# ForeNova NovaGuard

## User Manual

| | |
|---|---|
| **Product Version** | 3.7.12 |
| **Document Version** | 01 |
| **Released on** | Jan. 10, 2023 |



Copyright © ForeNova Technologies Inc. 2023. All rights reserved.

Unless otherwise stated or authorized, ForeNova Technologies Inc. (hereinafter referred to as "ForeNova") and its affiliates reserve all intellectual property rights, including but not limited to copyrights, trademarks, patents, and trade secrets, and related rights to text, images, pictures, photographs, audio, videos, charts, colors, and layouts as presented in or concerning this document and content therein. Without prior written consent of ForeNova, this document and content therein must not be reproduced, forwarded, adapted, modified or displayed or distributed by any other means for any purpose.

## 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 ForeNova. Unless otherwise provided in the contract, ForeNova disclaims warranties of any kind, either express or implied, for the content of this document.

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

# Technical Support

For technical support, please visit:

https://www.forenova.com/en/about-us/contact-us/technical-support

Send information about errors or any product related problem to

tech.support@forenova.com.

# About This Document

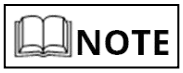
This document describes the architecture, features, installation, and O&M management of ForeNova NovaGuard.

# Intended Audience

This document is intended for:

- Network design engineers
- O&M personnel

# Note Icons

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

# Change Log

| Date | Change Description |
| --- | --- |
| Jan. 10, 2023 | This is the first release. |

# Contents

Technical Support ..... i

Change Log ..... iii

1 Product Overview ..... 1

1.1 Introduction ..... 1

1.2 Key Features ..... 2

1.2.1 Network-wide Endpoint Inventory ..... 2

1.2.2 Endpoint Security Compliance Audit ..... 2

1.2.3 Real-Time Protection from Ransomware ..... 3

1.2.4 System Vulnerability Detection and Rectification ..... 3

1.2.5 Proactive Detection of Intrusion Attacks ..... 3

2 Installation ..... 4

2.1 Preparation ..... 4

2.1.1 Manager Installation Environment ..... 4

2.1.2 Agent Installation Environment ..... 4

2.1.3 Network Connectivity Requirements ..... 5

2.1.4 Trusted File Whitelisting ..... 6

2.2 Manager Installation ..... 6

2.2.1 Manager Software Installation ..... 6

2.3 Product Activation ..... 12

2.4 Endpoint Management ..... 13

2.5 Protection Configuration ..... 13

2.5.1 Trusted Files Configurations ..... 14

2.5.2 Security Protection Configuration ..... 15

2.6 Agent Installation ..... 18

2.6.1 Installation on the Windows Operating System ..... 18

2.6.2 Installation on Linux Servers ..... 23

2.6.3 Installation on the Mac Operating System ..... 25
2.7 Agent Uninstallation ..... 31
2.7.1 Uninstallation on the Windows Operating System ..... 31
2.7.2 On Linux Servers ..... 31
2.7.3 On the Mac Operating System ..... 31
2.7.4 On the Manager ..... 32
3 Manager ..... 39
3.1 Manager Login ..... 39
3.2 Home Page ..... 39
3.2.1 Endpoints ..... 40
3.2.2 Windows Protection ..... 40
3.3 Endpoints ..... 51
3.3.1 Groups ..... 51
3.3.2 Inventory ..... 69
3.3.3 Endpoint Discovery ..... 76
3.3.4 Security Protection ..... 78
3.4 Micro-Segmentation ..... 117
3.4.1 Business Clarification ..... 117
3.4.2 Creating Business Assets, Roles, IP Groups, and Services ..... 118
3.4.3 Policies ..... 121
3.4.4 Traffic Statistics ..... 122
3.4.5 Other ..... 122
3.5 Detection ..... 123
3.5.1 Virus Scan ..... 123
3.5.2 Vulnerability Scan ..... 129
3.5.3 Security & Integrity Check ..... 132
3.6 Response ..... 135
3.6.1 Threat Response ..... 135

3.6.2 Endpoints ..... 135
3.6.3 Security Events ..... 137
3.6.4 Advanced Threats ..... 141
3.6.5 Remediation ..... 148
3.6.6 Threat Hunting ..... 152
3.6.7 Remote Access ..... 159
3.6.8 Blacklist and Whitelist ..... 161
3.7 Logs ..... 163
3.7.1 Security Logs ..... 163
3.7.2 Coordinated Action ..... 164
3.7.3 Operation Logs ..... 164
3.7.4 Admin Logs ..... 165
3.7.5 Reports ..... 166
3.8 System ..... 167
3.8.1 Integrated Devices ..... 167
3.8.2 Branches ..... 172
3.8.3 Administrators ..... 180
3.8.4 Licensing ..... 185
3.8.5 System ..... 187
4 Agent ..... 206
4.1 Windows Agent ..... 206
4.1.1 Home Page ..... 206
4.1.2 Security ..... 206
4.1.3 Virus Scan ..... 207
4.1.4 Vulnerability Scan ..... 211
4.1.5 Realtime Protection ..... 211
4.1.6 Tools ..... 214
4.1.7 NovaGuard Agent-Settings ..... 214

4.1.8 Security Logs ..... 220
4.1.9 Quarantine and Trust Zones ..... 221
4.1.10 System Tray ..... 224
4.1.11 Customization ..... 225
4.2 MAC Agent ..... 225
4.2.1 Main Page ..... 225
4.2.2 Virus Scan ..... 226
4.2.3 Quarantine ..... 227
4.2.4 Feedback ..... 228
5 Product Update ..... 229
5.1 Manager Update ..... 229
5.2 Agent Update ..... 229
5.2.1 Auto Update ..... 229
5.2.2 Concurrent Update ..... 230
5.3 Antivirus Database and Engine Update ..... 231
5.3.1 Automatic Online Update ..... 231
5.3.2 Manual Offline Update ..... 231
5.3.3 IOA Databases and IOC Databases Update ..... 232
5.4 Vulnerability Database and Patch Package Update ..... 233
5.4.1 Automatic Online Update ..... 233
5.4.2 Manual Offline Update ..... 233
6 Maintenance ..... 235
6.1 Endpoints ..... 235
6.1.1 Groups ..... 235
6.2 Licenses ..... 236
6.3 Server Protection ..... 237
6.3.1 Version and Database Check ..... 238
6.3.2 Exit Password and Uninstallation Password ..... 238

6.3.3 Manager Accounts and Passwords ..... 239
6.3.4 Remote Access Protection Password ..... 239
6.3.5 Administrator Login IP Address Restriction ..... 240
6.3.6 Security Compliance Check ..... 241
6.3.7 Vulnerability Scan ..... 241
6.3.8 Policy Optimization ..... 242
6.4 Security Event Handling ..... 243
6.4.1 Rules ..... 243
6.4.2 Case ..... 244
7 High-risk Operations ..... 247
8 FAQ ..... 249
8.1 Installation ..... 249
8.2 Anti-Malware ..... 251
8.3 Micro-Segmentation ..... 253
8.4 Others ..... 254
9 Acronyms and Abbreviations ..... 256

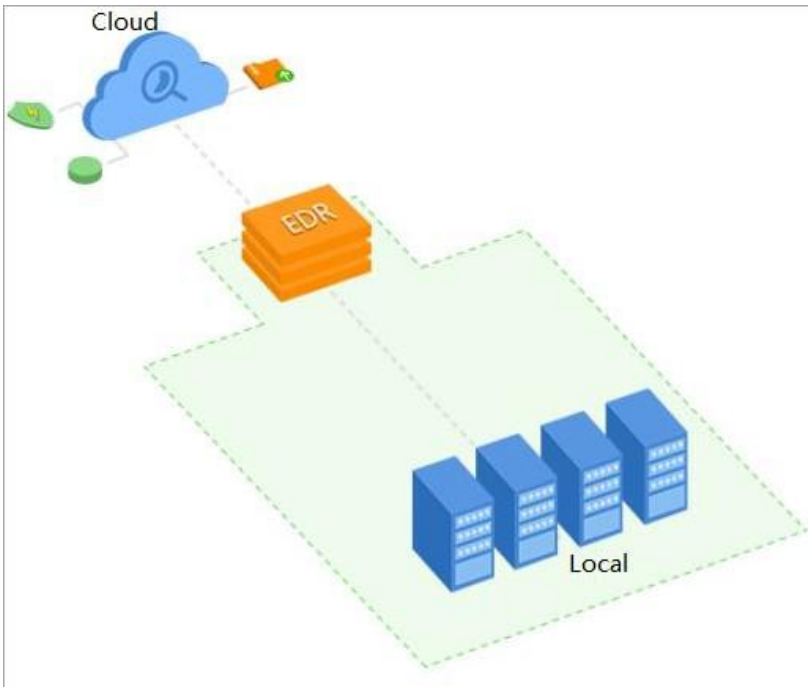
# 1 Product Overview

NovaGuard is an endpoint security solution provided by ForeNova. It consists of the cloud service center, lightweight endpoint security software NovaGuard Agent (Agent for short), and NovaGuard 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, NovaGuard can integrate and coordinate with Cyber Command and Platform-X, forming the new-generation security protection system.

## 1.1 Introduction

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

## 1.2.2 Endpoint Security Compliance Audit

Each organization has its 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 with 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 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. NovaGuard can identify different ransomware families accurately, recognize ransomware infection and encryption features after professional analysis, and 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. NovaGuard 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 upon and then infected with ransomware or crypto mining. Most attackers crack weak passwords using brute force methods to intrude on endpoint hosts. NovaGuard 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

NovaGuard is an endpoint security solution that consists of the cloud service center, Manager, and Agent. This chapter describes how to install NovaGuard, 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 Windows and Linux operating systems. The following table lists the supported operating systems and versions.

| Operating System | Version |
|---|---|
| Windows | Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, and Windows 11. |
| Windows Server | Windows Server 2003 SP2<br>Windows Server 2008/2008 R2<br>Windows Server 2012/2012 R2 |

| | |
|---|---|
| | Windows Server 2016/2019 |
| Linux | CentOS 5.x/6.x/7.x/8.x<br>Ubuntu 10.x/11.x/12.x/13.x/14.x/16.x/17.x/18.x/20<br>Debian 6.x/7.x/8.x/9.x<br>RHEL 5.x/6.x/7.x/8.x<br>SUSE 11/12/15<br>Oracle Linux 5.x/6.x/7.x |
| Mac | Mac OS 12<br>Mac OS 11.x<br>Mac OS 10.13<br>Mac OS 10.14<br>Mac OS 10.15 |

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 NovaGuard 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 the ForeNova 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.forenova.com |

| | | | |
|---|---|---|---|
| | | Licensing | https://auth.forenova.com |
| | | Cloud-Based Engine | https://analysis.forenova.com |
| | | Terms of Use and Privacy Policy | https://clt.forenova.com |
| | | IOC Rules Upgrade | https://intelligence.forenova.com |
| | | Patches, signature, and antivirus database | http://download.forenova.com<br>https://download.forenova.com |

Table 3: Network connectivity requirements

### 2.1.4 Trusted File Whitelisting

To prevent false error reports during virus scans 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 scans 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.forenova.com and choose **Self-Service** > **Software Download** > **Endpoint**.

NOTE

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

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

Download the installation and update package of the official version for update.

Offline agent installer can download at: https://community.forenova.com (Path: **Self Services** > **Download** > **Endpoint**)

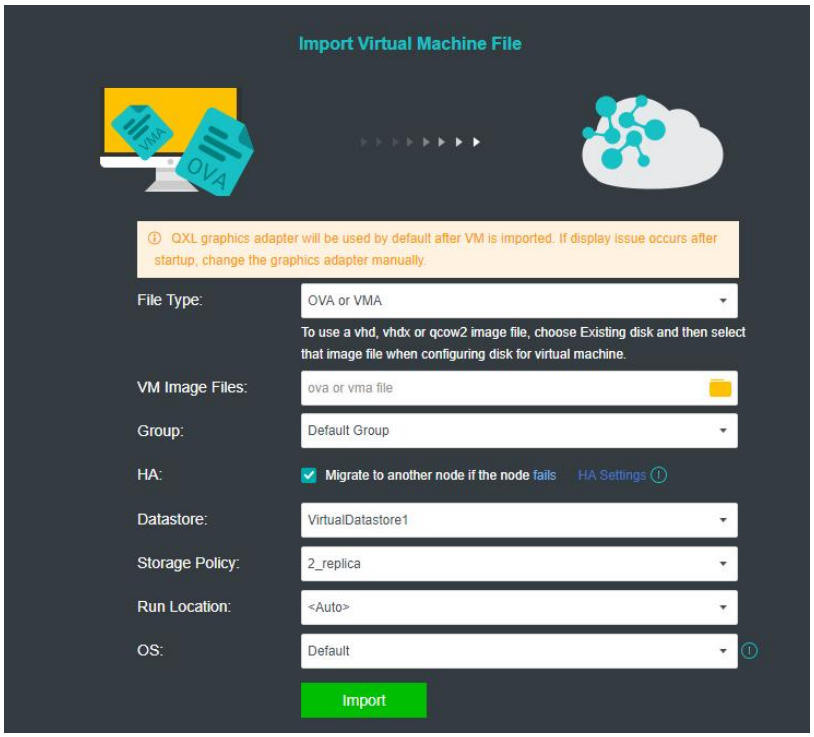
### 2.2.1.2 Installation in OVA Image Mode

NOTE

The following describes installing 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.

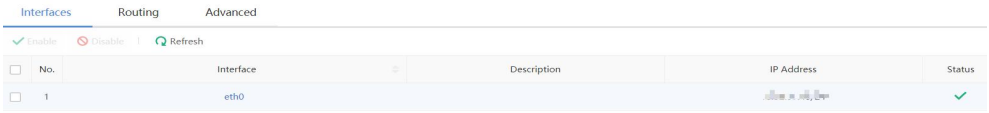
NOTE

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's IP address.

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

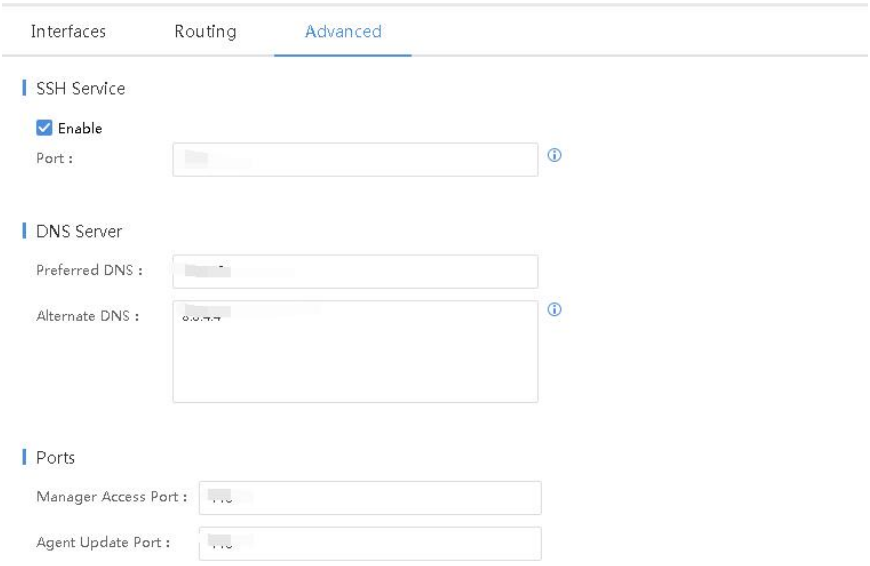



3. Configure DNS addresses.

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.

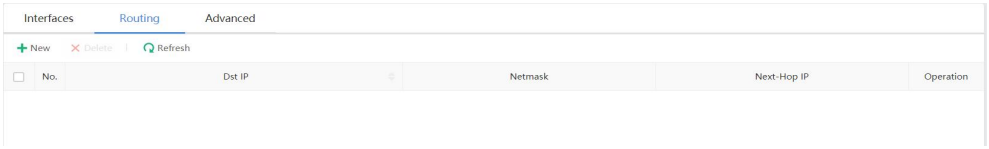



4. Configure routes.

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

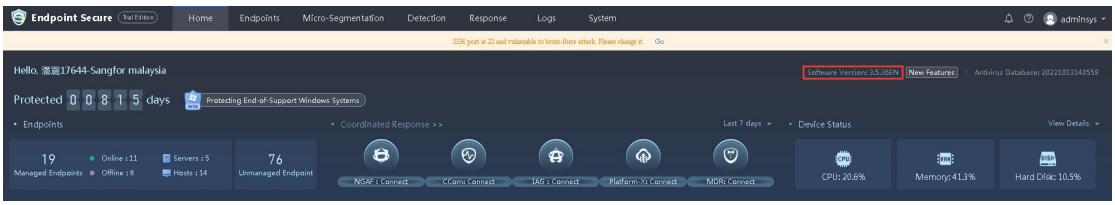
**NOTE**

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.

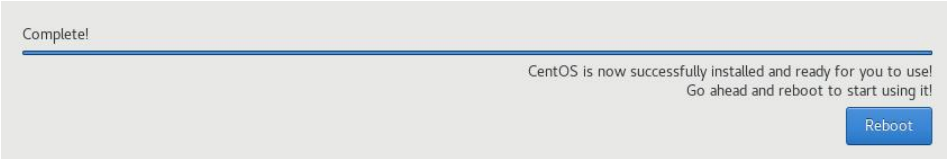
---

**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.



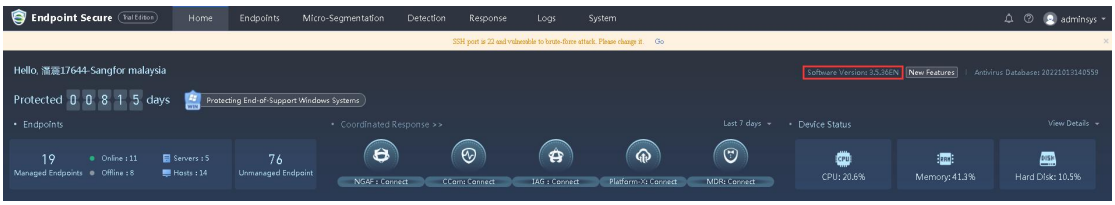

3. Click **Reboot** to restart the server.

**Step 3.** Configure the network.

For details, see **Configure the network** in **Chapter 2.2.1.2**.

**Step 4.** Verify that the Manager installation is successful.

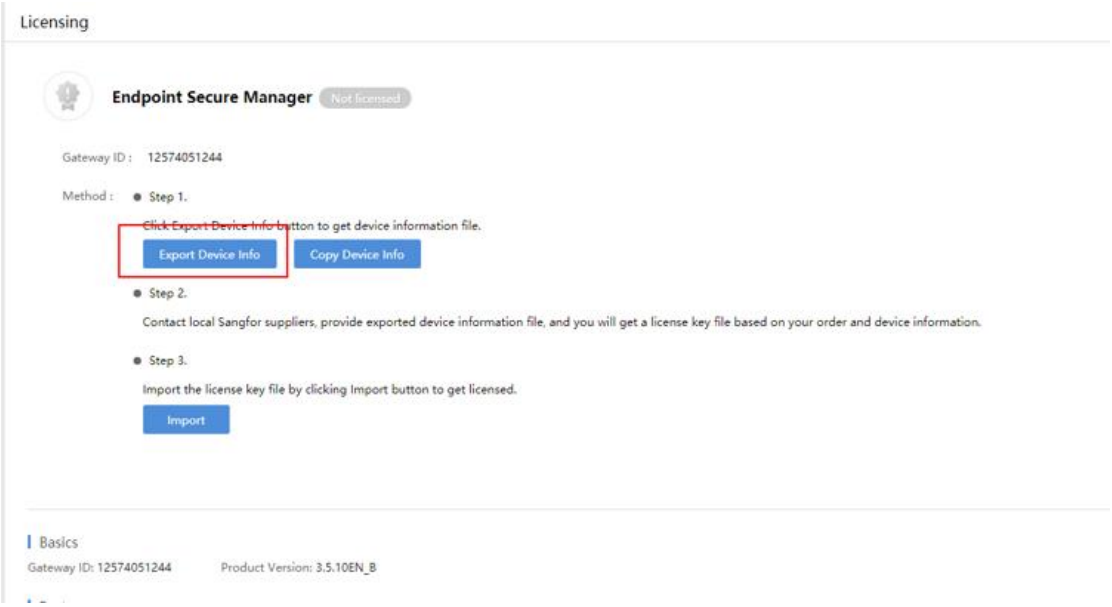
Log in to the Manager (default address: https://10.251.251.251, default user name and password: **admin** and **admin**) and check whether the version number on the home page is correct, as shown in the following figure. If the version number is correct, the installation is successful.



# 2.3 Product Activation

After the Manager is installed, you must activate the Manager before installing the Agent and using the NovaGuard Manager. Perform the following operations to activate the Manager as a customer:

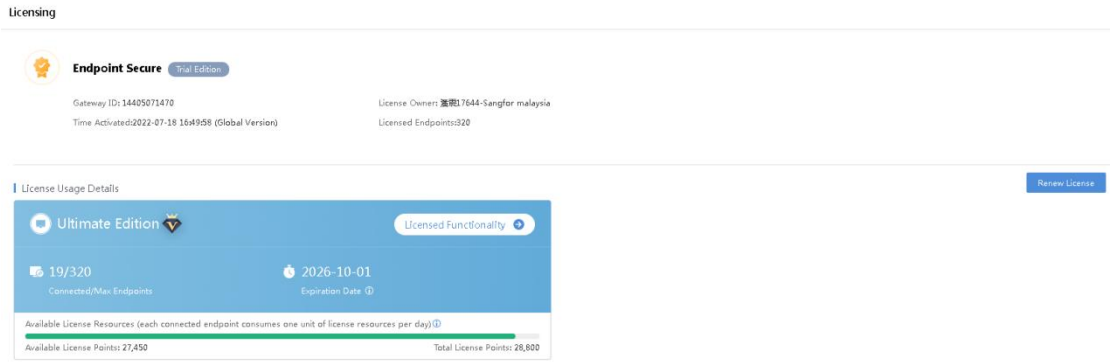
**Step 1.** Click **Export Device Info** button to get the device information file.




**Step 2.** Contact local ForeNova 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 each type's licensed endpoints is displayed, indicating that the Manager is activated successfully.



## 2.4 Endpoint Management

NovaGuard supports tree organization to manage intranet endpoints, manual creation of groups, import of groups, LDAP synchronization of OU and domain users, and selecting online groups by end users. Users can choose the grouping method according to their actual needs.

## 2.5 Protection Configuration

Security protection covers the basic configuration, anti-malware, real-time protection, anti-ransomware, trusted files, vulnerability remediation, endpoint control, and other security protection. The functions supported by different endpoints are as follows. The following table describes the supported security protection for Windows PC, Windows Server, and Linux.

| Security Protection | Windows PC | Windows Server | Linux | MAC |
|---|---|---|---|---|
| Basic Config | √ | √ | × | × |
| Virus Scan | √ | √ | √ | × |
| Realtime Protection | √ | √ | √ | × |
| WebShell Detection | × | √ | √ | × |
| Ransomware Protection | √ | √ | × | × |
| Brute-Force Attack Protection | √ | √ | √ | × |
| Fileless attack protection | √ | √ | × | × |
| Enhanced Server Protection | × | √ | × | × |
| Trusted Files | √ | √ | × | × |
| Quarantine Management | √ | √ | √ | × |

| | | | | |
|---|---|---|---|---|
| Vulnerability Remediation | √ | √ | × | × |
| Unauthorized Outbound Access Detection | √ | √ | × | × |
| USB Control | √ | √ | × | × |
| RDP Secondary Authentication | × | √ | × | × |

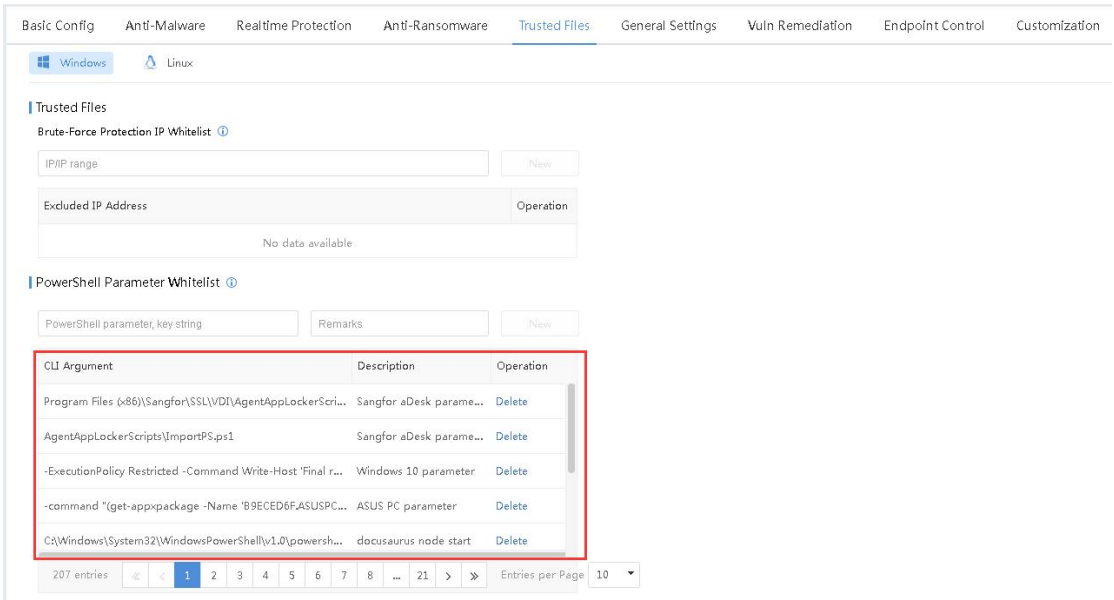
Table 4: Supported security protection for Windows PC, Windows Server, Linux, and MAC

## 2.5.1 Trusted Files Configurations

To avoid false positives that virus scans may cause, collect trust files in advance and add them to the whitelist. The whitelist file includes the business software, tools, and PowerShell script parameters (it needs to be whitelisted if PowerShell writes an operation and maintenance script).

