delete files in the isolated area through the Endpoint Secure Manager or Agent.

8.3 Micro-Segmentation

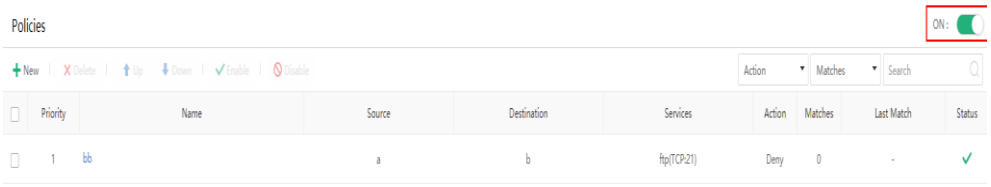
1. What can I do if the micro-segmentation policy does not take effect?

Solution:

Troubleshoot the fault as follows. If the fault persists, contact the service provider for processing.

- Check whether the operating system version of the endpoint is Windows XP or Windows Server 2003. The micro-segmentation function is not supported on endpoints running Windows XP or Windows Server 2003.

- Log in to the Endpoint Secure Manager, choose **Micro-Segmentation** > **Policies,** and check whether the **Micro-Segmentation** switch is turned on, as shown in the following figure.

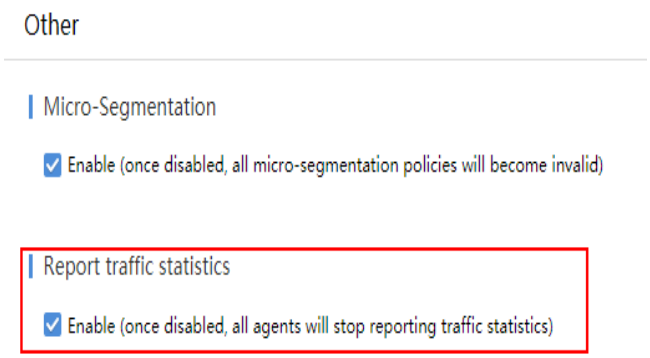


2. What can I do if micro-segmentation traffic statistics are not displayed?

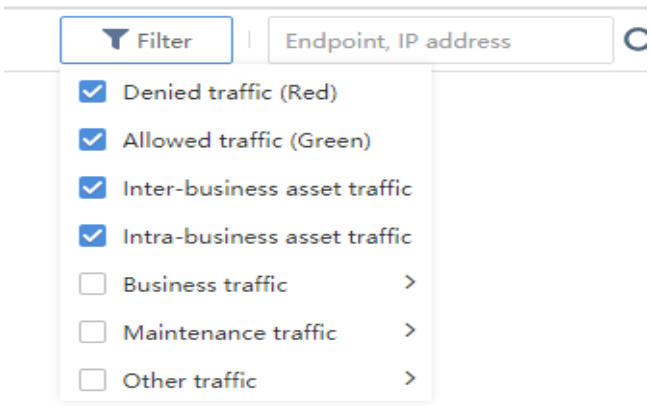
Solution:

Troubleshoot the fault as follows. If the fault persists, contact the service provider for processing.

- Log in to the Endpoint Secure Manager, choose **Micro-Segmentation** > **Other**, and check whether **Report traffic statistics** is enabled, as shown in the following figure.



- Log in to the Endpoint Secure Manager, choose **Micro-Segmentation** > **Traffic Statistics**, and check whether **Filter** is enabled, as shown in the following figure.



8.4 Others

If you have other requirements, for example, modifying port 443 of the Endpoint Secure Manager, restoring the login password of the Endpoint Secure Manager, and migrating the Endpoint Secure Manager to another server, contact the service provider for processing.

9 Acronyms and Abbreviations

	English Full Name
IAG	Internet Access Gateway
NGAF	Next Generation Advance Firewall
CVE	Common Vulnerabilities & Exposures
ES	Endpoint Secure
HCI	Hyper-Converged Infrastructure
CCom	Cyber Command
PX	Platform-X

SANGFOR