1. PowerShell parameters whitelist

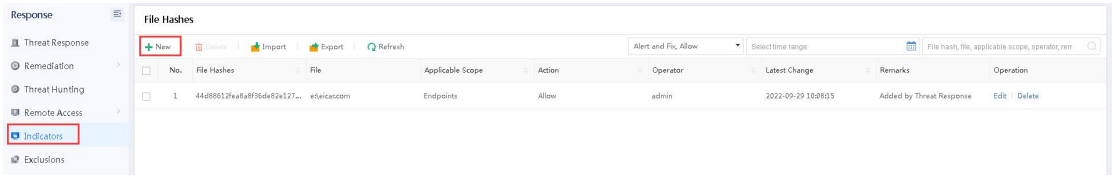
Navigate to **Endpoints** > **Security Protection** > **Trusted Files**, and add the **PowerShell Parameter Whitelist,** as shown in the figure below:

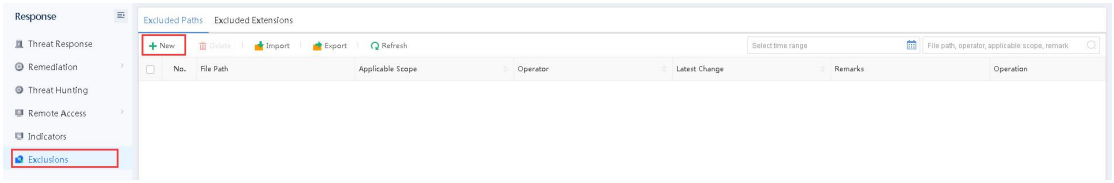



2. File Whitelist

Navigate to **Response** > **Indicators** or **Response** > **Exclusions**, add whitelist files

according to md5, or directly add excluded files or directories, as shown in the figure below:



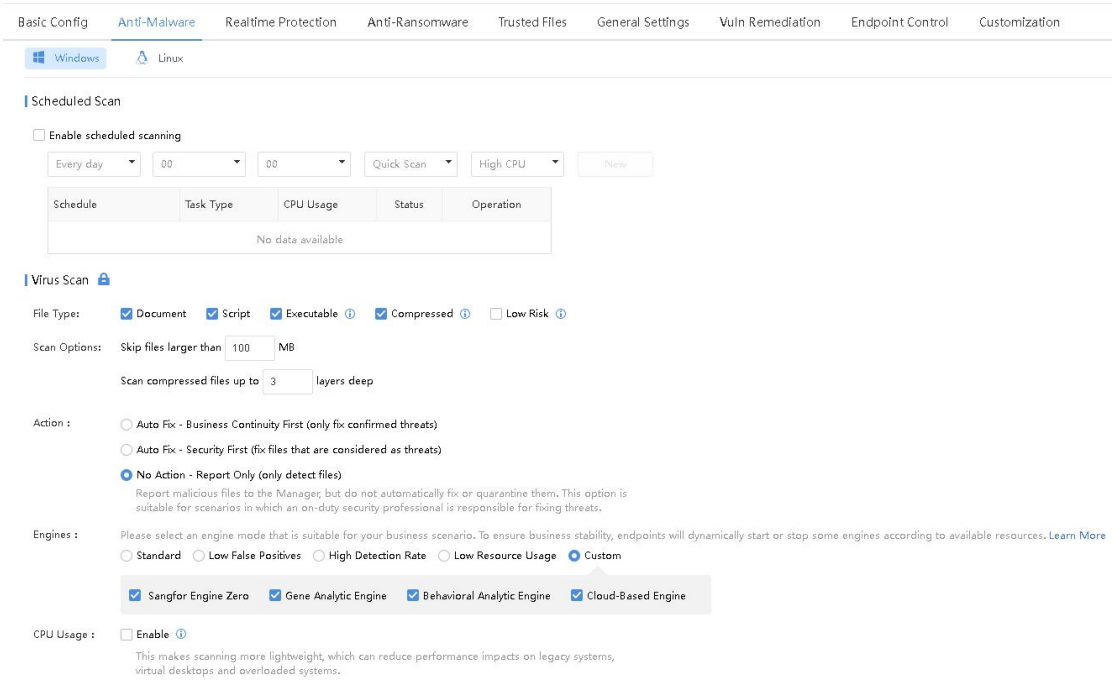

## 2.5.2 Security Protection Configuration

Security protection configuration includes the following three parts.

Configure the security protection according to the following requirements when the product is first deployed:

1. Virus Scan

Navigate to **Endpoints > Security Protection > Anti-Malware > Virus Scan**, and configure the **Scan Options** and **Action**:



**Scheduled Scanning:** It is recommended to enable it. It is recommended to regularly scan once a week, choose noon or non-working time, set scan type to quick scan, and select balanced scan mode.

**File Type:** Do not select the **Low Risk** file type (not selecting it will help improve the scanning speed). Select all other file types. Actions to deal with after a threat is found: Set to auto fix - business continuity first.

**Engines:** Configure according to the actual situation. The default configuration is standard mode.

Engine Modes

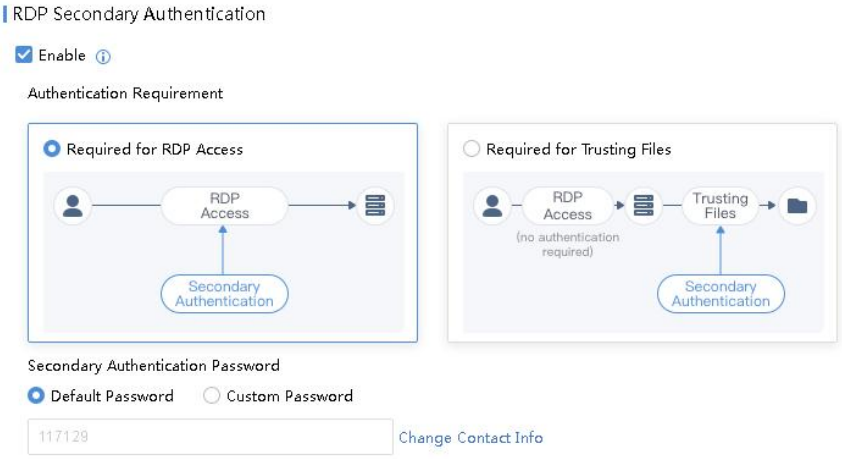
| Mode | Scenario | Used Mem... | Detection R... | False Positi... |
|---|---|---|---|---|
| Standard | General server and office network scenarios | Medium-Low | High | Low |
| Low False P... | General office scenarios involving important serv... | Low | High | Very Low |
| High Detect... | Scenarios with strict security protection requirem... | Medium-Low | Very High | Medium-Low |
| Low Resour... | Scenarios involving endpoints with overloaded sy... | Very Low | High | Low |

**CPU Usage:** If the endpoint computer configuration is relatively low or the Agent is installed in the desktop cloud environment, the resource optimization mode needs to be enabled.

2. RDP Secondary Authentication

The group where the Windows Server is located needs to enable the RDP secondary authentication to prevent the server from being brute-forced by the attacker's remote desktop login and gain server permissions. When you log in to the console, you will be prompted to enable secondary authentication for remote desktop login. Follow the prompts to enable secondary authentication for RDP.

You can also go to **Endpoint > Security Protection**, select the group where Windows Server is located, and configure the policy through **Anti-Ransomware > RDP Secondary Authentication**, as shown in the figure below.

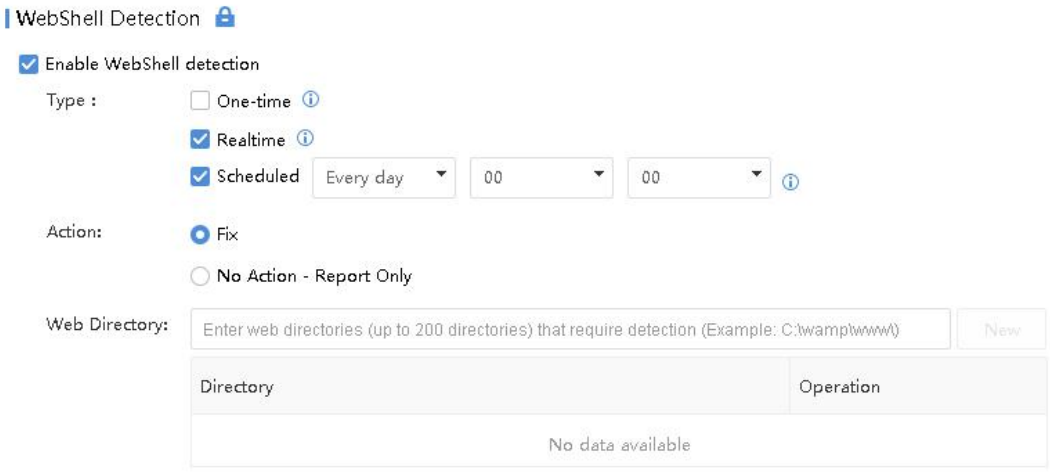



**Authentication Requirement:** select **Required for RDP Access**

**Secondary Authentication Password:** Select **Default Password**, and configure the NovaGuard administrator's name and mobile phone number correctly. The default password is the last six digits of the NovaGuard administrator's mobile phone number so that the server administrator can quickly obtain the authentication password when logging in to the server via a remote desktop.

3. WebShell Detection

Go to **Endpoint > Security Protection**, select the group where Windows Server is located, and configure the protection through **Realtime Protection > WebShell Detection**, as shown in the figure below.




**Type:** Enable **Realtime** detection and **Scheduled** detection.

**Action:** Set the processing action after discovering the webshell and set it to **Fix.**

**Web Directory:** Set the WebShell detection directory. The directory where the web server is located is detected by default, or you can self-define the custom directory.

**The following security protection is enabled by default and can keep the default configuration:**

WebShell detection, brute force detection, ransomware protection, and vulnerability remediation.

**You can enable the following security protection according to requirements:**

Micro-segmentation, enhanced server protection, USB control, and unauthorized outbound access detection.

# 2.6 Agent Installation

## 2.6.1 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.

### 2.6.1.1 Common Installation Scenarios

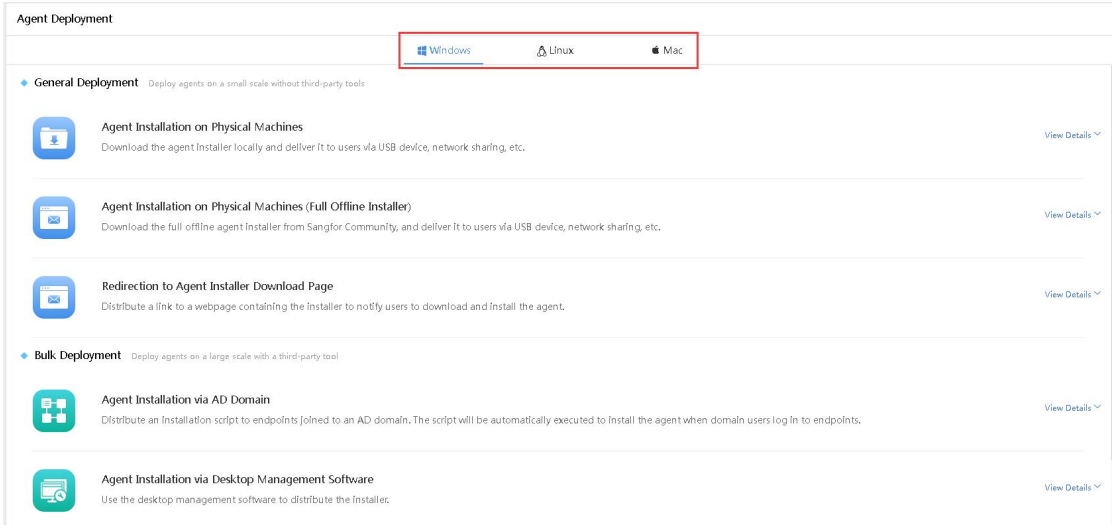
In common installation scenarios, you need to download the Agent installation package from the Manager and use a USB flash drive or other mobile media to import the package to the endpoint for installation as an administrator. The installation procedure is as follows:

1. **Navigate to System > Agent Deployment** and click **View Details** next to **Agent Installation on Physical Machines**.

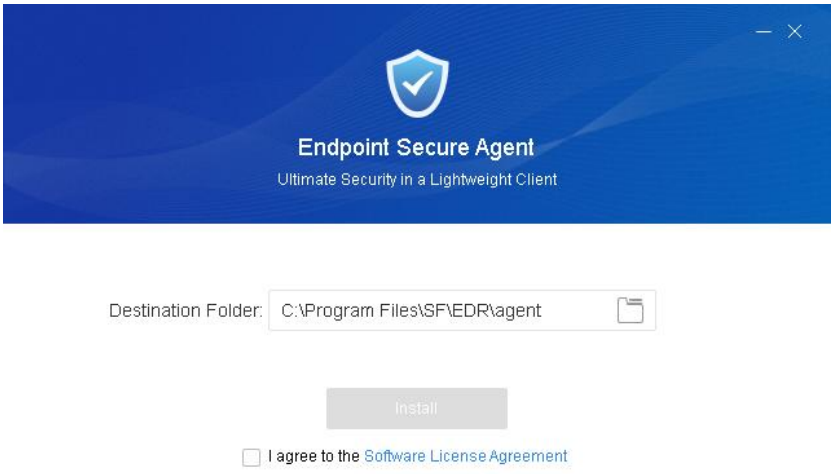
NOTE

The default PC Agent installation package name (similar to **edr_installer_117.48.147.100_443.exe**) contains the Manager communication address

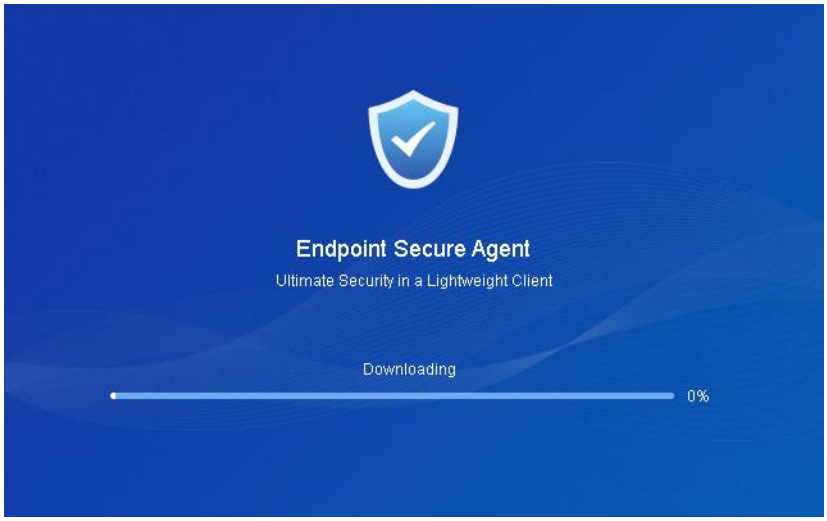
information. Do not change the installation package name after the installation package is downloaded.

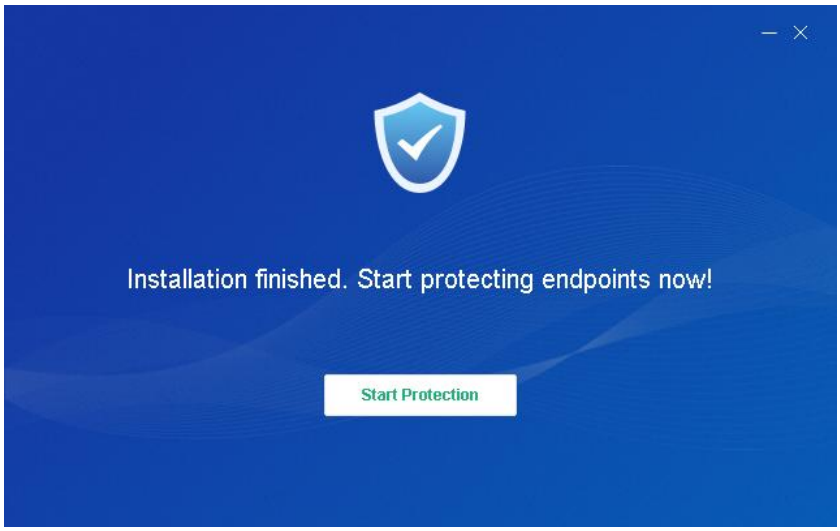



2. Copy the installation package to the endpoint on which the Agent needs to be installed.
3. Double-click the installation package on the endpoint.

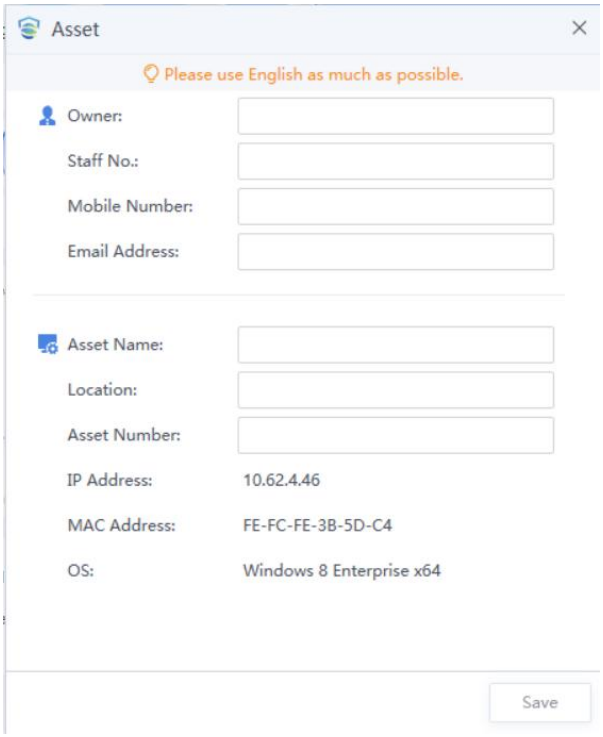


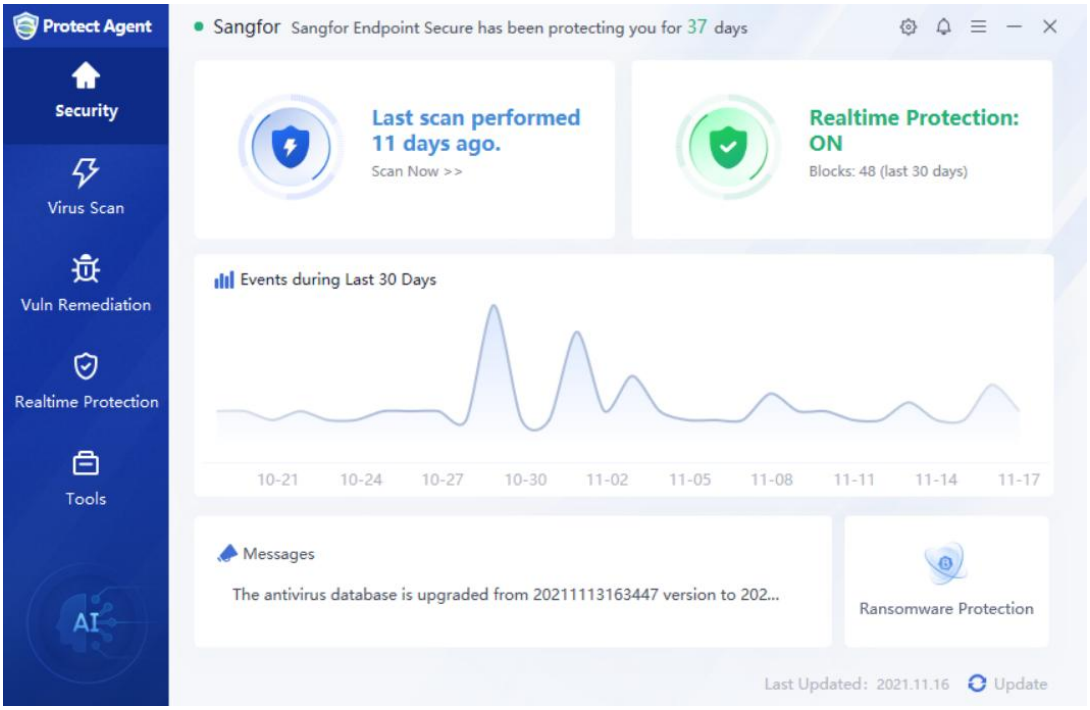

Select **I agree to the Software License Agreement** and click **Install**. The installation program connects to the Manager to download the required installation components, as shown in the following figure.



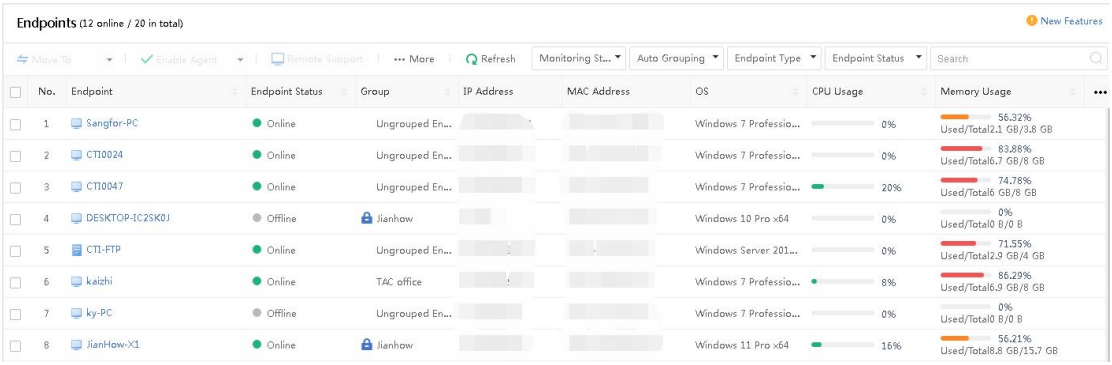




After the installation is complete, click **Start Protection** and enter asset information, as shown in the following figure.




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




## 2.6.1.2 Large-scale Installation Scenarios

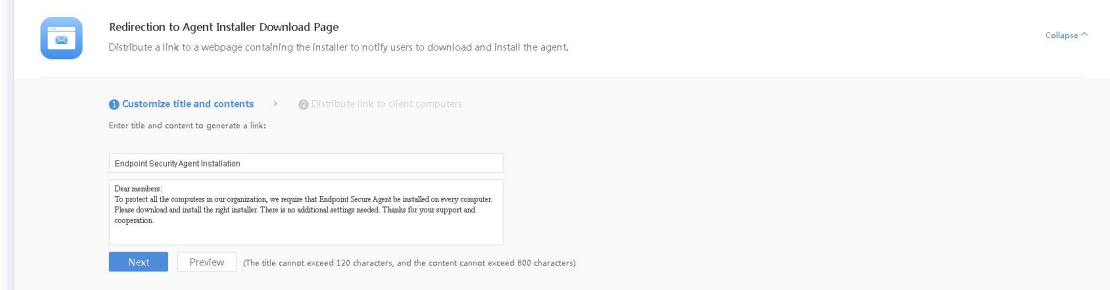
In large-scale installation scenarios, you can install the Agent by distributing a link to an installation notice webpage, using the IAG, using a VM template, or distributing the installation package by desktop management software. Select an installation mode based on the installation scenario on the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

### 2.6.1.2.1 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.

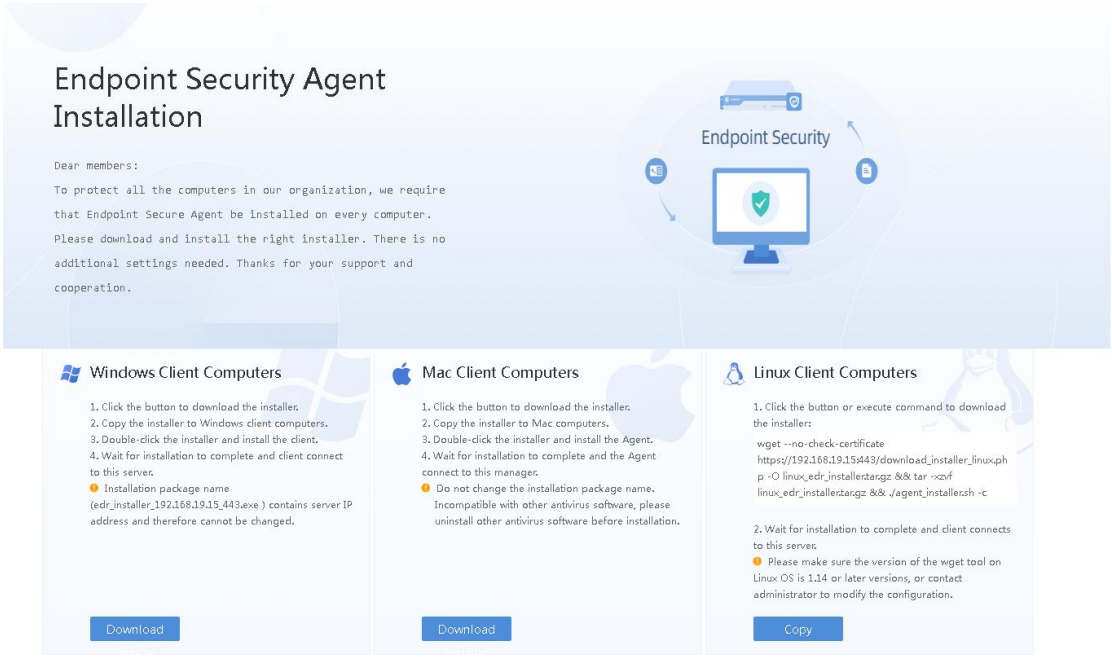
Choose **System**> **Agent Deployment**, select **Redirection to Agent Installer Download Page**, and enter the installation notice page title and content. Preview the installation notice to verify the notice information and click **Save and Generate Link**.




2. Copy the link and send it to endpoints.

Send the link to endpoint users in emails using OA or 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.




### 2.6.1.2.2 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. The installation procedure is as follows:

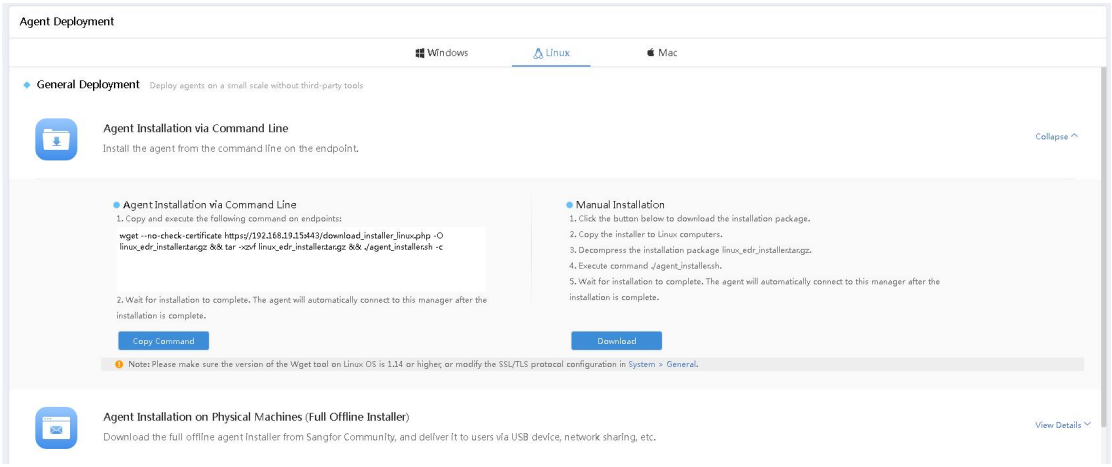
1. Import the downloaded Agent components to the VM template.
2. Install the Agent components on the VM.
3. Configure the template update policy to immediate or scheduled updates to install the Agent components in batches.

### 2.6.1.2.3 Desktop Management Software

This installation mode applies when desktop management 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.

## 2.6.2 Installation on Linux Servers

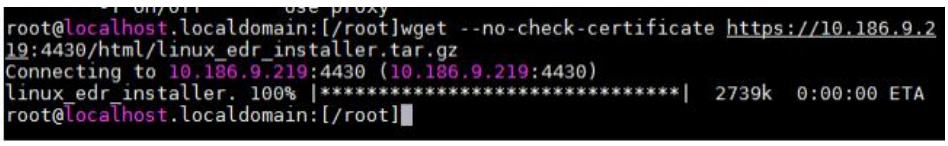
You can download the Agent installation package on Linux servers to install the Agent in common installation scenarios or use a script tool to install the Agent in large-scale installation scenarios.




## 2.6.2.1 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. 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 **/sf/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 an ipset is displayed during installation, you can select **y** or **n**. You should select **y** to install the ipset and then install the Agent.

### 2.6.2.2 Large-scale Installation Scenarios

You can also distribute a link to an installation notice webpage in large-scale installation scenarios. Use the IAG or 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.

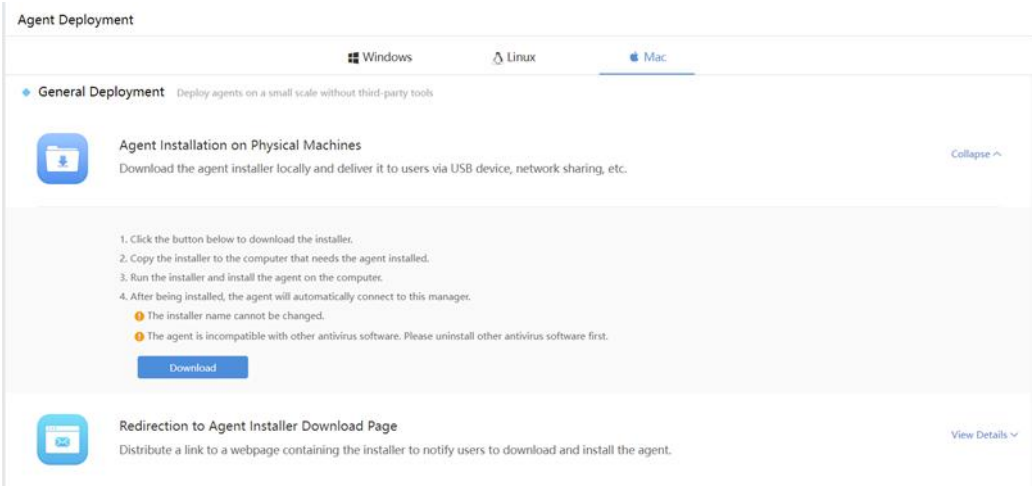
During script execution, the script tool connects to the Linux servers in SSH mode, automatically downloads the Agent components from the Manager, installs the Agent components, and brings the Agent components online to the Manager. The whole process is automatic.

NOTE

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

## 2.6.3 Installation on the Mac Operating System

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



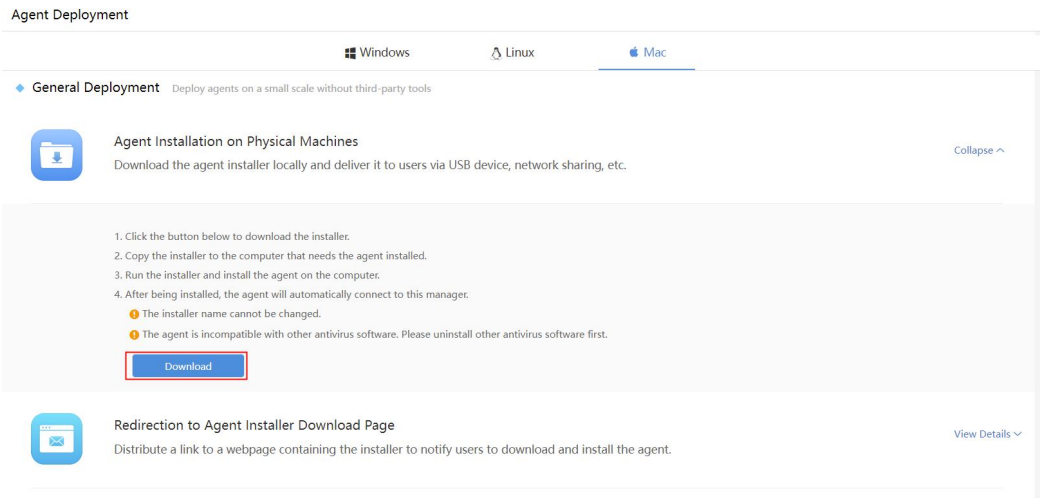

## 2.6.3.1 Common Installation Scenarios

The MAC OS Deployment Agent supports Download Installer deployment and web promotion deployment.

### 2.6.3.1.1 Download Installer deployment

Admin downloads the Agent installation package locally and delivers it to end users for installation and deployment through U disk, network sharing, etc.

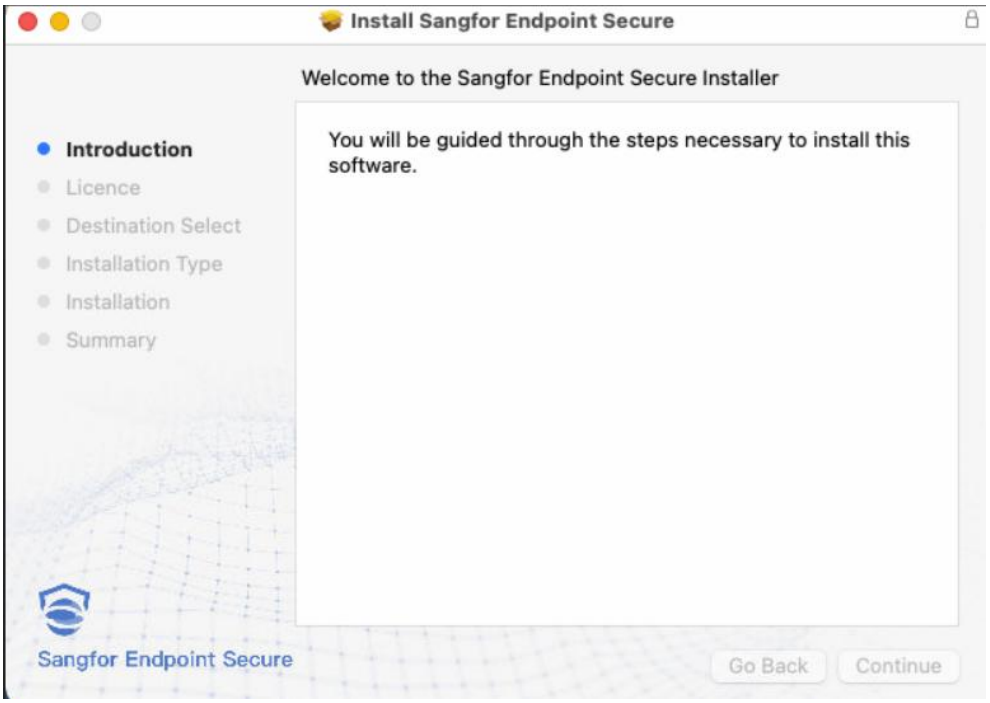
Go to **System > Agent Deployment,** select **MAC, and click View Details of Agent Installation On Physical Machines to** download the installer, as shown in the figure below.

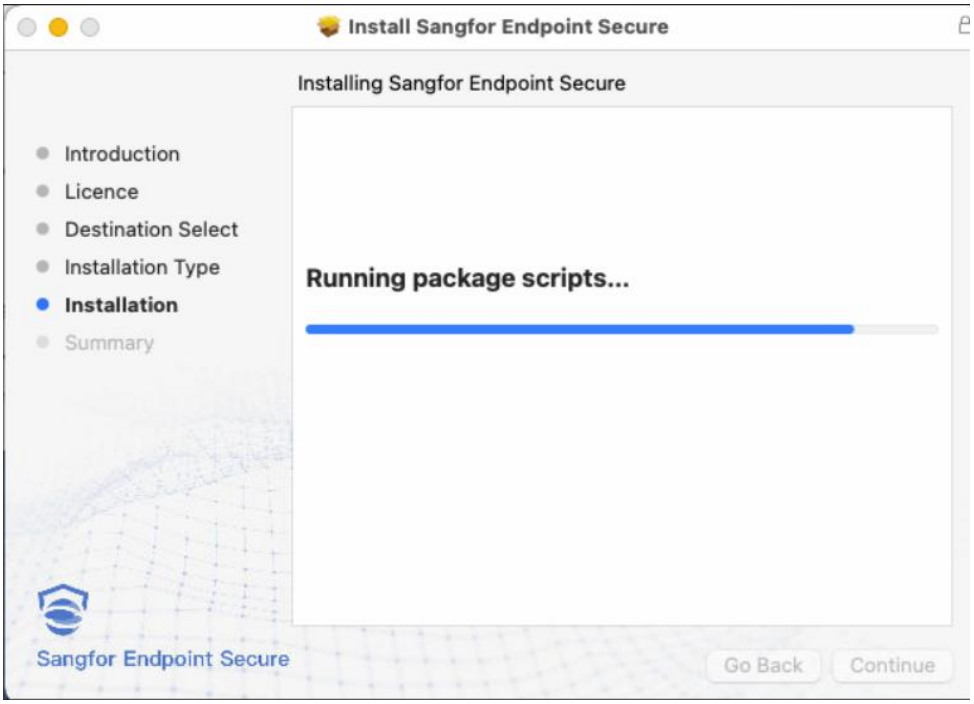


**NOTE**

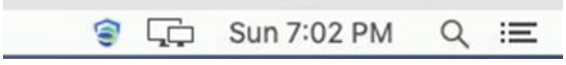
The default name of the MAC client installation program (similar to edr_installer_MGR IP_4430.exe) contains the communication address and port information of NovaGuard Manager. Please do not change the installation program name after downloading.

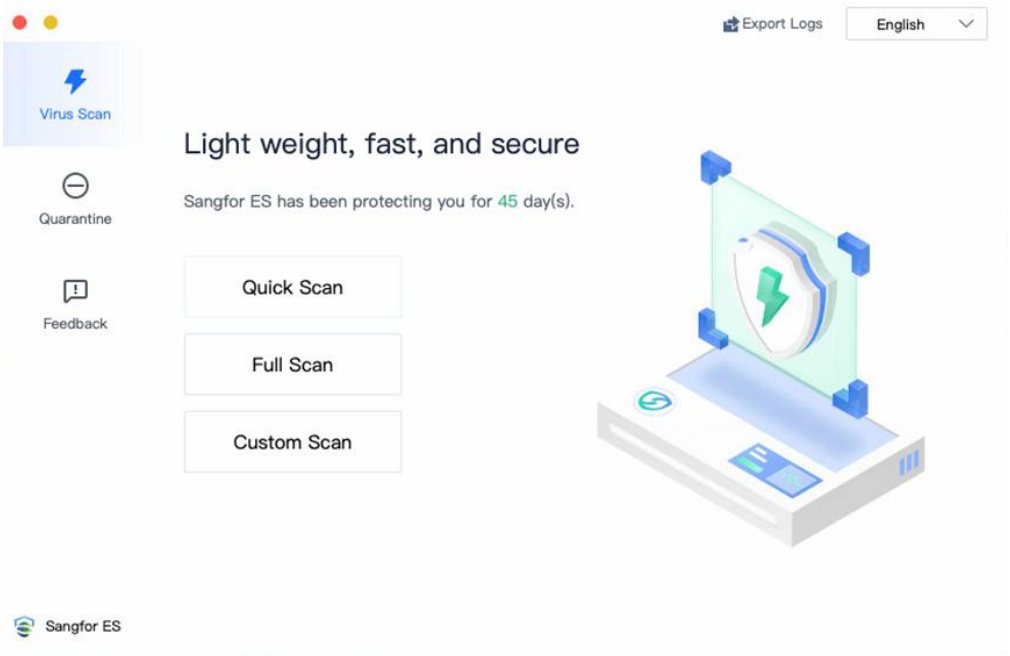
Double-click the installer, as shown in the figure below, and follow the wizard to install it.




After the installation is complete, a ForeNova icon is generated in the MAC OS menu bar, indicating that it has been installed, as shown in the figure below.

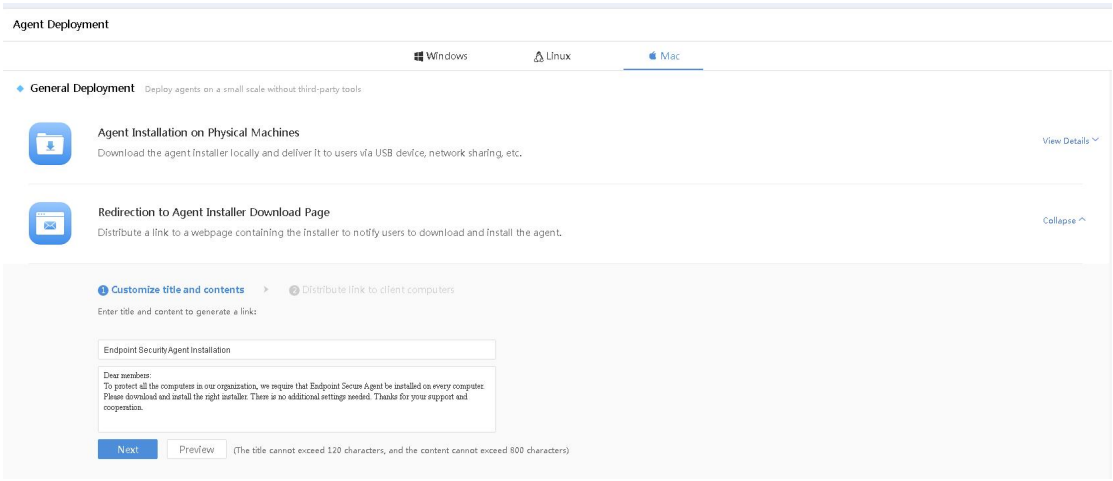




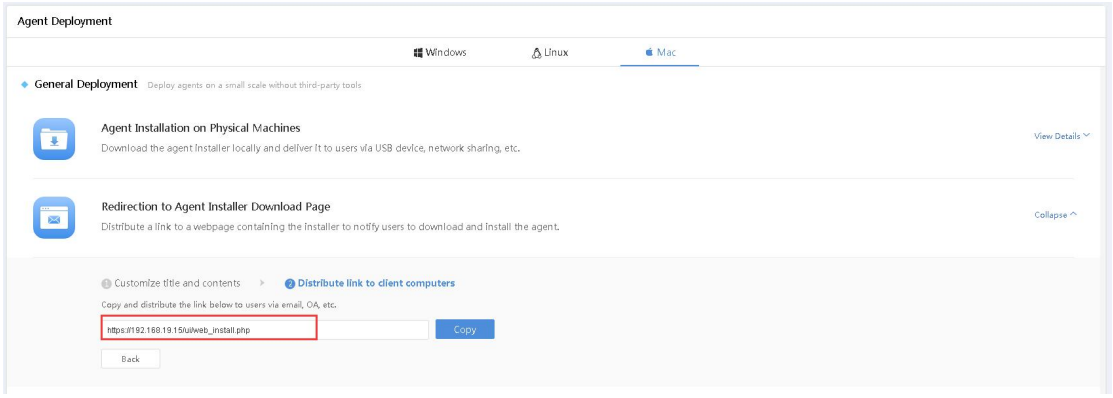

### 2.6.3.1.2 Redirection to Agent Installer Download Page

Admin publishes the deployment notice's web page and sends the publishing page link to the user by email, OA, etc. The user downloads the agent installation package for installation and deployment.

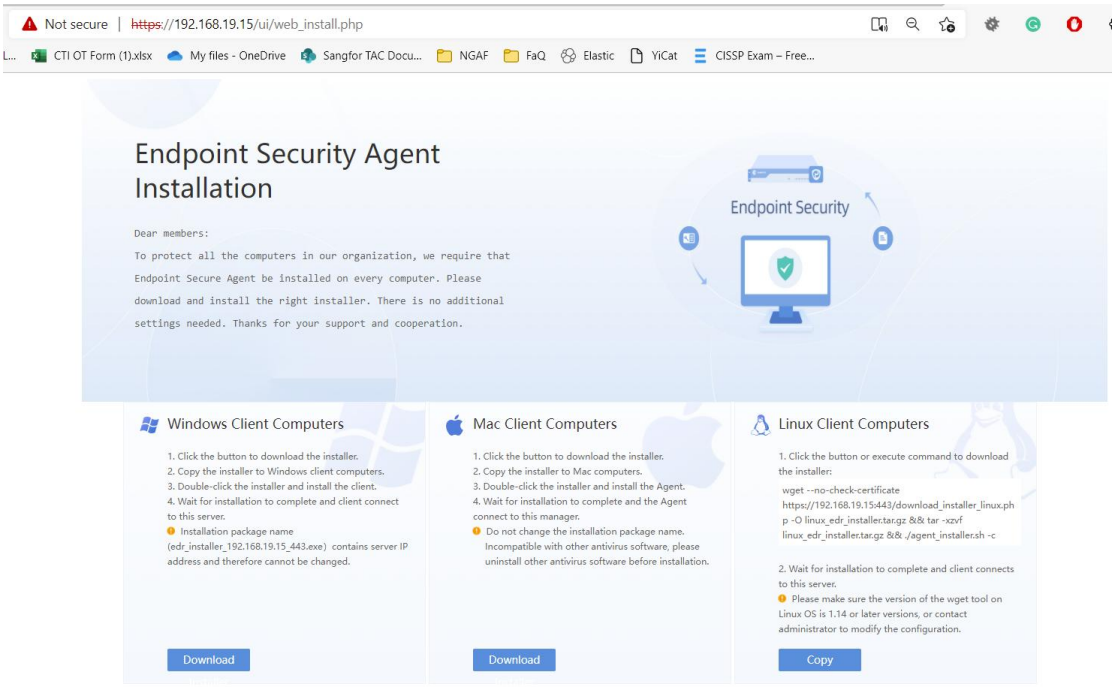
Go to **System > Agent Deployment**, select **MAC**, and open **Redirection to Agent Installer Download Page**, as shown in the figure below.




Edit the title and content of the notification page. Then, click **Next** to generate a download link, as shown below.




Admin sends the download link to the user via email, OA, etc. The user downloads the Agent installation package for installation and deployment, as shown in the figure below.



# 2.7 Agent Uninstallation

## 2.7.1 Uninstallation on the Windows Operating System

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

NOTE

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

## 2.7.2 On Linux Servers

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




## 2.7.3 On the Mac Operating System

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

```
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.    *
*                                              *
************************************************

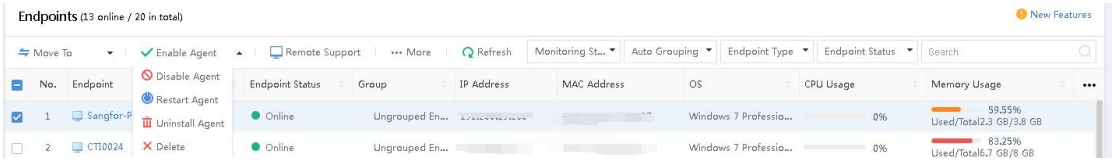
LSSs-Mac:~ root#
```

## 2.7.4 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 the **https://EDR_IP:EDR port number** in the address box, and press **Enter**. The default port number is 443.

**NOTE**

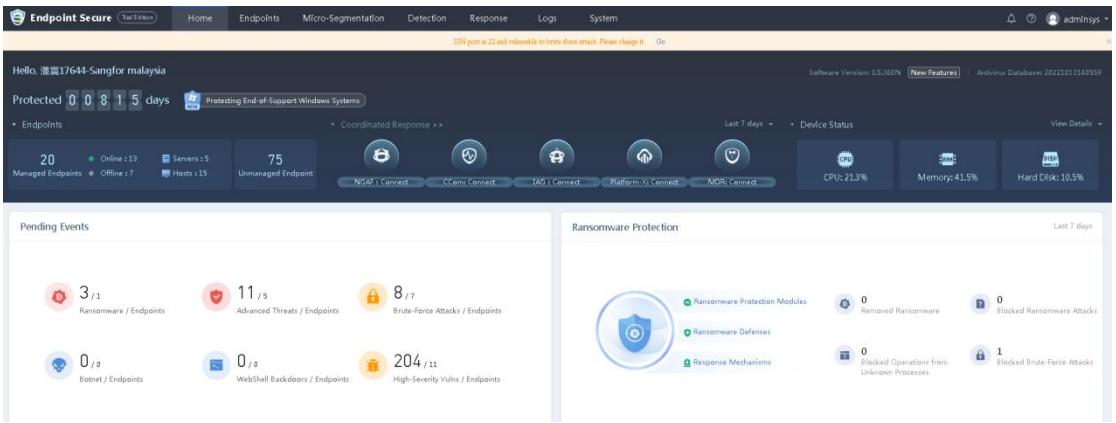
If the message "**The identity of this website or the integrity of this connection cannot be verified**" is displayed, click **Yes**.

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

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

## 3.2 Home Page

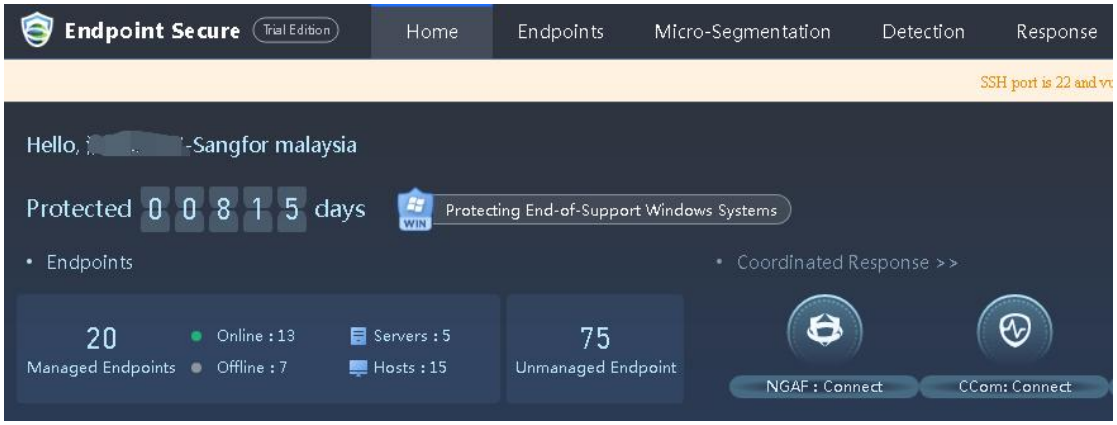
You can view the manager and endpoint running status on the Manager's **Home** page. The **Home** page contains the **Endpoints**, **Pending Events**, **Ransomware Protection**, **Target Endpoints**, **Security Events**, and **Coordinated Response** modules, as shown in the following figure.



## 3.2.1 Endpoints

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

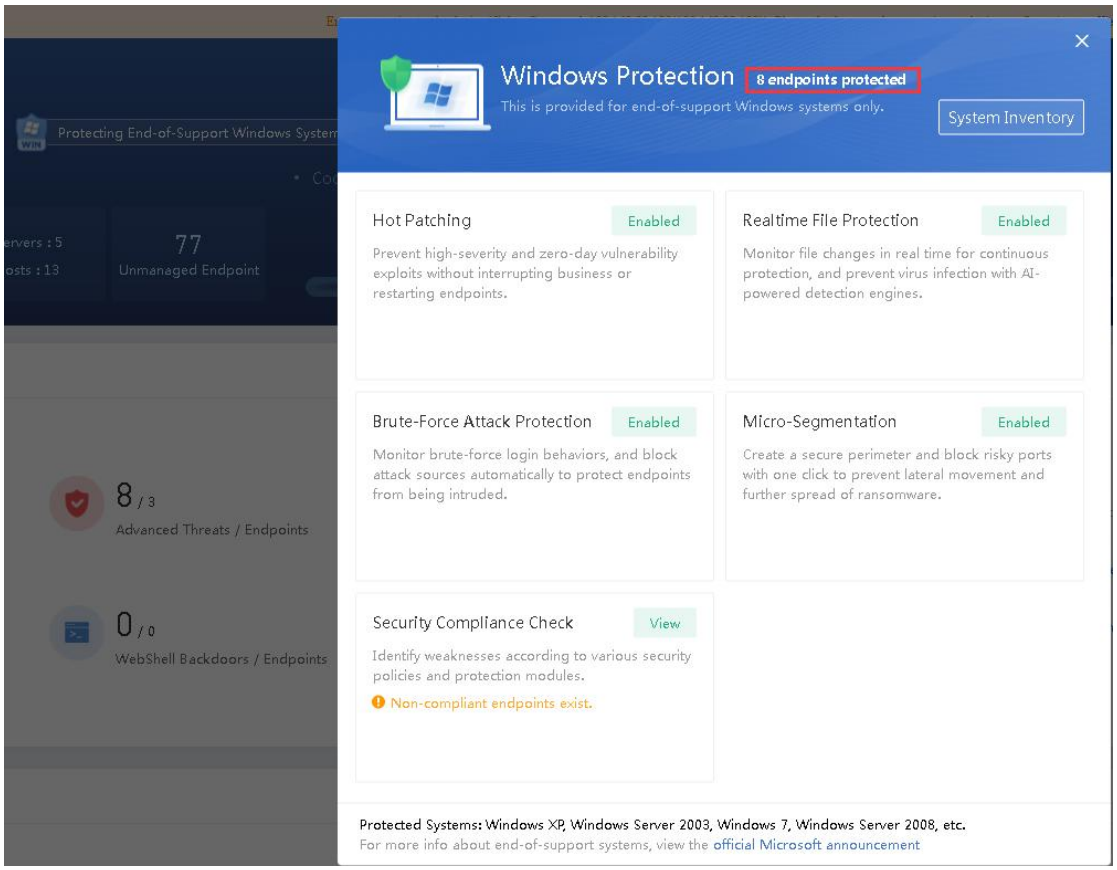
If you click **Managed Endpoints**, the **Groups** page under **Endpoints** is displayed. You can view detailed endpoint information on the Groups page, including the names, statuses, IP addresses, and operating systems.



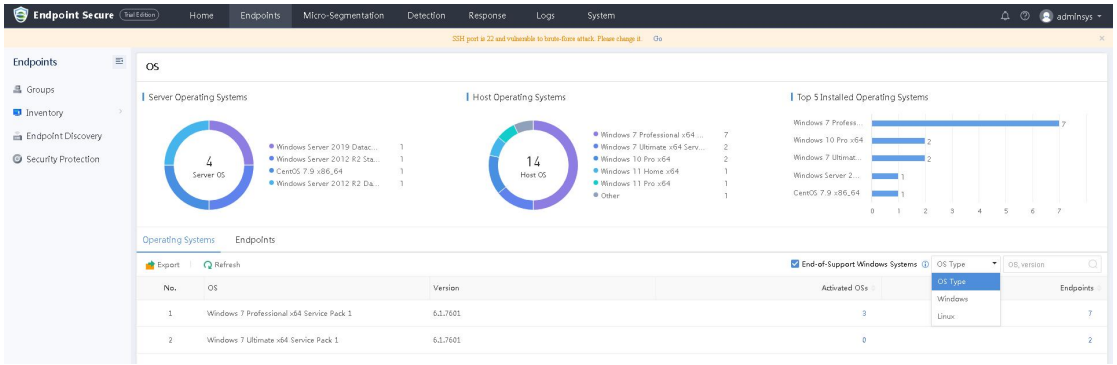

## 3.2.2 Windows Protection

Windows Protection is a dedicated protection plan provided by NovaGuard for Microsoft end-of-support Windows operating systems. This plan allows NovaGuard to provide multiple core functions, such as zero-day vulnerability prevention, file protection, brute-force attack protection, system weakness identification, risky port blocking, and 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. On the **Home** page, click **Protecting End-of-Support Windows Systems** 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 updates, replacement, or endpoint iteration.




3. View the statuses (**Enabled** or **Go**) of protection measures, including **Hot Patching**,

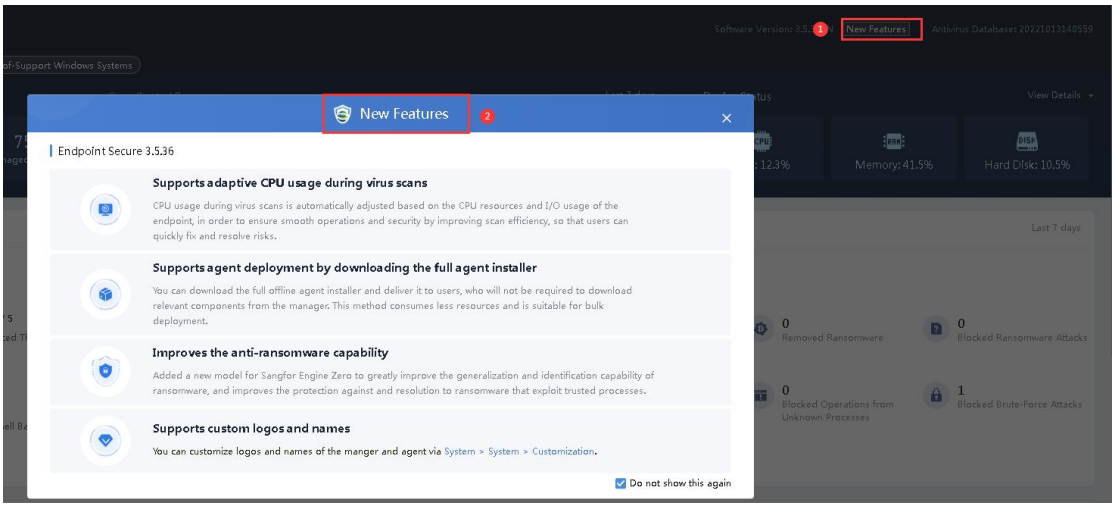
**Realtime File Protection**, **Brute-Force Attack Protection**, **Micro-Segmentation**, and **Security Compliance Check**.

**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** page. On the **Vuln Remediation** page, you can view the details of vuln remediation or disable this function.

- **Realtime File Protection**: This function is an AI-powered multidimensional threat detection mechanism. This function allows NovaGuard 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** page. On the **Realtime Protection** page, you can view the realtime protection details or disable this function.
- **Brute-Force Attack Protection**: This function allows NovaGuard 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** page. On the **Realtime Protection** page, you can view the realtime protection details or disable this function.
- **Micro-Segmentation**: This function allows NovaGuard 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, you can switch the ON button and add micro-segmentation policies under Micro-Segmentation.
- **Security & Integrity Check**: This function allows NovaGuard 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.

## 3.2.2.1 New Features

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




## 3.2.2.2 Banner Reminder

1. ISLP compliance reminder

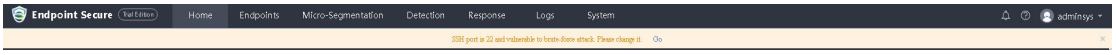
When the ISLP requirements are not met, for example, when the **admin** account has not been disabled or renamed, a banner reminder is displayed, as shown in the following figure.



Click **Go**. 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 to prevent information leakage as the security administrator due to improper permission assignment.

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 **Go** to display the **Advanced** page under **System** > **System** > **Network**. On the

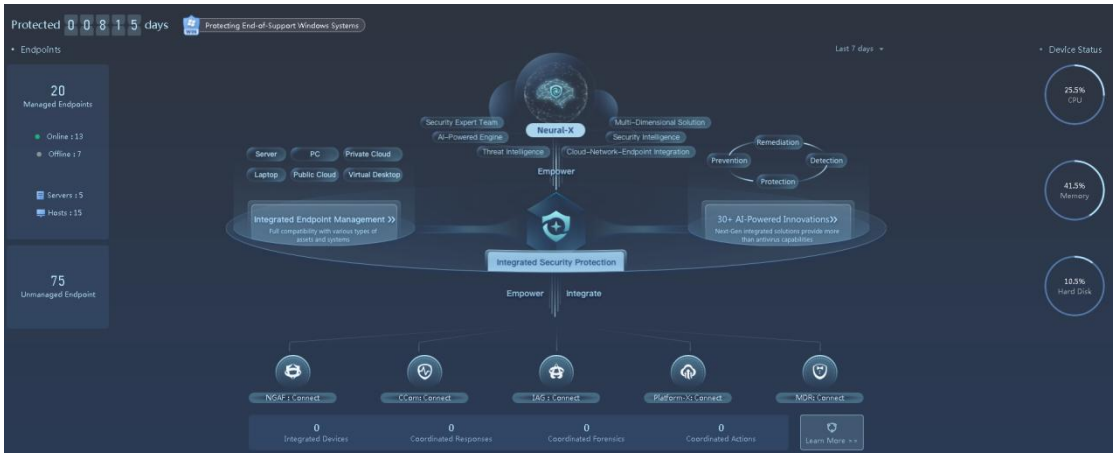
**Advanced** page, change the port number to prevent virus infection due to brute force cracks and ensure system security.

### 3.2.2.3 Coordinated Response

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

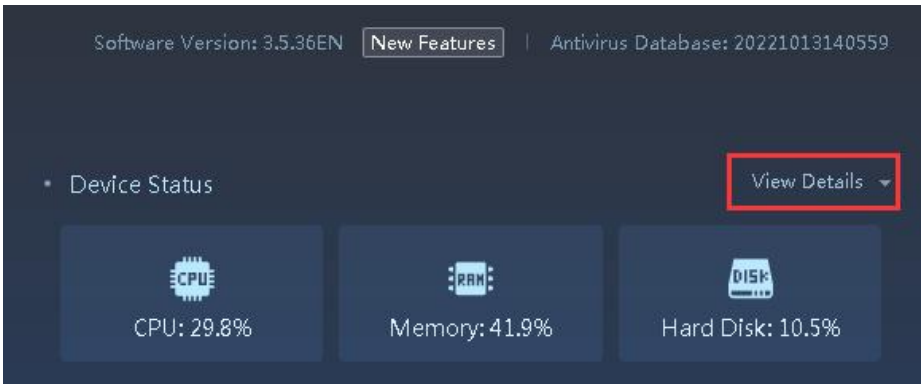



On the **Home** page, you can click the down arrow to view the integration value and overall capability framework of the NovaGuard more intuitively. In the upper right corner, you can select **Last 7 days**, **Last 30 days**, or **Last 90 days** from the drop-down list to view the NovaGuard working status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




### 3.2.2.4 Device Status

The **Device Status** module displays the Manager's CPU, memory, and hard disk usage. 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.

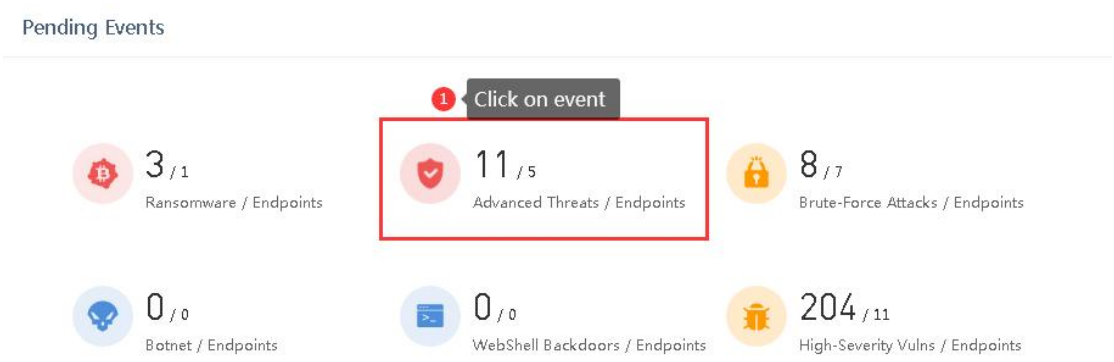


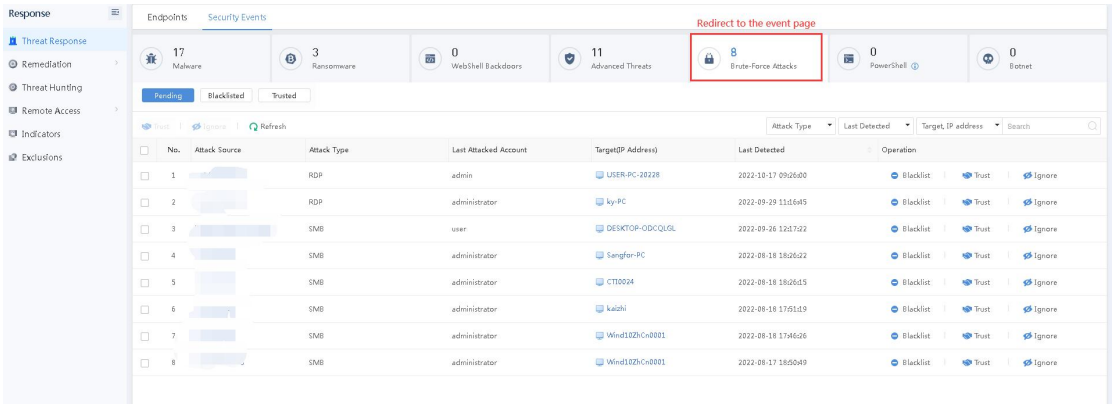




## 3.2.2.5 Pending Events

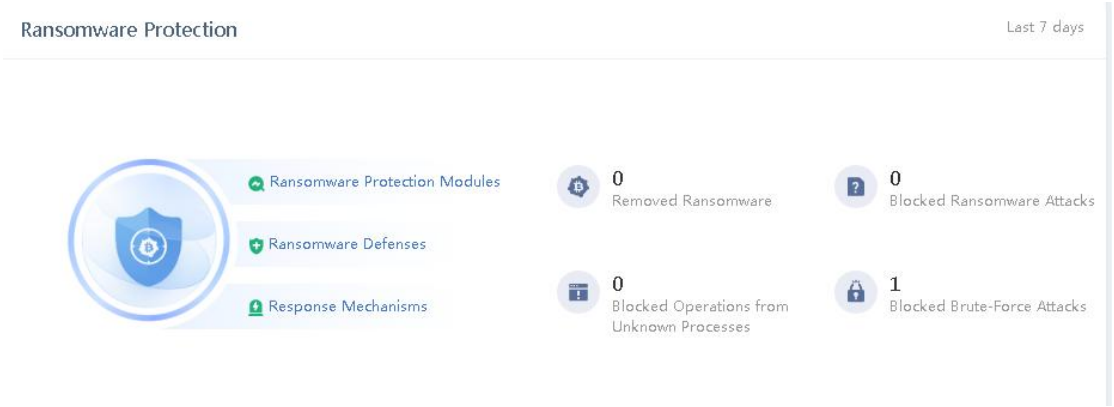
The **Pending Events** module displays the number of pending security events, such as ransomware, brute force attacks, botnets, WebShell backdoors, high-risk vulnerabilities, and the number of endpoints affected by each type of event. You can click on an event. You can view the details about the security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




## 3.2.2.6 Ransomware Protection

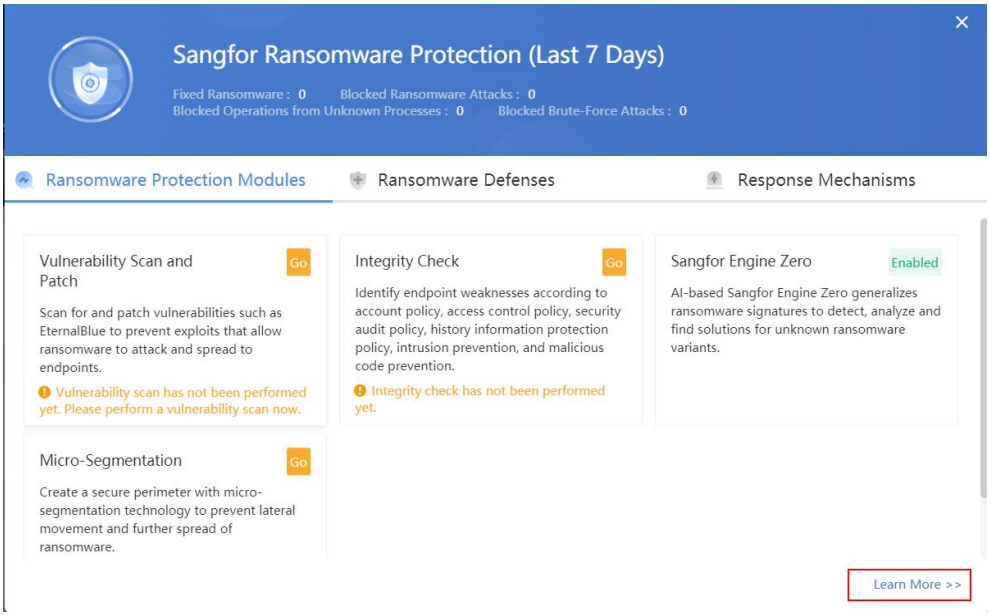
The **Ransomware Protection** module displays **Removed Ransomware**, **Blocked Ransomware Attacks**, **Blocked Operations from Unknown Processes**, and **Blocked Brute-Force Attacks**, as shown in the following figure.



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

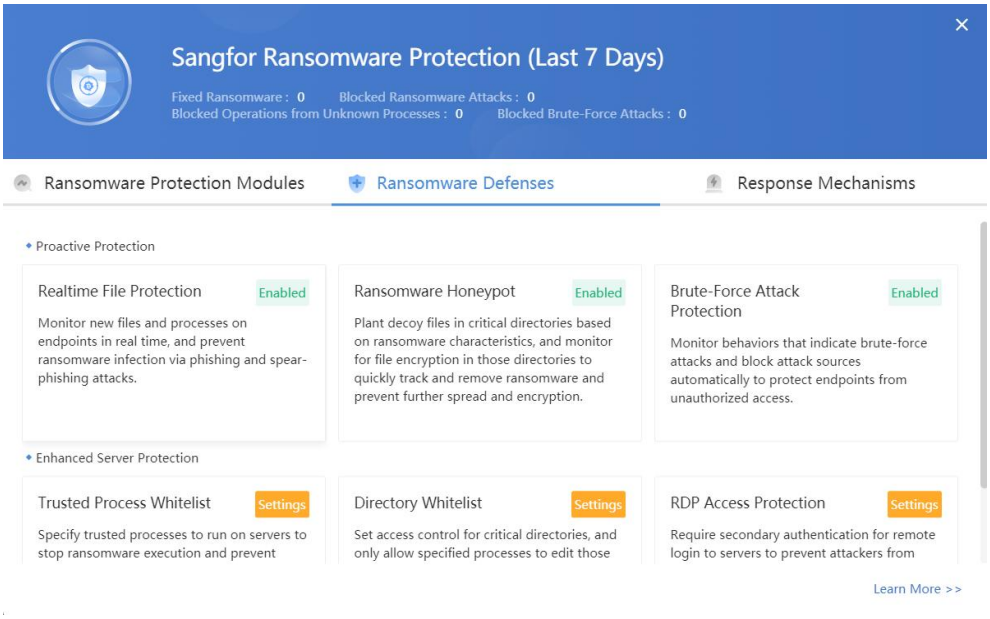



- **Vulnerability Scan and Patch**: This function implements the NovaGuard to scan for and patch vulnerabilities such as EternalBlue with one click. The vulnerabilities can be exploited by ransomware to initiate attacks and spread. You can click it and redirect to the **Vulnerability Scan** page. On the **Vulnerability Scan** page under **Detection**, you can view the scan status, vulnerability quantity, and handling status and create vulnerability scan tasks to scan vulnerabilities.
- **Integrity Check**: This function allows NovaGuard 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 it and redirect to the **Vulnerability Scan** page. On the **Security & Integrity Check**

page under **Detection**, you can view endpoint integrity check details and perform an integrity check for a specified endpoint.

- **Engine Zero**: AI-based Engine Zero generalizes ransomware signatures to detect, analyze, and find solutions for unknown ransomware variants.
- **Micro-Segmentation**: This function allows NovaGuard to create a dynamic security perimeter using the micro-segmentation technology to prevent lateral movement and further ransomware spread.

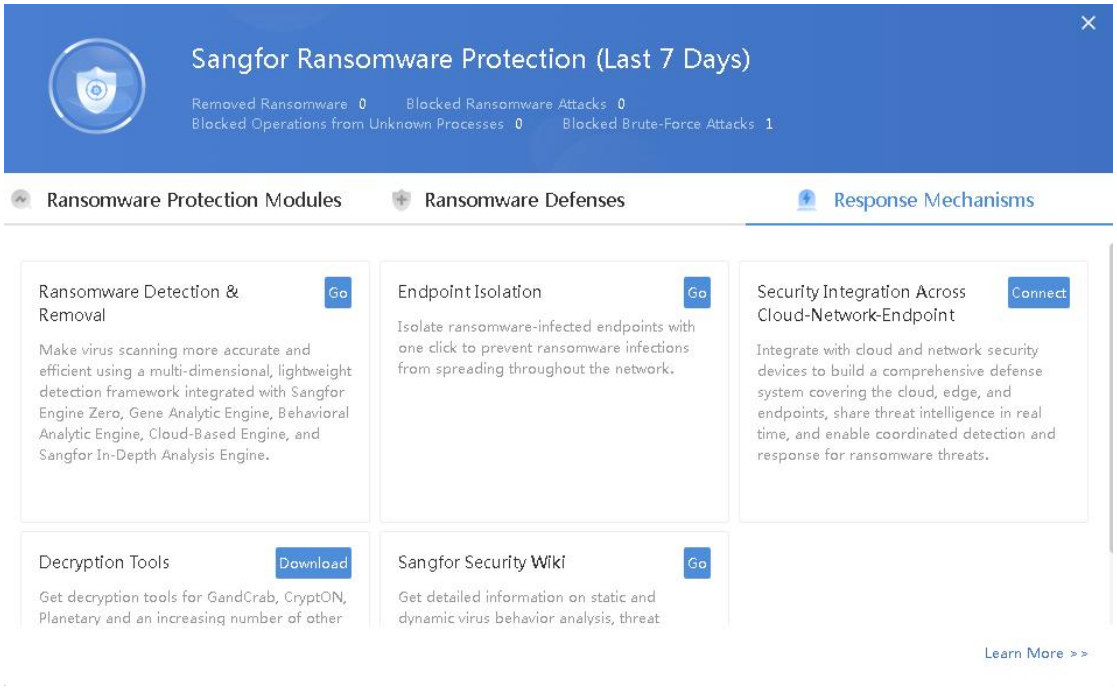
3. The following figure shows **Ransomware Defenses**.




- **Realtime File Protection** (proactive protection): This function allows NovaGuard 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 NovaGuard to plant decoy files in critical directories based on ransomware characteristics. It monitors file encryption and quickly tracks and removes the ransomware to prevent further ransomware spread and encryption.
- **Brute-Force Attack Protection** (proactive protection): This function allows NovaGuard 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 NovaGuard 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 NovaGuard 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.

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

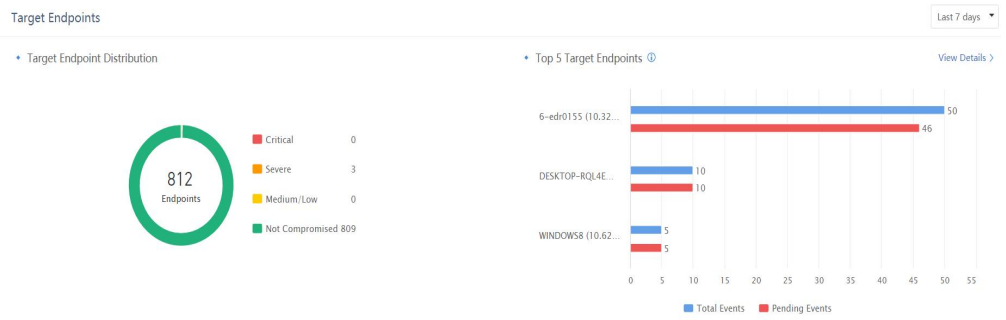



- **Ransomware Detection & Removal**: makes virus scanning more accurate and efficient using a detection framework integrated with Engine Zero, Gene Analysis Engine, Behavior Analytic Engine, Cloud-based Engine, and In-Depth Analysis Engine.
- **Endpoint Isolation**: isolates ransomware-infected endpoints 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.

- **Decryption Tools**: gets decryption tools for GandCrab, CryptON, Planetary, and an increasing number of other ransomware that encrypt your files.
- **ForeNova Security Wiki**: gets detailed information on static and dynamic virus behavior analysis, threat reports, impacts, targeted attack events, and other related threat intelligence.

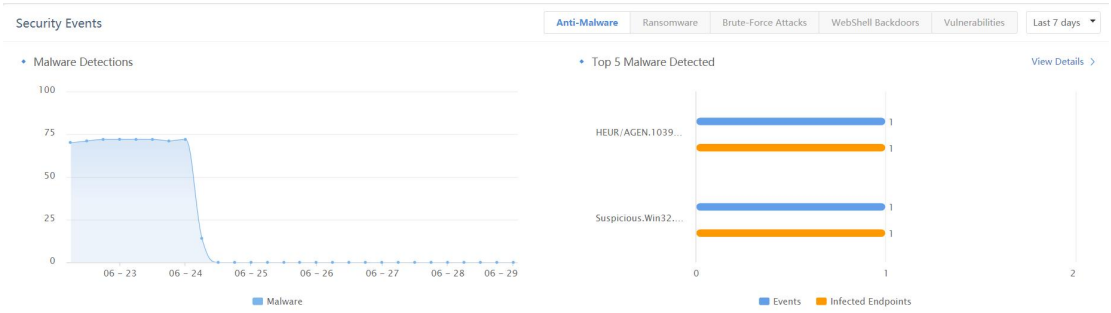
### 3.2.2.7 Target Endpoints

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** list 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**.




### 3.2.2.8 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

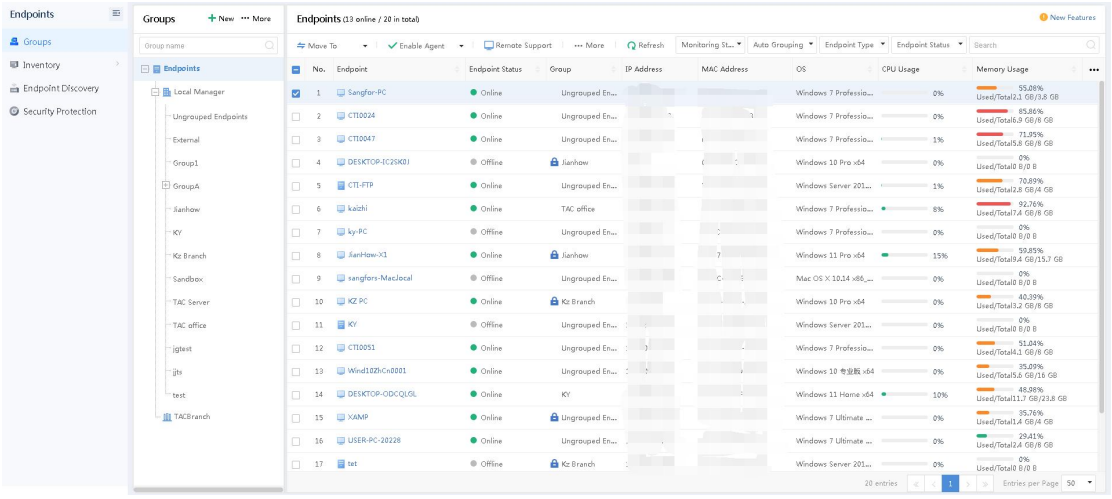
The **Endpoints** page allows you to discover, check, and group endpoints and use policies to manage endpoints and endpoint groups. The policies include **Basic Config**, **Anti-Malware**, **Realtime Protection**, **Anti-Ransomware**, **Trusted Files**, **General Settings**, **Vuln Remediation, Endpoint Control, and Customization**.

## 3.3.1 Groups

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

1. **Endpoint Information Display**

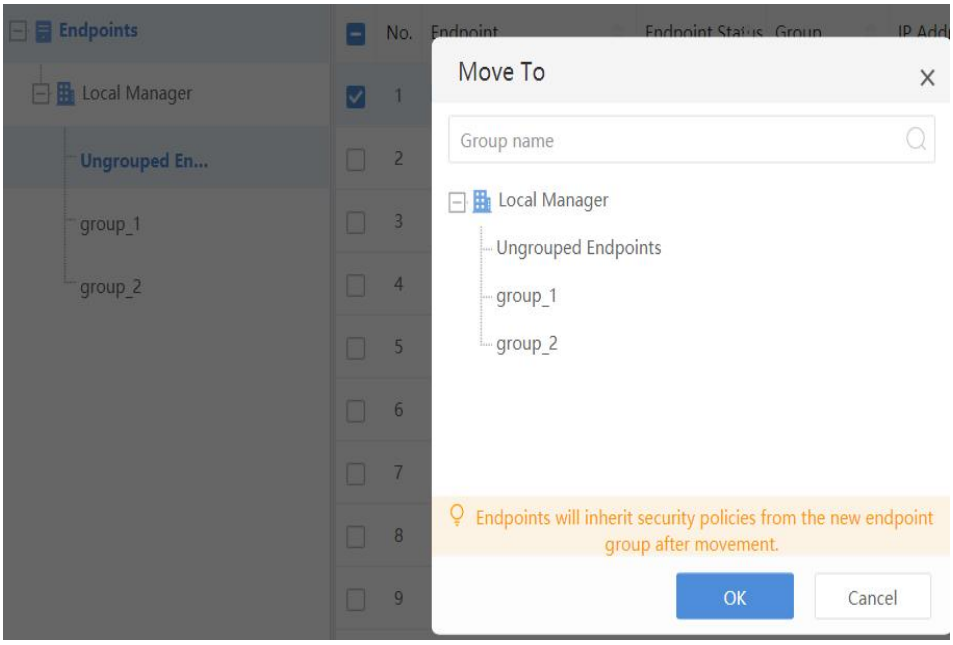
Endpoint information includes the endpoint name, status, group, IP address, MAC address, operating system, CPU usage, memory usage, hostname, asset user, asset number, asset location, monitoring status, and last connected. In addition, you can click **...** on the right to filter and specify display options.



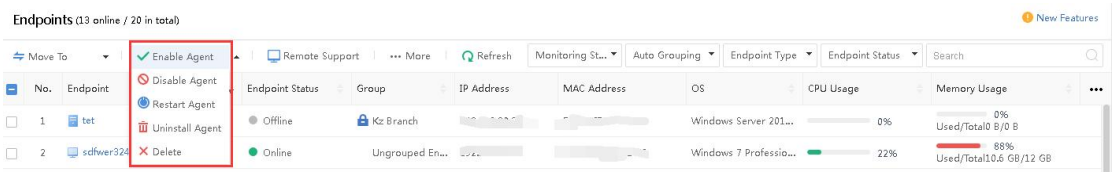

5. **Endpoint Management**

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.

### 3.3.1.1.1 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.

#### 3.3.1.1.2 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.

#### 3.3.1.1.3 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**.
6. Click **Sample File** to download it and edit the file content as instructed.
7. Click **Browse**, select the edited XLS or XLSX file, and upload it.
8. 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.

9. 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**.
10. 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.

### 3.3.1.1.4 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.

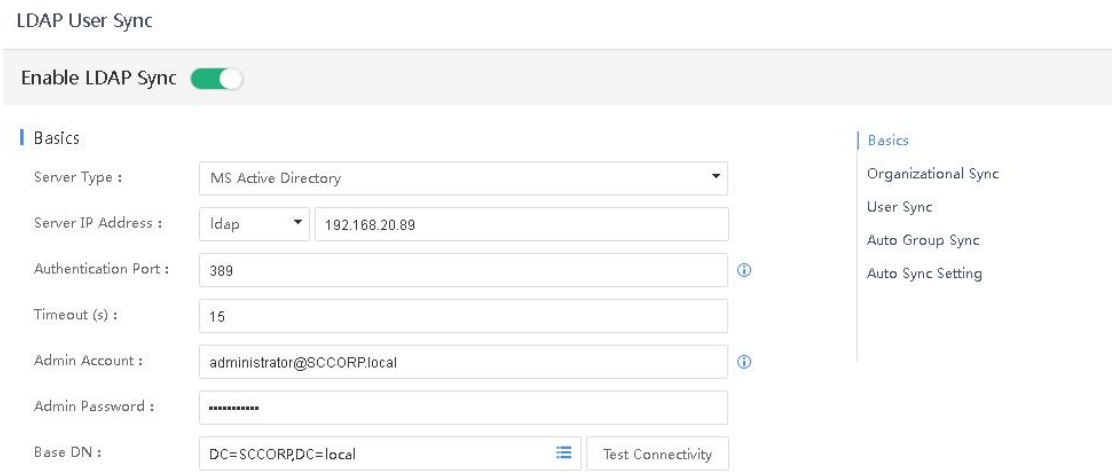
### 3.3.1.1.5 LDAP Sync

The customer's intranet already has an AD domain controller server, and intranet assets are managed uniformly on the AD domain controller server. The administrator needs a way to synchronize the OUs and users specified by the AD domain server to the ForeNova to achieve unified user information management.

**LDAP Sync Configuration**

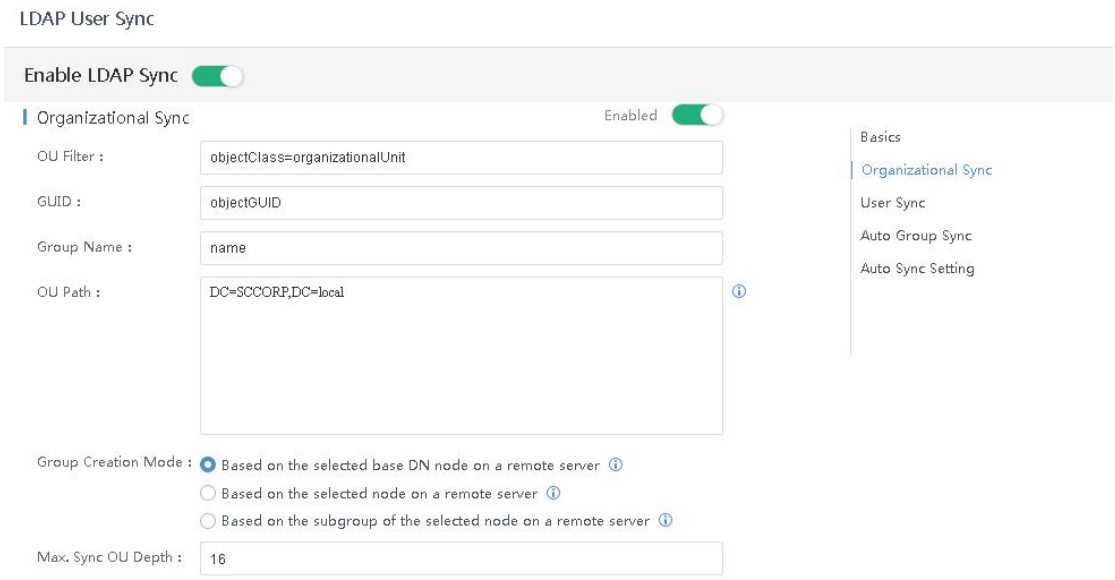
Go to **System > System > LDAP User Sync.**

1. Basic Configuration



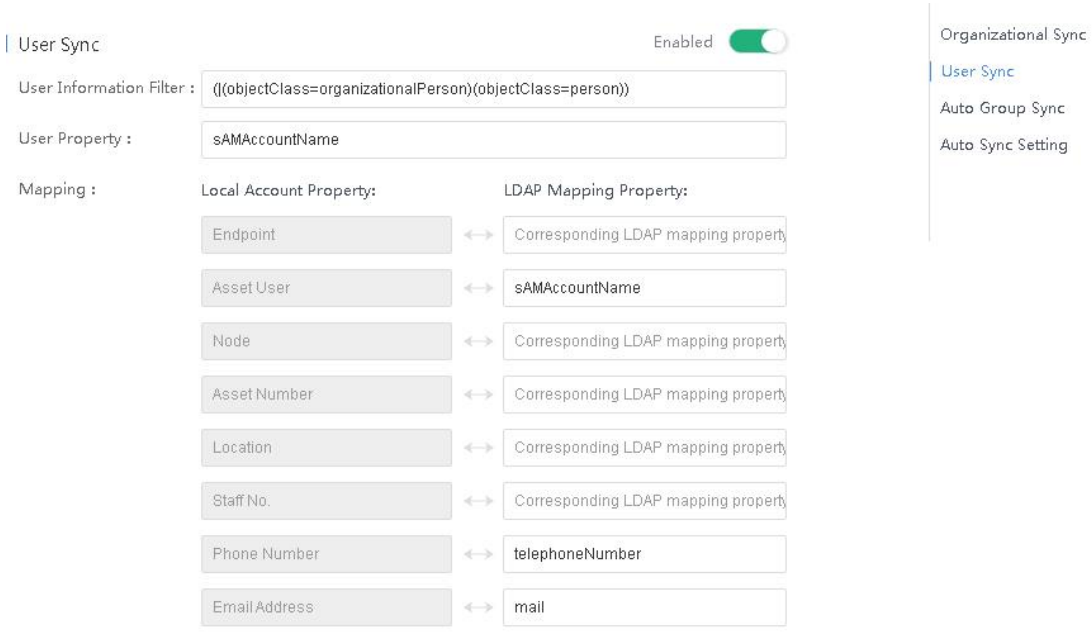

**Basic configuration**: Configure the AD domain controller server IP address, Authentication Port, Admin Account, Admin Password, and Base DN. The administrator account needs to be in the following format, such as administrator@domain.com.

2. **Organizational Sync**




Configure the **OU Path** and the **Group Creation Mode**, and keep the other settings as defaults.

3. **User Sync**




Map domain user attributes to ForeNova management information. The rest keep the default configuration.

### 4. Auto Grouping



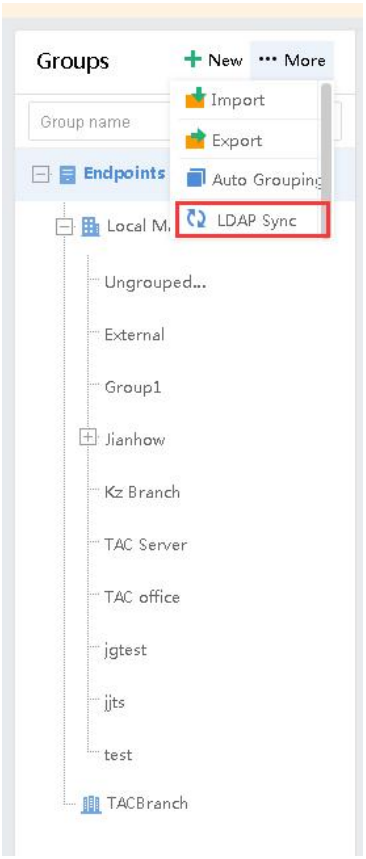

**Auto Group Sync**: Achieve automatic grouping on the NovaGuard management according to the OU where the endpoint account name is located. The endpoint has been logged in with a domain account, and the automatic grouping can be triggered only when the LDAP synchronization is triggered.

### Trigger LDAP Sync

LDAP synchronization can be triggered by manual synchronization or auto synchronization.

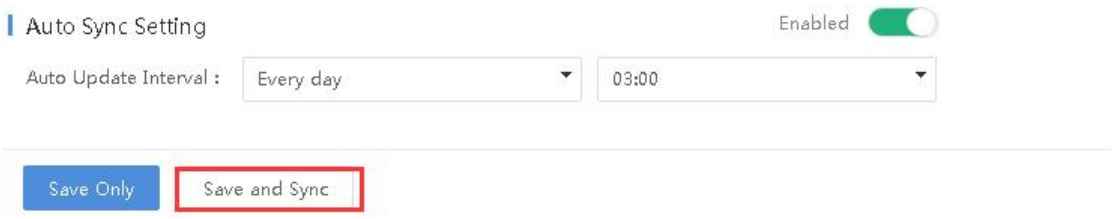
#### 1. Manual Trigger

Go to **Endpoints > Groups > More, and** click **LDAP Sync** to trigger an immediate sync manually, as shown below.




### 2. Auto Sync

Enable **Auto Sync setting**. Real-time synchronization will start when you click **Save and Sync**.

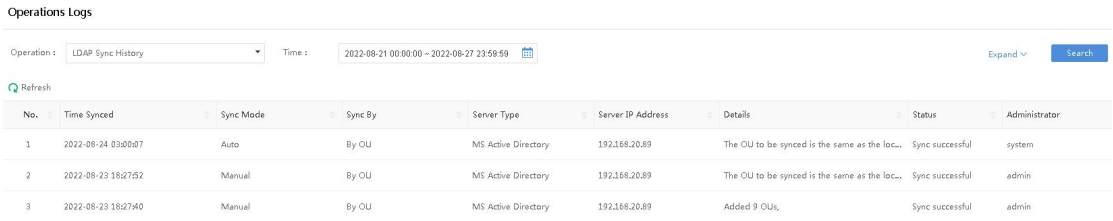



### LDAP Sync Result

The domain OU is synchronized to the endpoint group page, as shown in the figure below. When the agent is installed on an endpoint and logged in with a domain account, it will automatically go online to the group where the domain controller OU is located.




View **Logs > Operation Logs** to view the details of LDAP synchronization history, as shown in the following figure.



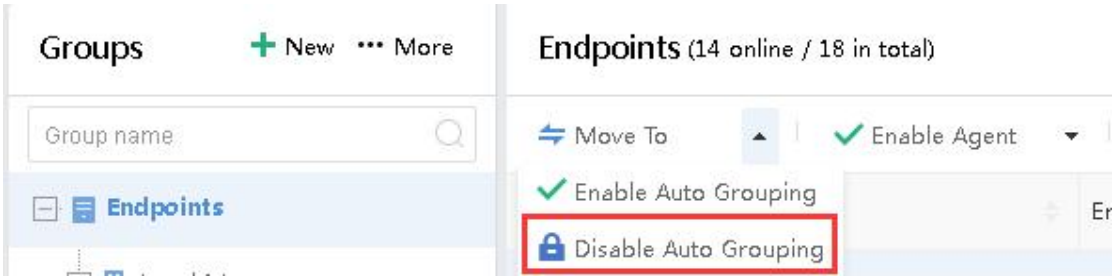

### 3.3.1.1.6 User Selects Online Group

In the multi-branch scenario, there is an IP conflict between endpoints in different branches, and the endpoint cannot go online automatically to the group to which it belongs based on the IP address. There is no AD domain control environment. At this point, the end user can select the group to which it belongs.

**Configuration**

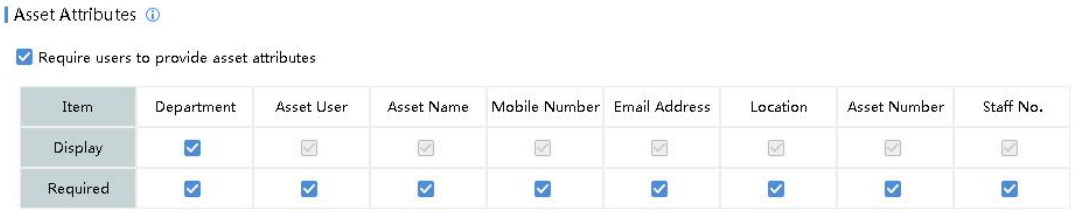
**1. Create or import new group**

Go to **Endpoints > Groups,** and move the mouse to the drop-down list of **Move To** to disable automatic grouping by IP, as shown below.



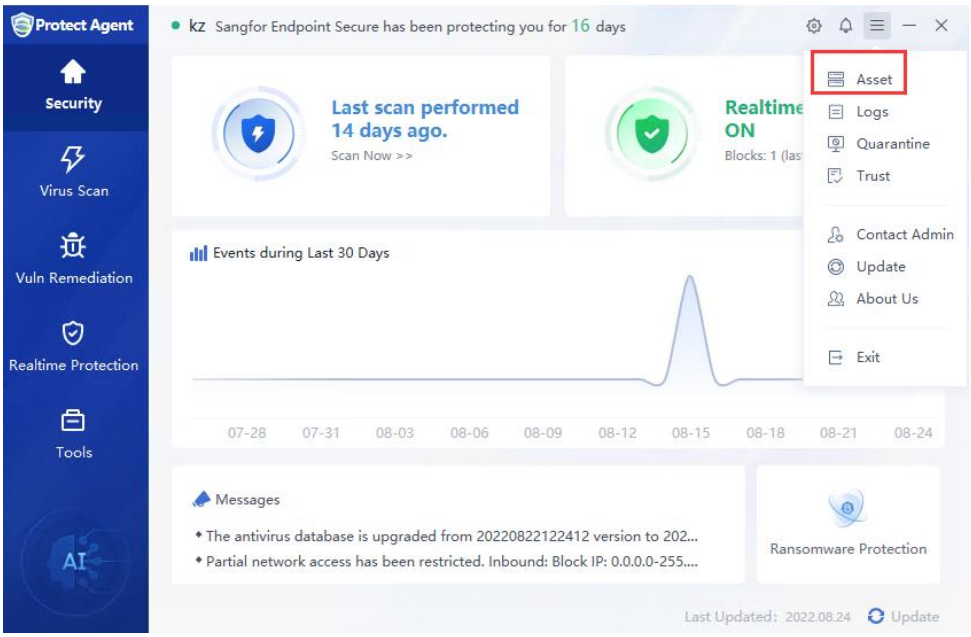

**2. Enable Asset Attributes**

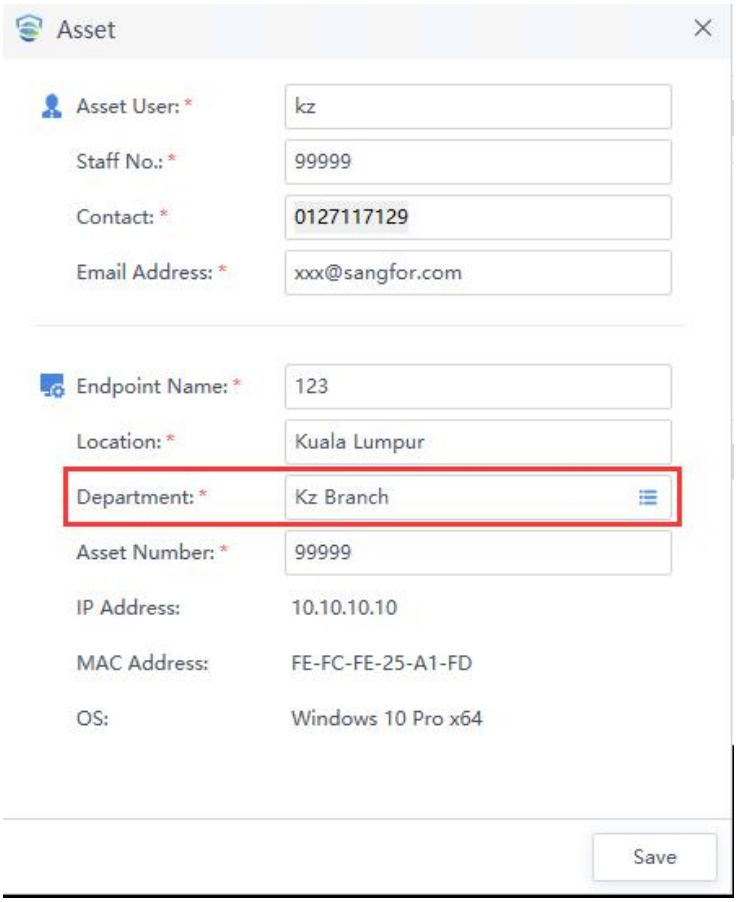
Go to **Endpoints > Security Protection > Basic Config**, enable asset attributes, and select **Display** and **Required**, as shown in the figure below.




**3. User select online group**

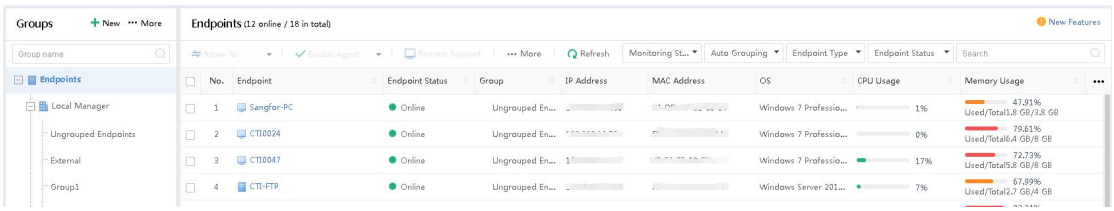
When installing the Agent for the first time on the endpoint and registering the asset attributes or modifying them after installation, you can set the **department** to which it belongs, as shown in the figure below.



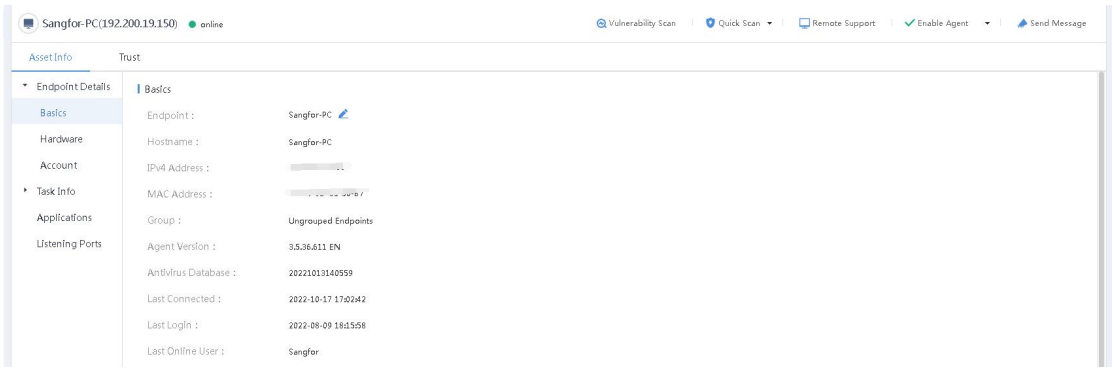

## 3.3.1.2 Endpoint Information Display

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.




### 3.3.1.2.1 Basics

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

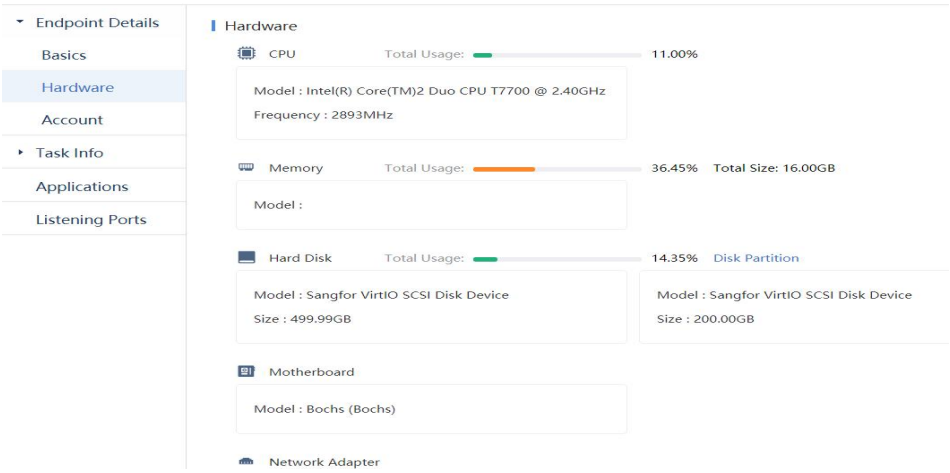
**Basic information**: includes the endpoint name (editable), hostname, IPv4 address, MAC address, group, Agent version, antivirus database version, last connected time, last login time, and last online user.

**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.

### 3.3.1.2.2 Hardware

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

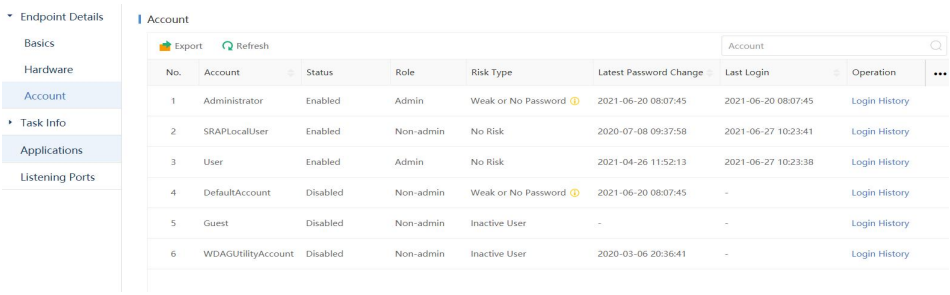



### 3.3.1.2.3 Account

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.

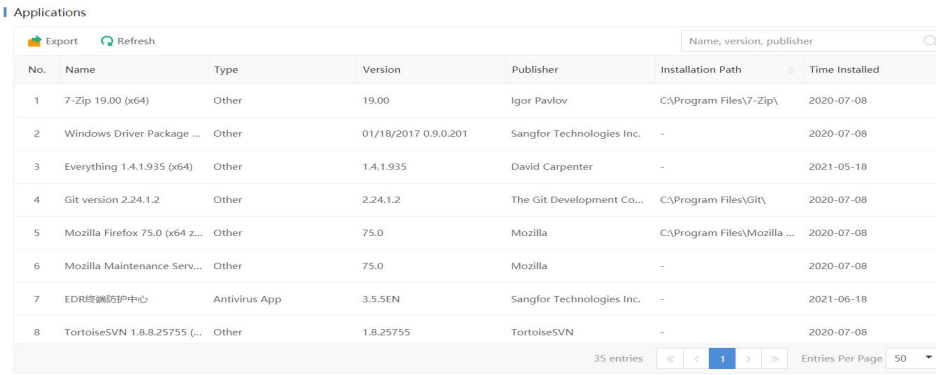



### 3.3.1.2.4 Task Info

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

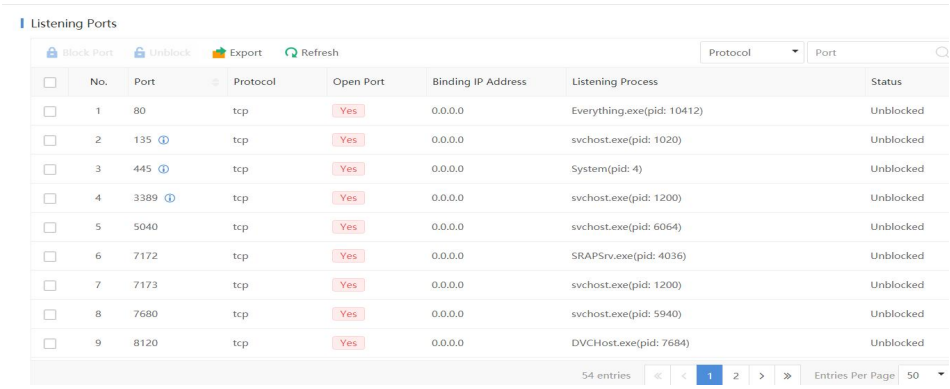
### 3.3.1.2.5 Applications

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.



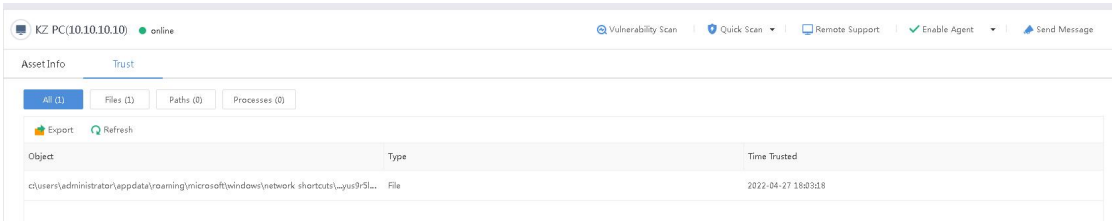

### 3.3.1.2.6 Listening Ports

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.



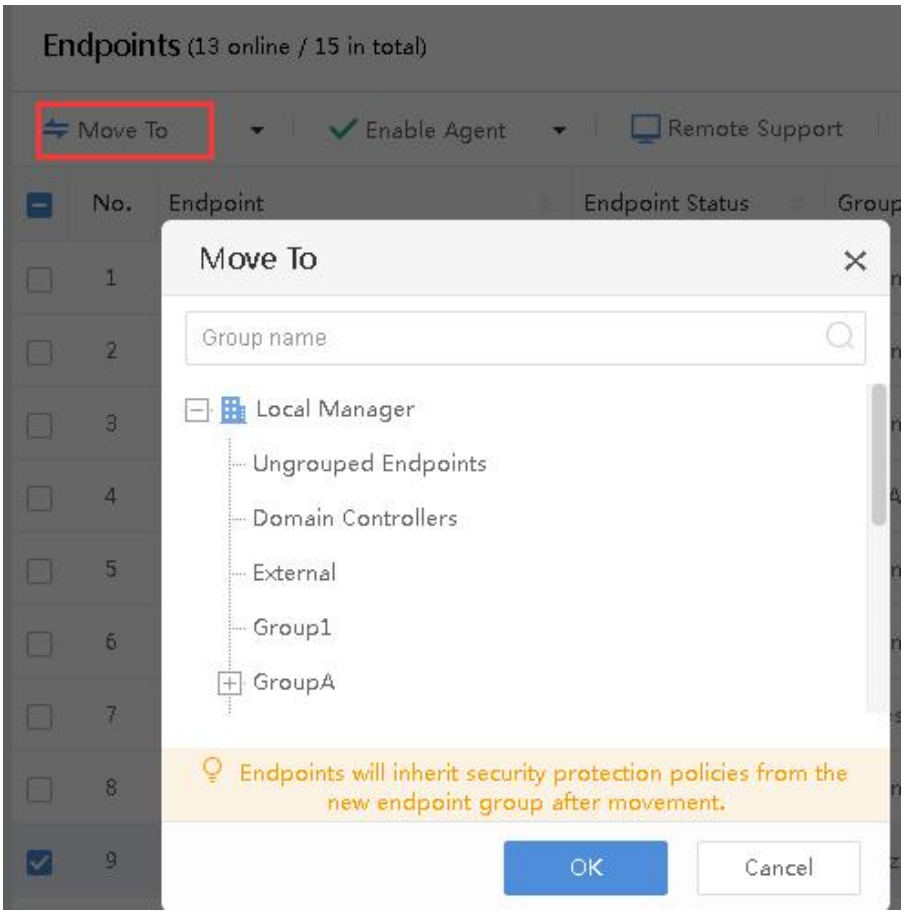

### 3.3.1.2.7 Trust

You can view the trust file or trust directory on the ForeNova manager added by the client on the client side to prevent the endpoint from adding some files unreasonably, and the administrator does not know it, which will eventually lead to an attack. You may navigate to **Endpoints > Group**, click a **selected endpoint** > **Endpoints Details > Trust** to view the trust file added by the endpoint, as shown in the figure below.




### 3.3.1.2.8 Move To

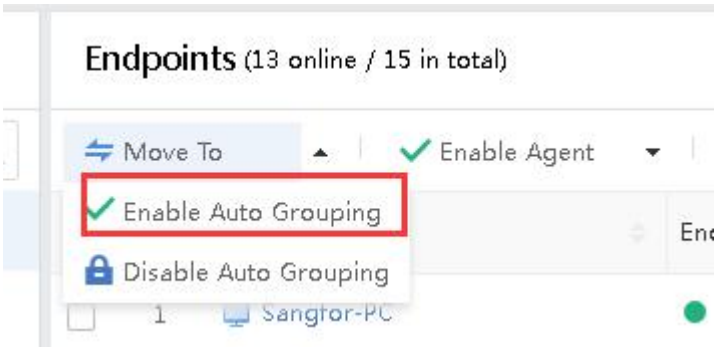
For an online endpoint, you can manually adjust its grouping through **Move To,** as shown in the figure below.




When the automatic grouping according to IP function is enabled, the endpoint whose group is manually moved and adjusted will be automatically marked with an icon, indicating that the group to which the endpoint belongs is locked and will not be automatically grouped according to IP again, as shown in the figure below.



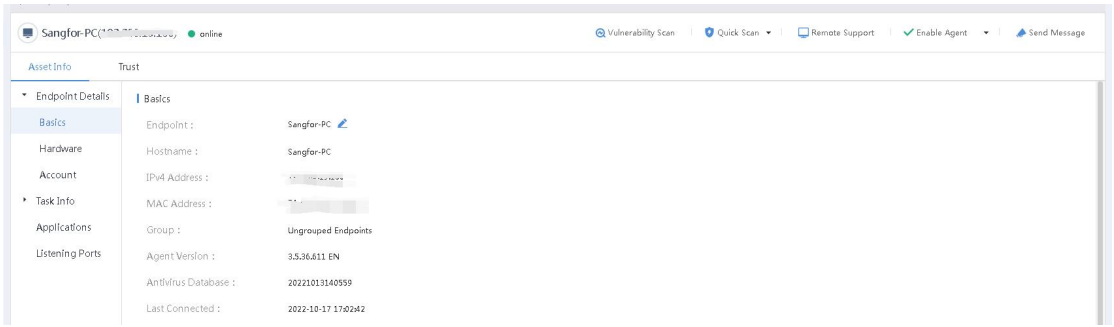

You can select the endpoint and click **Enable Auto Grouping** to enable this feature, as shown in the figure below.




## 3.3.1.3 Remote Endpoint Management

### 3.3.1.3.1 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 NovaGuard Manager.

**NOTE**

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

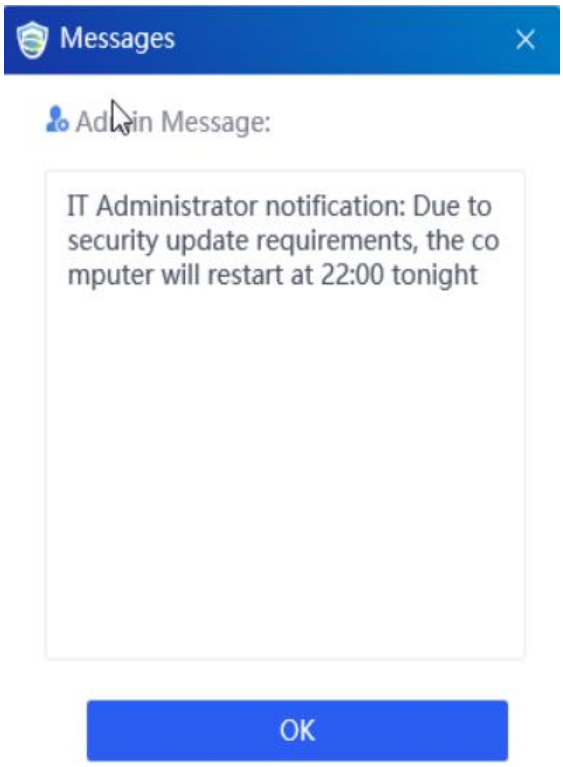
To release a license, uninstall the Agent from an endpoint and delete the endpoint from the NovaGuard Manager.

### 3.3.1.3.2 Send Message

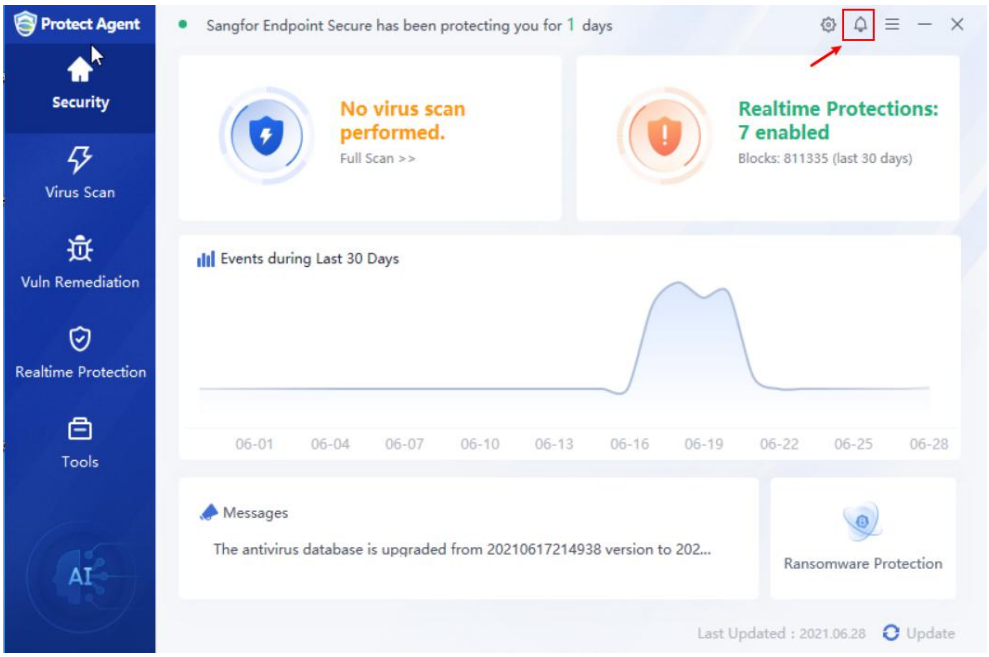
On the **Endpoints** page, you can select one or more endpoints with the Agent installed and send messages to these endpoints. The procedure is as follows:

3. Choose **Endpoints** > **Group**, select one or more endpoints, and click **Send Message** in the status bar.

4. On the **Send Message** page, complete the information editing and click **OK**. The following figure shows that selected endpoints will receive the corresponding message.



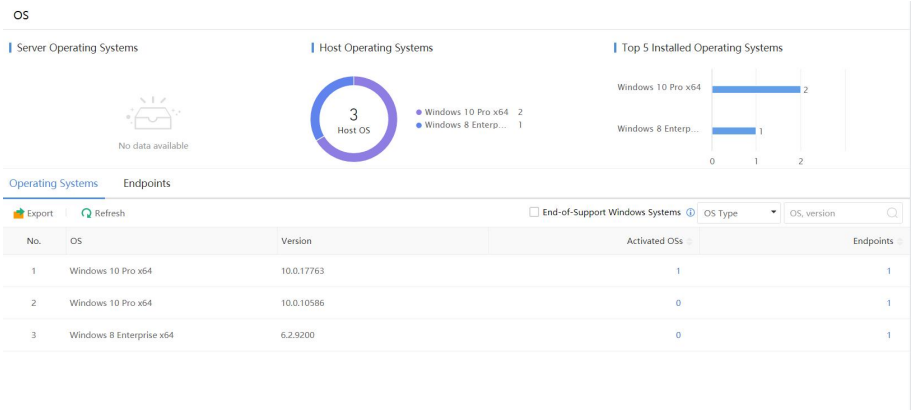

5. Click **OK** or **X** in the upper-right corner of the endpoint to close the message. You can click the **Messages** icon in the following figure to view historical messages.


Protect Agent
Security
Virus Scan
Vuln Remediation
Realtime Protection
Tools
AI
Sangfor Endpoint Secure has been protecting you for 1 days
No virus scan performed.
Full Scan >>
Realtime Protections: 7 enabled
Blocks: 811335 (last 30 days)
Events during Last 30 Days
06-01
06-04
06-07
06-10
06-13
06-16
06-19
06-22
06-25
06-28
Messages
The antivirus database is upgraded from 20210617214938 version to 202...
Ransomware Protection
Last Updated : 2021.06.28
Update

## 3.3.2 Inventory

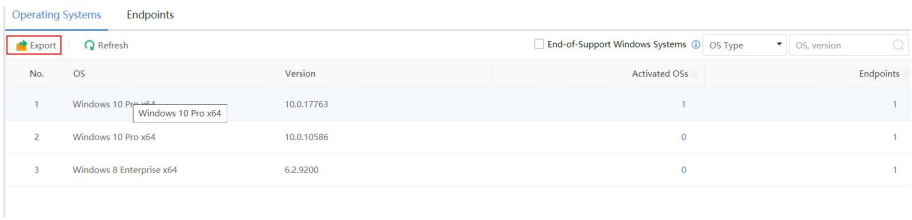
The **Inventory** module checks endpoints on the entire network and displays endpoint statistics. It includes the **OS**, **Applications**, **Listening Ports**, **Users, Database Apps, Websites, Web Frameworks, Web Services, and Web Apps**. However, endpoint inventory data does not contain Mac endpoints because Mac endpoint information is not collected.

### 3.3.2.1 OS

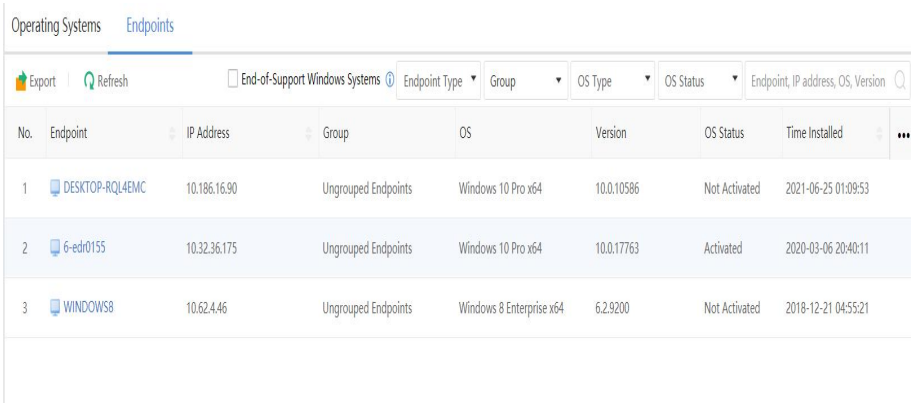



The **OS** page displays the distribution of operating system versions of endpoints on the entire network, as shown in the preceding figure.

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 **OS** page, 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.



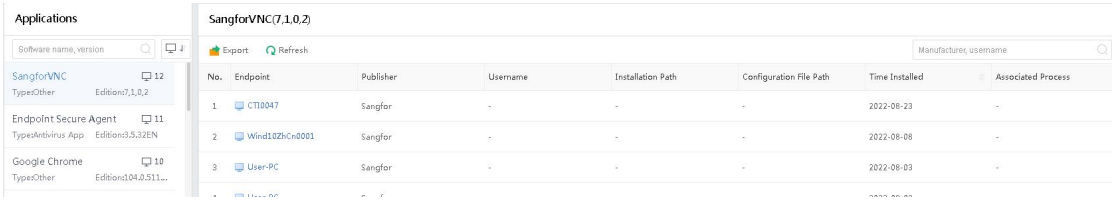

NOTE

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.

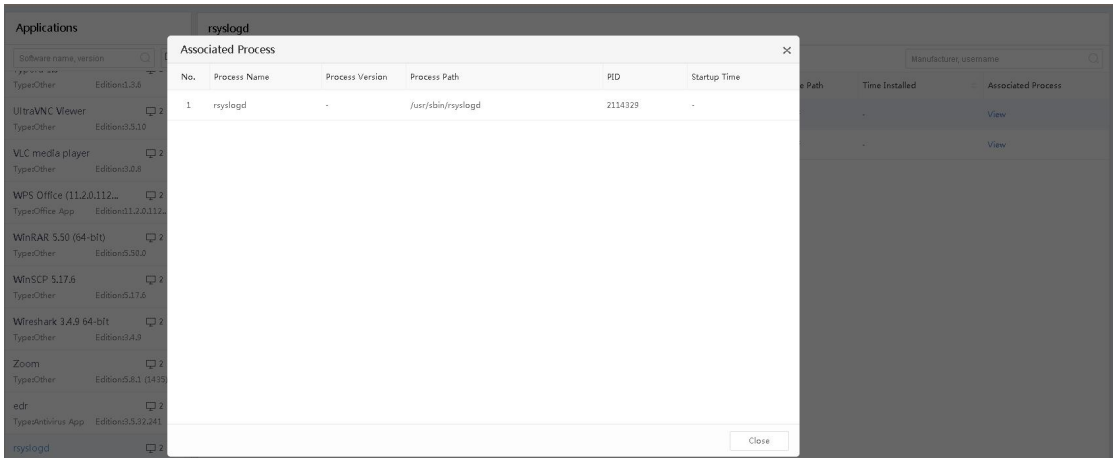
## 3.3.2.2 Applications

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



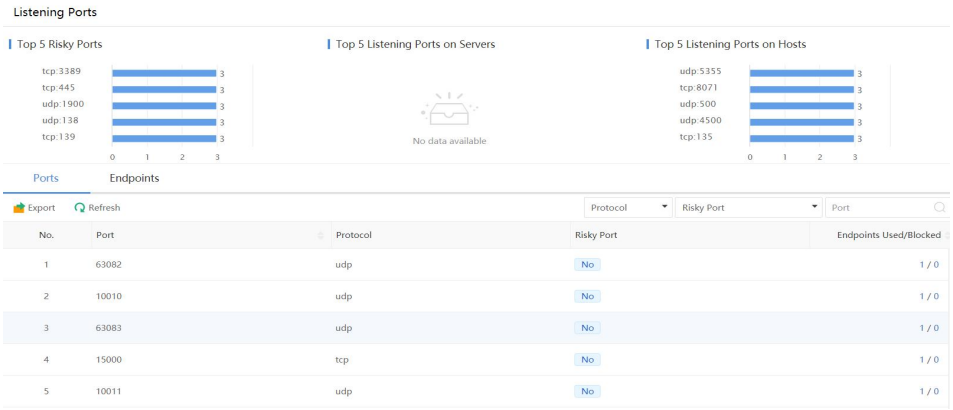

As shown in the figure above, it will display the endpoint distribution of the application software in the whole network, sort the installation amount from most to least, and count the number of endpoints.

You can view the associated process information of the software corresponding to the endpoint.



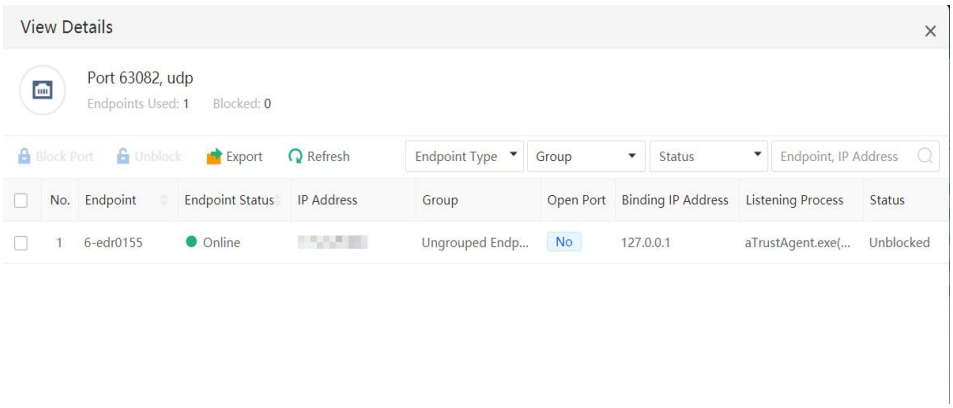

It supports application searching through the **software name** and **version** search box and supports designated endpoint searching through the **Publisher** and **username**.

## 3.3.2.3 Listening Ports




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

1. Detailed information includes the top 5 risky 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.

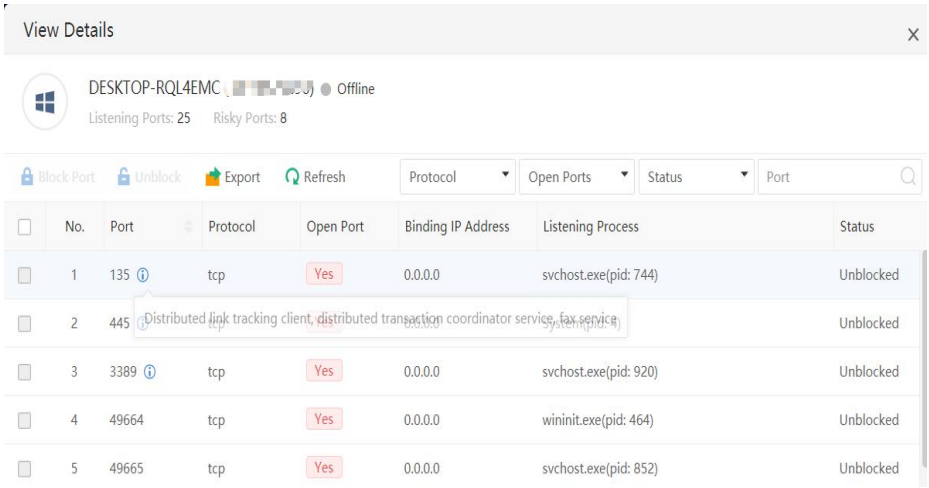



NOTE

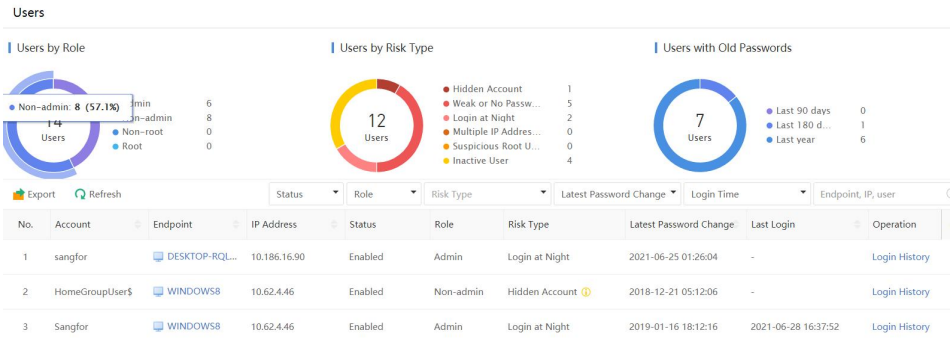
**Block Port**: You can select endpoints for which a port needs to be blocked and click **Block Port** to block the port for the selected endpoints. You can click **Unblock** to unblock a blocked port.

**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 endpoint group. 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.

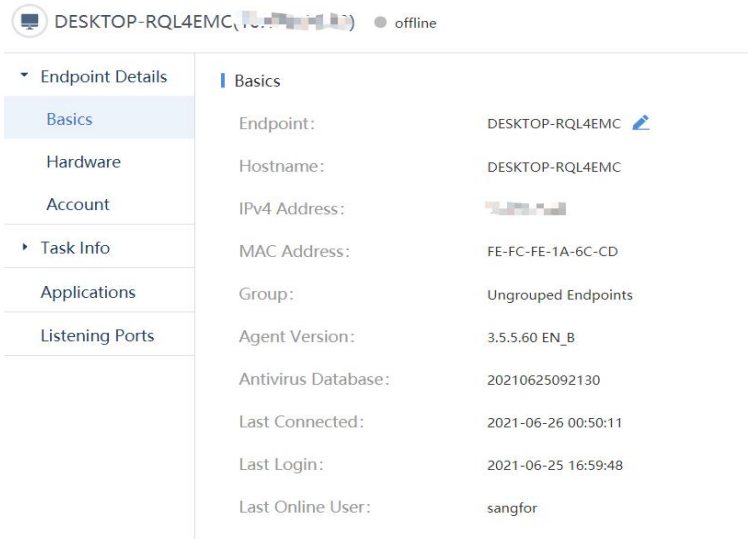


## 3.3.2.4 Users

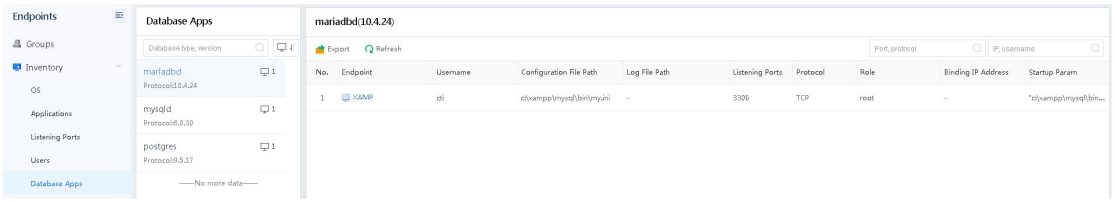



The **Users** page displays the account information of hosts on the entire network, including the account status, account type, role, and password status. Based on account information, the Manager further analyzes risks and provides account risk notifications, such as hidden accounts, weak passwords, suspicious root users, inactive users, logging 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, risk type, password change, etc.
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.



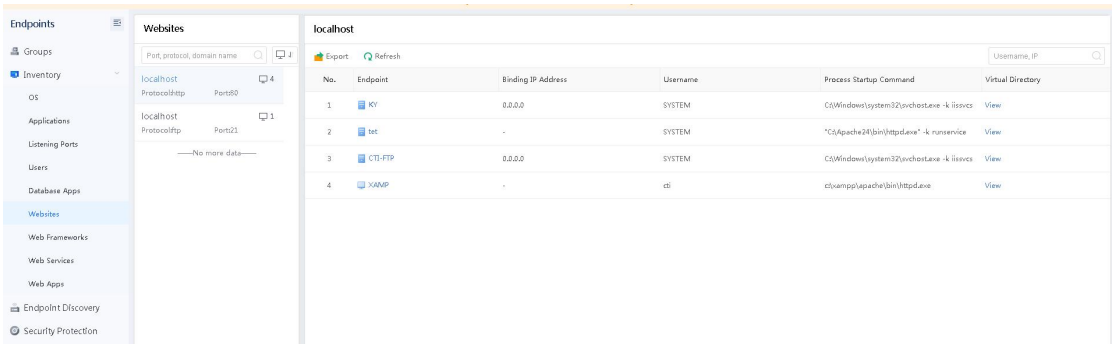
## 3.3.2.5 Database Apps




The database apps page can display the summary and detailed information of the entire network host installation database to conduct a network-wide investigation further and take security measures such as version upgrades or application reinforcement. As shown in the figure above, the main page information includes the following:

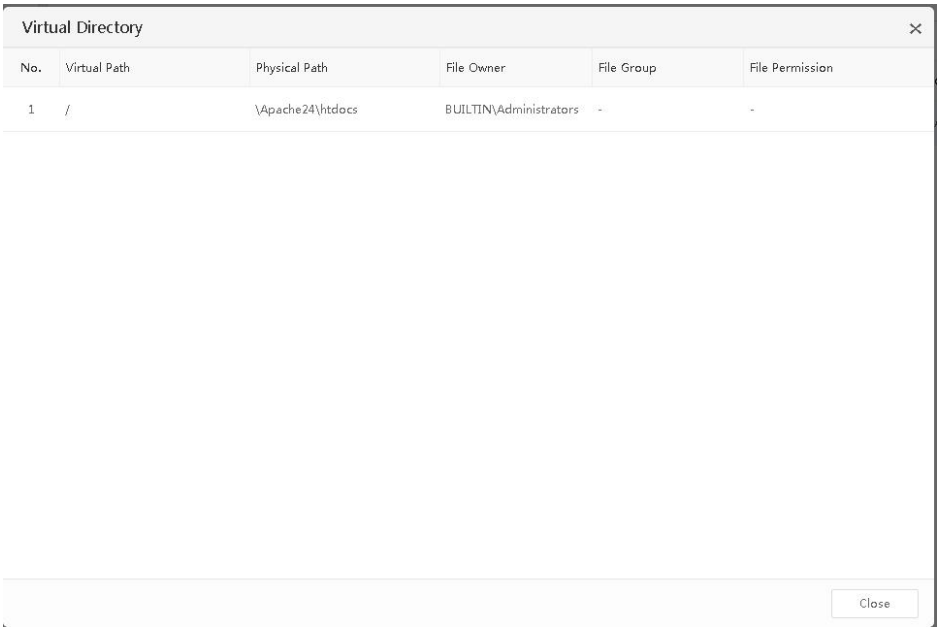
1. It can display the endpoint distribution of the entire network database, sort according to the number of installations from most to least, and count the number of endpoints.
2. Support to search the database through the database type and version search box, and support to search the specified endpoint through port/protocol, binding IP/running user.

## 3.3.2.6 Websites




The website's inventory page can display the summary and detailed information of the entire network host installation website, as shown in the figure above. The main page information includes:

1. It can display the endpoint distribution of the entire website, sort according to the number of installations from most to least, and count the number of endpoints.
2. It can display the virtual directory list of the endpoint corresponding to the website.



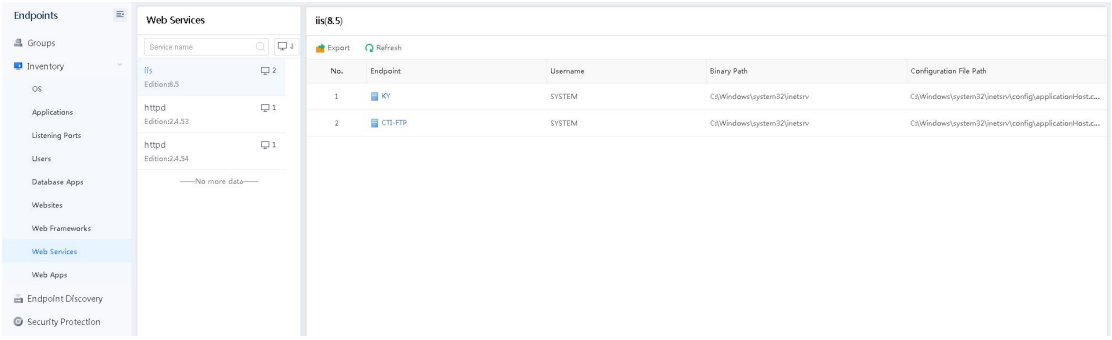

3. Support to search websites through the port, protocol, domain name search box, and support to search for the specified endpoint by username and IP.

## 3.3.2.7 Web Frameworks

The web framework inventory page displays the summary and detailed information of the entire network host installation web framework. The main page information includes:

1. It displays the endpoint distribution of the whole network web framework, sort according to the number of installations from most to least, and counts the number of endpoints.
2. Supports searching of web frameworks through the framework name/language search box and supports searching of specified endpoints through service type.

## 3.3.2.8 Web Services



The web service inventory page can display the summary and detailed information of the web service installed on the whole network host, as shown in the figure above. The main page information includes:

1. It displays the endpoint distribution of web services in the whole network, sorts according to the number of installations from most to least, and counts the number of endpoints.
2. Support searching of web services through the service name search box.

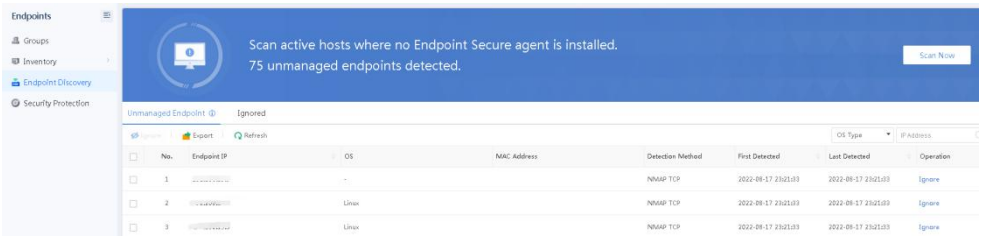
### 3.3.2.9 Web Apps

The web application inventory page can display the summary and detailed information of web applications installed on the whole network host, as shown in the figure above. The main page information includes: The main page information includes:

1. It can display the endpoint distribution of web applications in the whole network, sort according to the number of installations from most to least, and count the number of endpoints.
2. It can display the plug-in information of the endpoint corresponding to the web application.
3. Support searching of web applications through the application name search box.

## 3.3.3 Endpoint Discovery

The endpoint discovery function can proactively detect the intranet and identify uncontrolled endpoints (ForeNova client is not installed) in the intranet to achieve efficient intranet security weak point detection, network-wide asset detection, and timely prevention, as shown in the following figure.




1. After clicking **Scan Now** and completing the scan parameter settings, the intranet scan will be performed. The scan parameters include the following:

**Device:** You can set the NovaGuard Manager to initiate scanning or the Linux endpoint that

has installed the NovaGuard client to initiate scanning.

NOTE

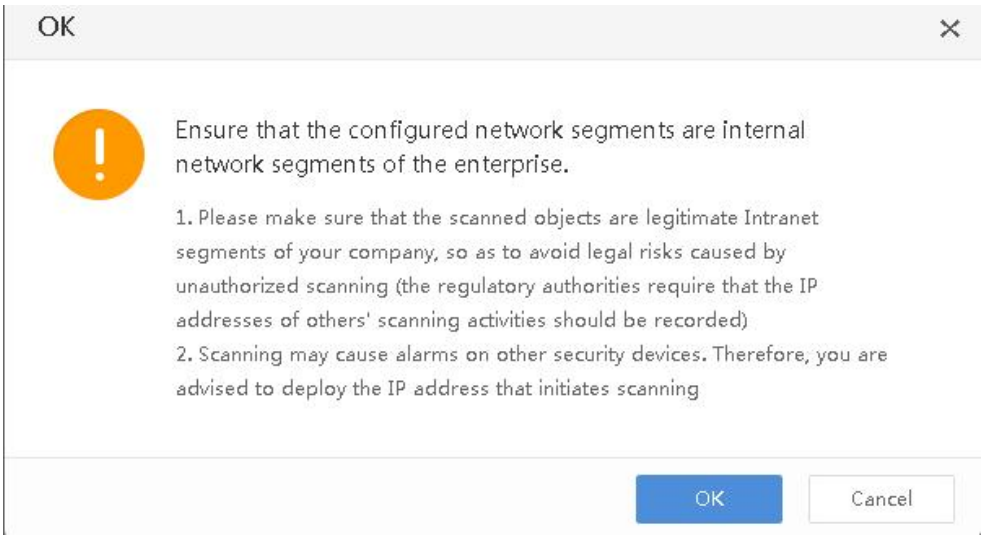
If the scanning range is large, it is recommended to set up concurrent scanning by multiple Linux endpoints with ForeNova clients installed to improve the scanning speed.

**Network Segment**: Set the scan range, and support to fill in the host address or network segment range.

NOTE

You can select the **Scan Method** and **Protocol** by expanding the **Advanced**. Or you can keep the default settings.

2. After clicking **OK**, the risk warning will pop up, as shown in the figure below. After understanding and accepting the risks, click **OK** to execute the scanning operation.




NOTE

During the scanning process, you can click **Cancel** to end the current scanning task.

3. After the scan is complete, the endpoint without ForeNova installed will be listed on the page. You can click the **Export** button to export in a table format, which is convenient for further statistical analysis by the administrator. If an endpoint does not need to install the NovaGuard client, you can click **Ignore**.

## 3.3.4 Security Protection

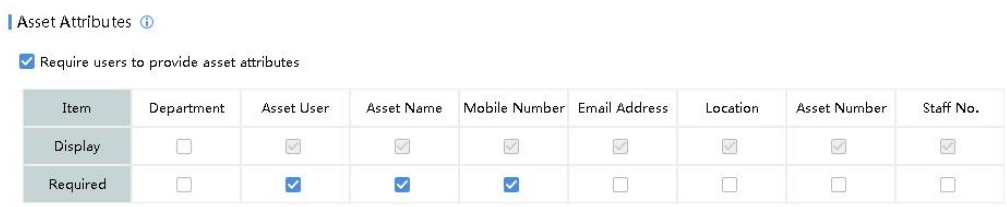
The **Security Protection** module formulates security policies for endpoint groups. It consists of the **Basic Config**, **Anti-Malware**, **Realtime Protection**, **Anti-Ransomware**, **Trusted Files**, **General Settings, Vuln Remediation**, **and Endpoint Control** tabs.

### 3.3.4.1 Basic Config

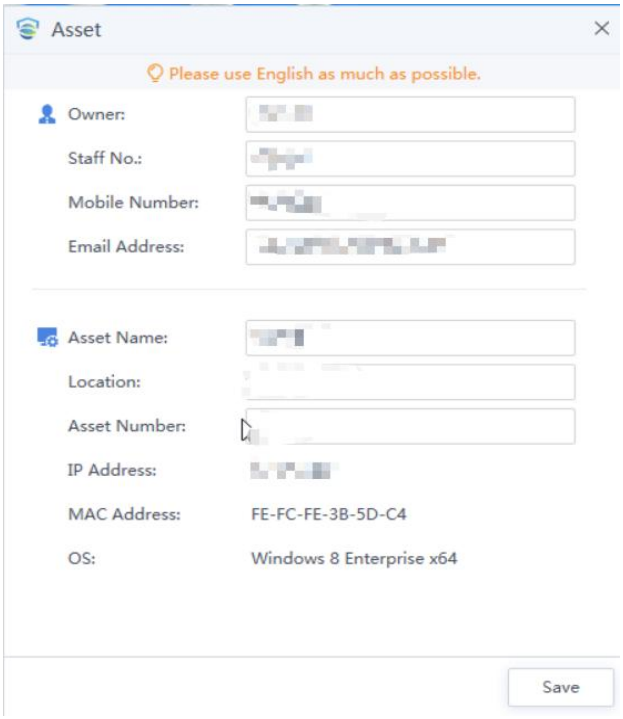
You can configure **Asset Attributes**, **Administrator Contact Information**, **Notifications**, **Agent Administration Passwords**, and **Endpoint Behavior Data & Log Collection** for Windows endpoints on the **Basic Config** tab. The configuration methods are as follows:

#### 3.3.4.1.1 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 department, asset user, asset name, mobile number, email address, location, asset number, and staff No., as shown in the following figure.

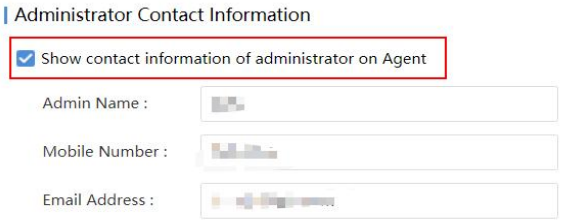


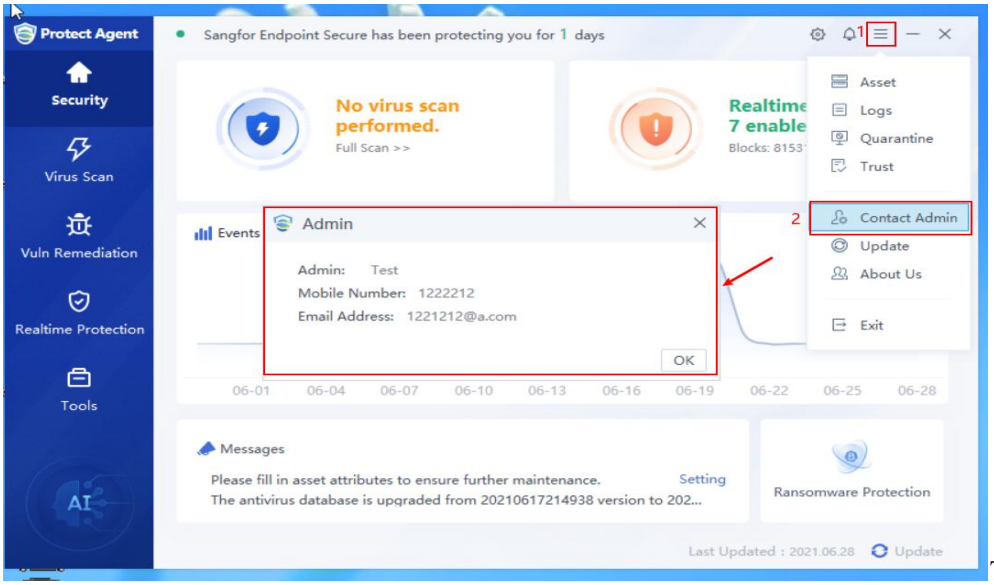

After **Asset Attributes** is configured, endpoint users can view details in system messages and complete endpoint registration as required, as shown in the following figure.




### 3.3.4.1.2 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.

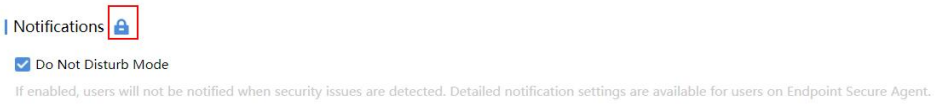





To Query the administrator's contact information on an endpoint, perform the operations shown in the following figure.

### 3.3.4.1.3 Notifications (Do Not Disturb Mode)

If you select **Mute notifications**, endpoint users will not be notified when detecting security issues. The following figure shows the configuration page.

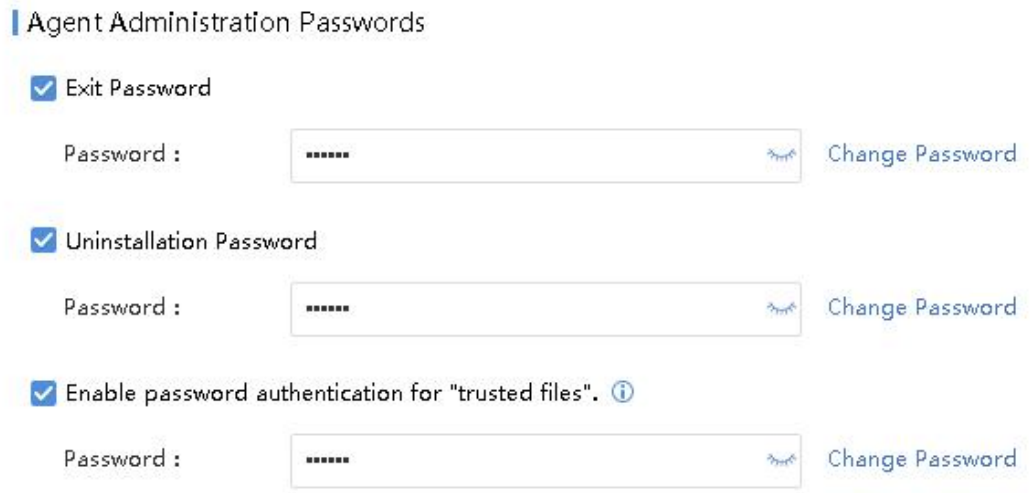



**NOTE**

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.

### 3.3.4.1.4 Agent Administration Passwords

After you configure agent administration passwords, endpoint users need to enter the configured password when they exit or uninstall the Agent and add it into trusted files, as shown in the following figure.

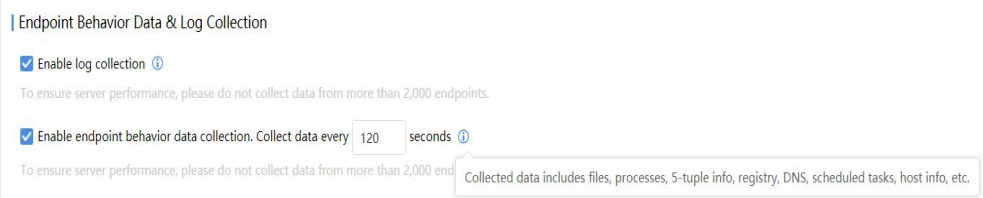



NOTE

Here, the password protection of the endpoint **trusted file** is only valid for Windows PC, not Windows Server.

### 3.3.4.1.5 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 configuring 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**.

## 3.3.4.2 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 scans but do not support policy configuration. The following sections describe how to configure the policies.

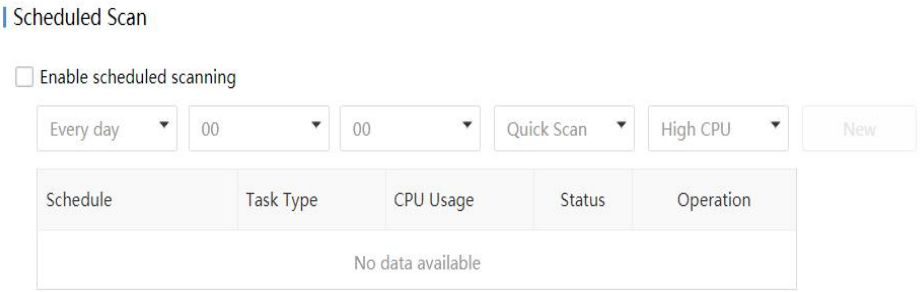



**NOTE**

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

### 3.3.4.2.1 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**, **Adaptive**, and **Low CPU** scan modes. The three modes differ from each other

mainly in CPU usage.

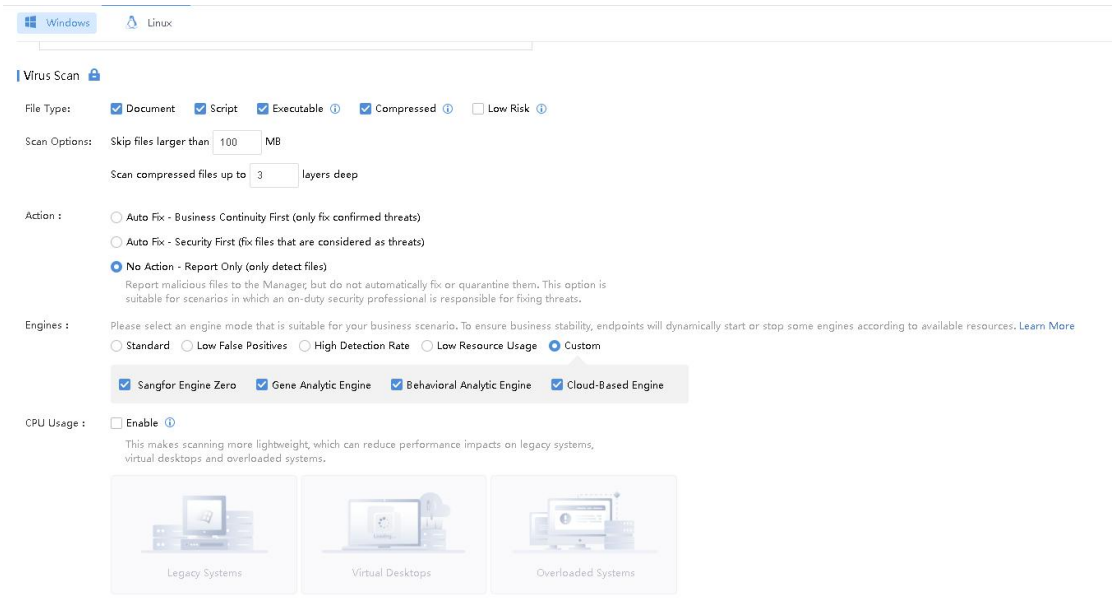
- **High CPU**: Scan is performed at full speed, and the CPU usage of the scanning is not limited.
- **Adaptive**: When scanning, the CPU usage is intelligently adjusted according to the endpoint usage to ensure that endpoint services are not stuck.
- **Low CPU**: Less CPU resources are occupied during the scan, and the CPU usage cannot exceed 10%.

### 3.3.4.2.2 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 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, ForeNova NovaGuard scans only executable files. Therefore, you are advised to select **Executable** for **File Type**. By default, all file types are selected.
2. ForeNova NovaGuard 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 **Auto Fix – Business Continuity First**, **Auto Fix – Security First**, and **No Action-Report Only**. By default, **Auto Fix – Business Continuity First** is selected.

- **Auto Fix – Business Continuity First**: Quarantines malicious files in the blacklist and reports detection logs for files that threaten system security but are not on the blacklist.
- **Auto Fix – Security First**: Quarantines all the detected files that threaten system security.
- **No Action - Report Only**: Reports security logs for all files that threaten system security but do not quarantine the files. This option is suitable for scenarios where an on-duty security expert is responsible for fixing threats.

**Engine**: The options **include Standard, Low False Positives, High Detection Rate, Low Resources Usage,** or **Custom**.

- **Standard**: **Engine Zero, Gene Analysis, Behavioral Analysis Engine,** and **Cloud Based Engine** will be selected.
- **Low False Positives**: **Gene Analysis, Behavioral Analysis Engine,** and **Cloud Based Engine** will be selected.
- **High Detection Rate: Engine Zero in Heuristic Mode, Gene Analysis, Behavioral Analysis Engine,** and **Cloud Based Engine** will be selected.
- **Custom**: You may select the engine according to your needs.

**Restrict CPU Usage**: If you select **Enable**, the amount of CPU resources ForeNova

NovaGuard 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

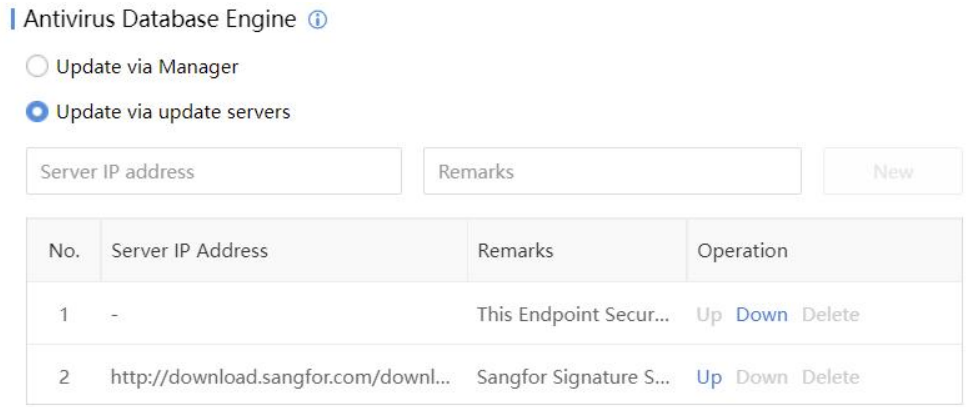
**Engine Zero** in Heuristic mode will increase the sensitivity of AI-based computing and heuristic level of analysis to enhance virus detection. However, false positives may occur. We recommend you enable it in the enhanced scenario with security experts on duty.

If you select **Enable** for **Restrict CPU Usage**, the number of CPU resources ForeNova NovaGuard can use varies based on the scan mode.

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

#### 3.3.4.2.3 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 below.




## 3.3.4.3 Realtime Protection

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

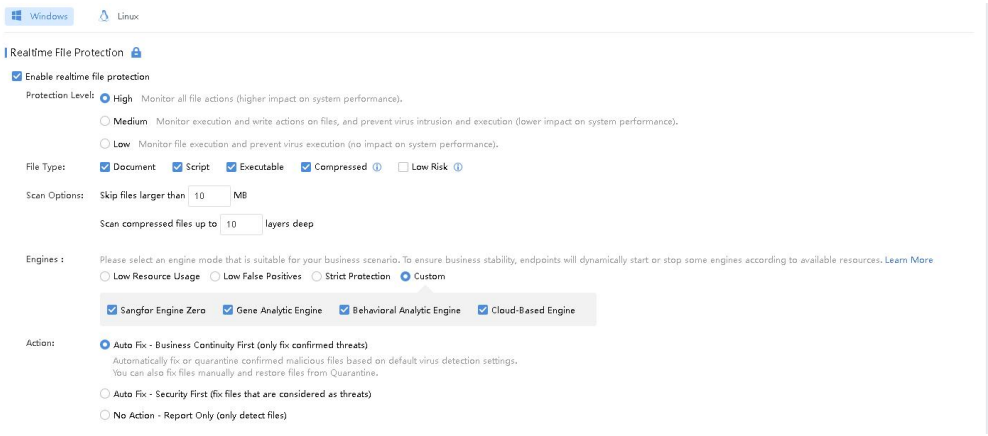
configure real-time protection for macOS endpoints.

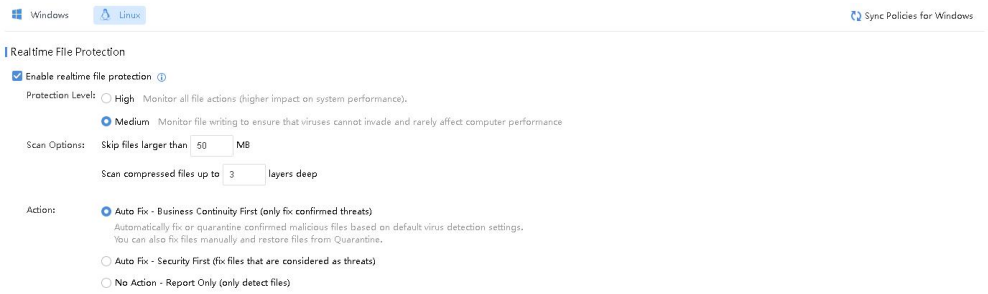
NOTE

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 can configure real-time file protection policies on the Agent.

### 3.3.4.3.1 Realtime File Protection

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




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**: The options **include Standard, Low False Positives, High Detection Rate, Low Resources Usage,** or **Custom**.

- **Standard**: **Engine Zero, Gene Analysis, Behavioral Analysis Engine,** and **Cloud Based Engine** will be selected.
- **Low False Positives**: **Gene Analysis, Behavioral Analysis Engine,** and **Cloud Based Engine** will be selected.
- **High Detection Rate: Engine Zero in Heuristic Mode, Gene Analysis, Behavioral Analysis Engine,** and **Cloud Based Engine** will be selected.
- **Custom**: You may select the engine according to your needs.

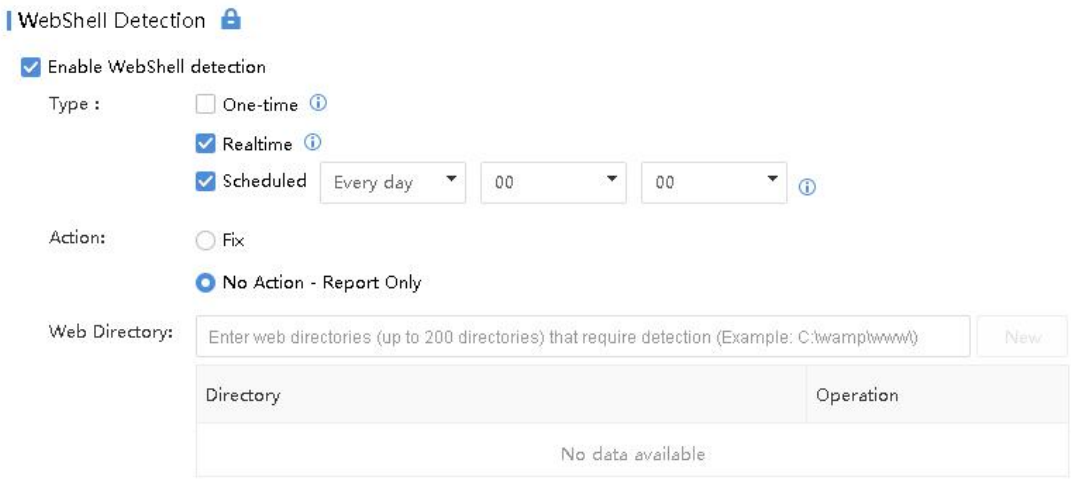
**Action**: You can specify the action to perform when malicious files are detected. The options include **Auto Fix – Business Continuity First**, **Auto Fix – Security First**, and **No Action-Report Only**. By default, **Standard** is selected.

- **Auto Fix - Business Continuity First**: Quarantines malicious files in the blacklist and reports detection logs for files that threaten system security but are not on the blacklist.
- **Auto Fix - Security First**: 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 where an on-duty security expert is responsible for fixing threats.

#### 3.3.4.3.2 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.

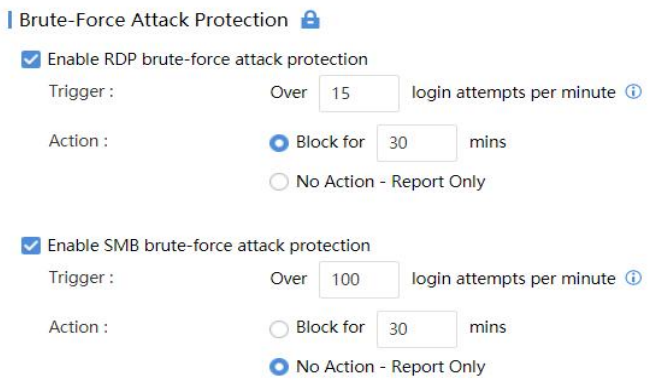
**Action**: You can specify the action to perform when WebShell backdoors are detected. The options include **Fix** and **No Action - Report Only**.

**Web directory:** Set the webshell detection directory. The web server's directory is detected by default, and a custom Web directory can also be detected.

### 3.3.4.3.3 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.



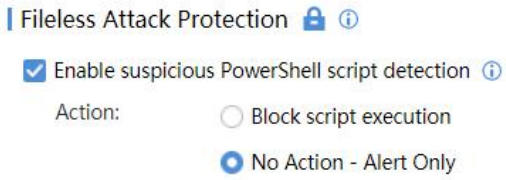

You can configure the following parameters:

- **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**.

### 3.3.4.3.4 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 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, ForeNova NovaGuard 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, ForeNova NovaGuard reports an alert but does not suspend the script execution. You can determine whether to allow or block the script execution.

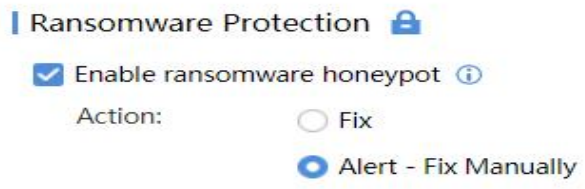
The following figure shows sample alert information.



## 3.3.4.4 Anti-Ransomware

### 3.3.4.4.1 Ransomware Protection (Only for Windows Endpoints)

In ransomware protection, ForeNova NovaGuard 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**. An alert is displayed in the lower right corner when ransomware is detected on an endpoint. The following figure shows an example.




### 3.3.4.4.2 RDP Access Protection

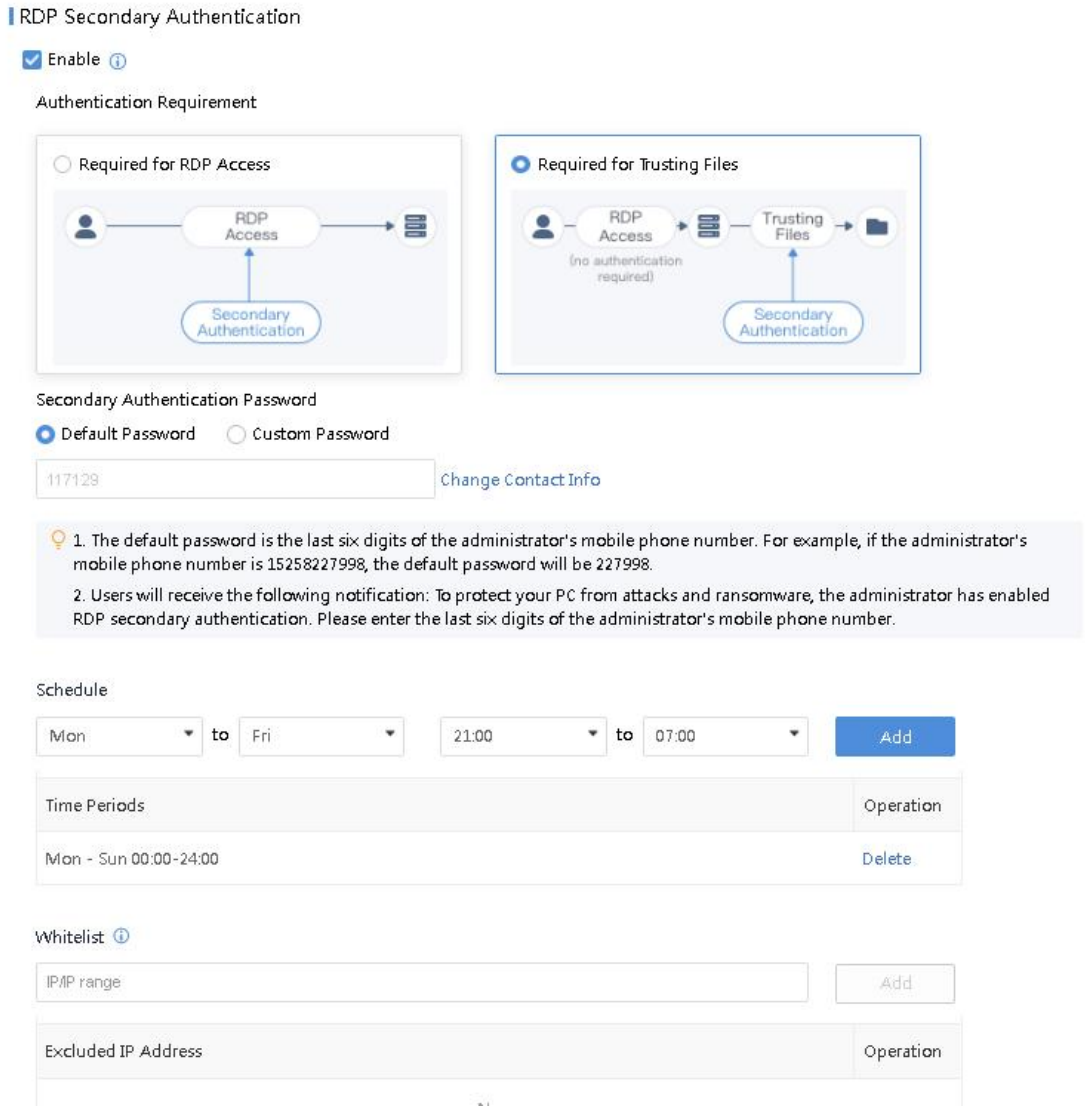
RDP brute-force login is a common attack vector that enables hackers to control servers and

initiate ransomware attacks. For business security, you are advised to enable protection against brute-force logins.

If you select **Enable**, ForeNova NovaGuard 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.

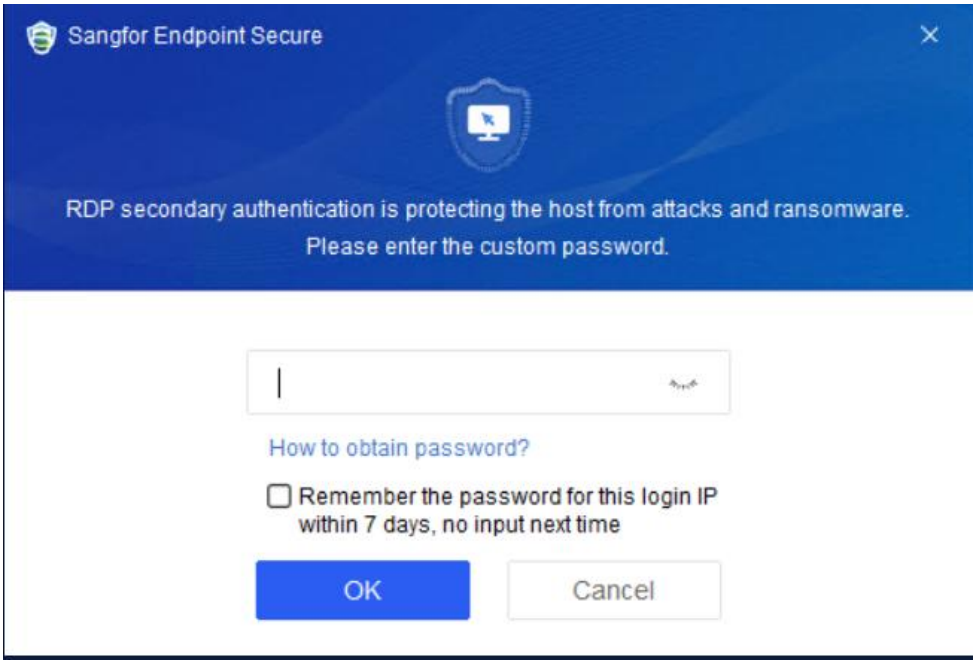



**Authentication Requirement Required for RDP Access**

To prevent hackers from successfully logging in to the server through a remote desktop and easily obtaining server permission, you can set the authentication method as RDP secondary authentication.

After setting the authentication method to RDP secondary authentication, NovaGuard will lock the server to protect the server when the hacker successfully logs into the server via a remote desktop. The figure below shows that the hacker needs to pass the NovaGuard secondary authentication to obtain the server permission.

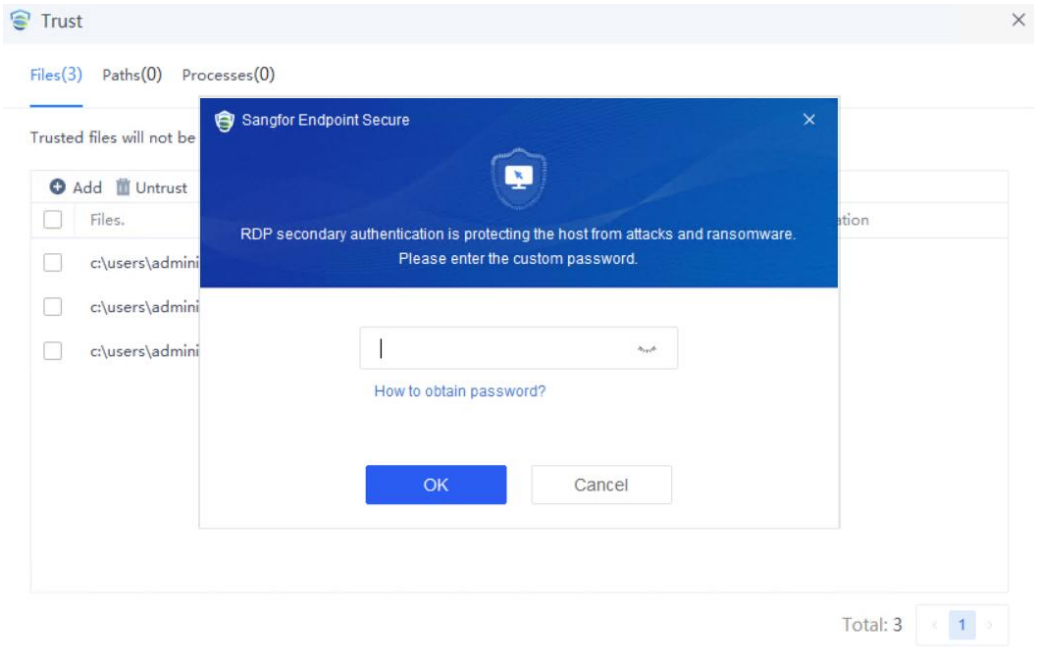
It is recommended to select this authentication method to protect the server.




**Required for Trusting Files**

Prevent hackers from adding virus files to the NovaGuard Trusted Files and planting ransomware viruses. You can set the authentication method as **Required for Trusting Files**.

The hacker successfully logged in to the server and tried to plant Ransomware. Because NovaGuard protects the server, the ransomware cannot run by default. However, if hackers add the Ransomware to the Trusted Files, they can successfully implant the Ransomware and run it for extortion. When the authentication method is set to RDP secondary authentication, when the hackers try to add the ransomware file to trusted files, they need to pass the RDP secondary authentication first, as shown in the figure below.




**Secondary Authentication Password**

**Default Password**

The verification code is the last 6 digits of the admin mobile phone number, such as 0127117129. Set the verification code to 117129. Go to **Endpoints > Security Protection > Basic Config,** and configure the contact information of the Endpoints administrator, as shown in the figure below.




**NOTE**

It is recommended to set the authentication key to the verification code and the admin mobile phone number to be configured correctly. The server operation and maintenance Admin can obtain the administrator's mobile phone number through the company address book or NovaGuard agent tray to obtain the remote desktop secondary authentication verification code.

**Custom Password**

To avoid the server admin being unable to access the server during the working period. You need to notify the server administrator of the custom password in advance.

**Schedule**

The Schedule sets the effective time of the remote desktop secondary authentication. The default is to take effect in all periods.

**Whitelist**

The whitelisted IPs do not require secondary authentication to log in to the server via remote desktop during scheduled periods. access

Computers with trusted servers can be added to the whitelist.

### 3.3.4.4.3 Enhanced Server Protection

Enhanced Server protection protects 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

Enhanced 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.

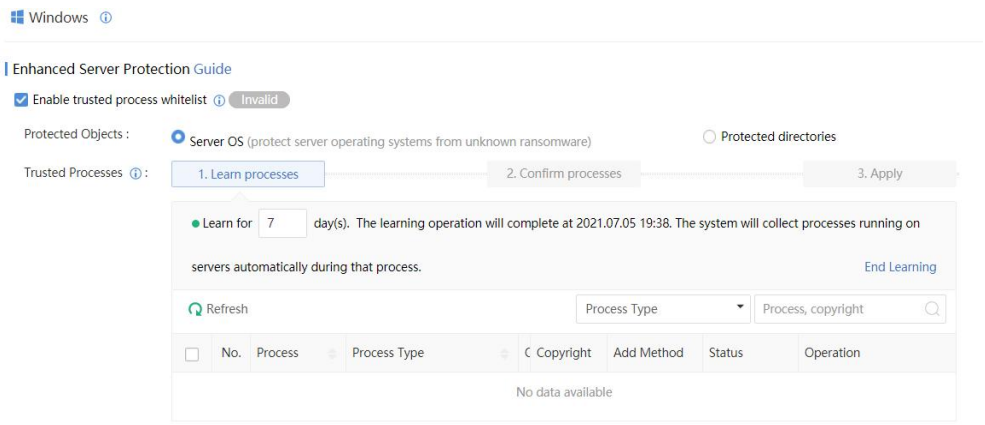
**Configuration procedure:**

**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.

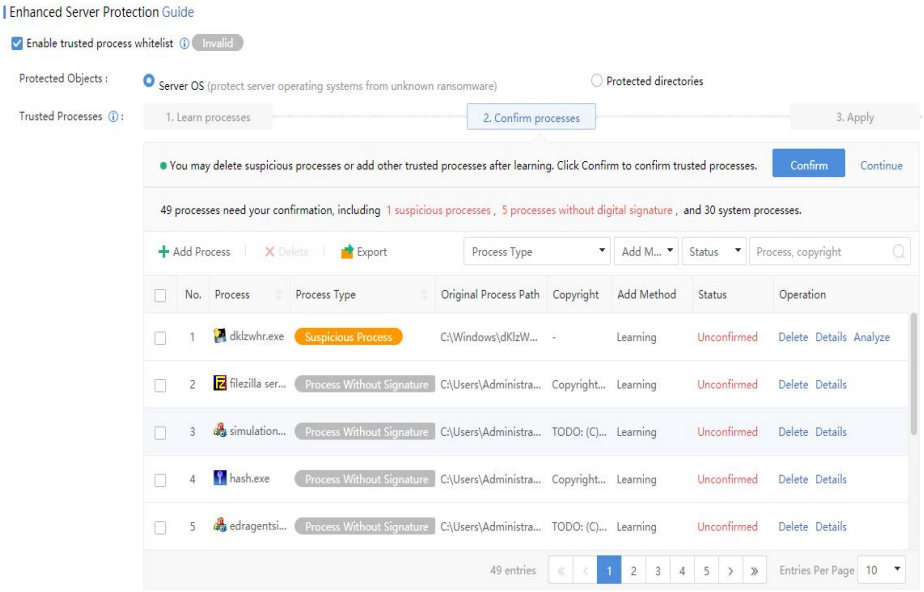
Select **Enable trusted process whitelist**, select **Server OS** for **Protected Objects**, specify a period for process learning, which ranges from 1 to 30 days, and click **Save**, as shown in the following figure.




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.

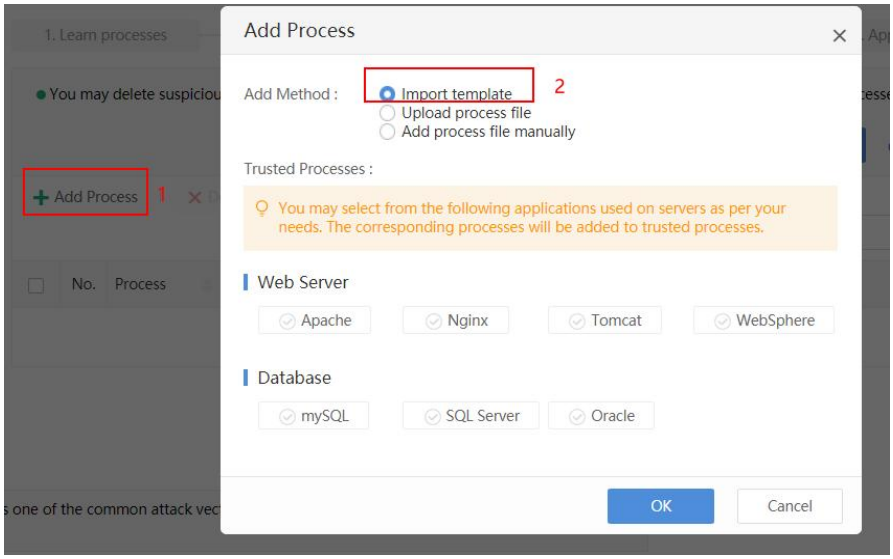



The process parameters are described as follows:

- **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 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:

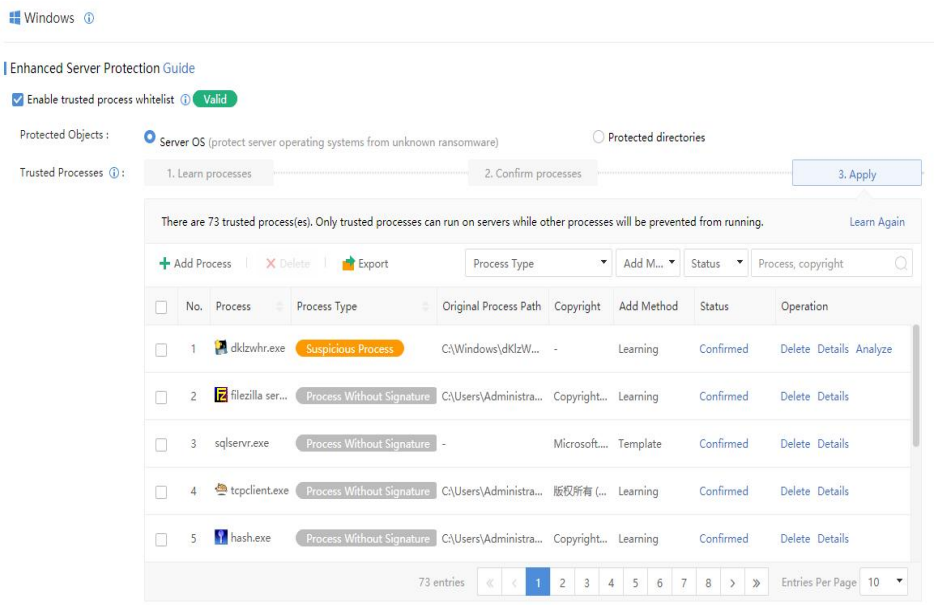
**Add Method**: The options include **Import template**, **Upload process file**, and **Add process file manually**.

- **Import template**: Select this option if the server you want to protect is a web server or a database server in the template.
- **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.

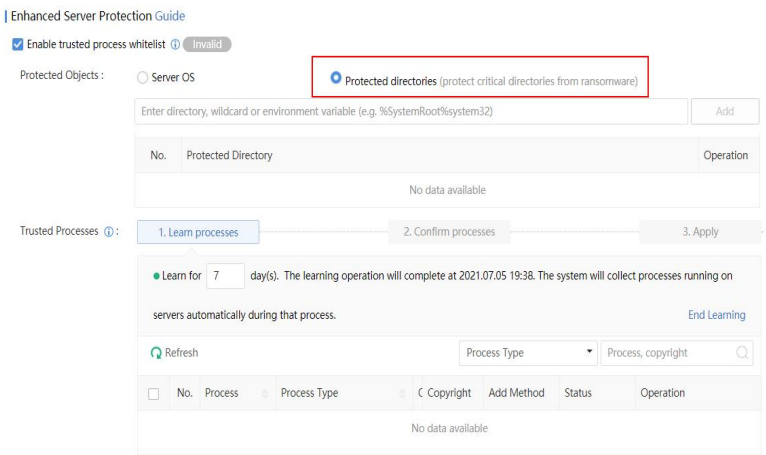
**Configuration procedure:**

**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.

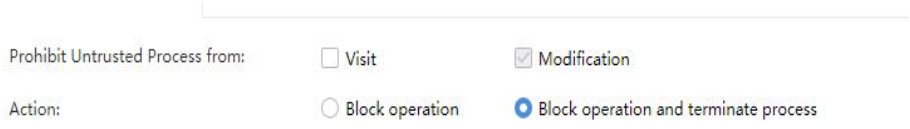
Select **Enable trusted process whitelist**, select **Protected directories** for **Projected Objects**, and add critical directories you want to protect. You can enter wildcard characters (*) and environment variables.




**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.



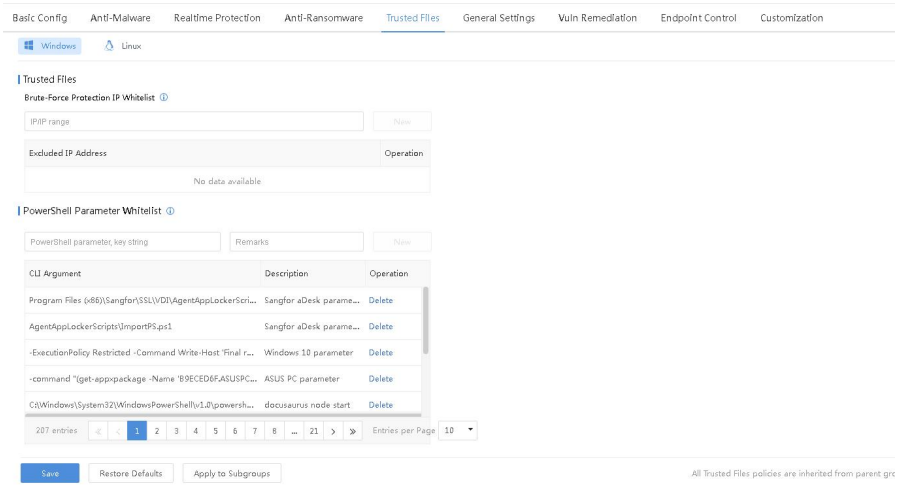

You can configure the following parameters:

- **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**.

## 3.3.4.5 Trusted Files

In the **Trusted Files** area, you can configure **Brute-Force Protection IP Whitelist and PowerShell parameter whitelist**. 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.

### 3.3.4.5.1 Windows



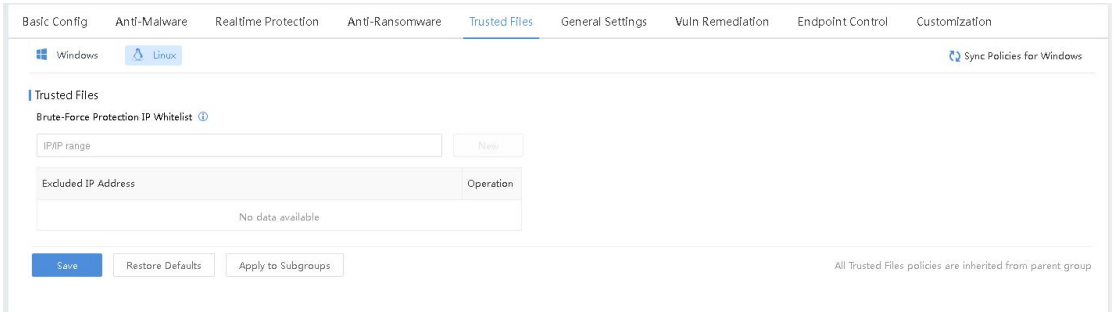

You can configure the following parameters:

- **Brute-Force Protection IP Whitelist**: You can add IP addresses, IP address ranges, and subnets to the whitelist. No alert is triggered if IP addresses in the whitelist initiate brute-force attacks.
- **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.

#### 3.3.4.5.2 Linux



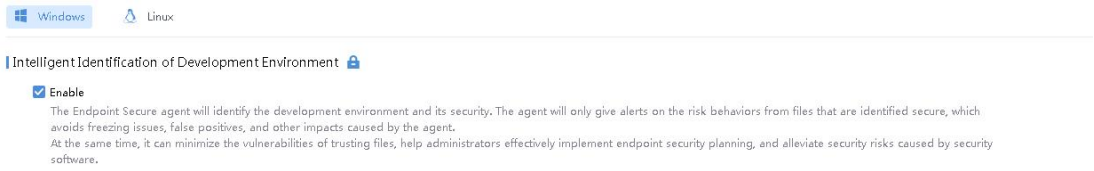

You can configure the following parameters:

- **Brute-Force Protection IP Whitelist**: You can add IP addresses, IP address ranges, and subnets to the whitelist. No alert is triggered if IP addresses in the whitelist initiate brute-force attacks.

## 3.3.4.6 General Settings

**Intelligent Identification of Development Environment**

Only the Windows terminal is supported to open the development environment intelligent recognition. The configuration interface is as follows.



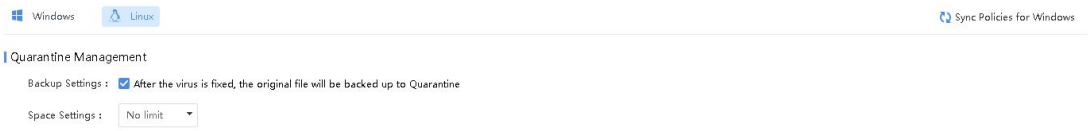

**Quarantine Management**

It supports backup settings and space settings for Windows endpoints or Linux endpoints. The configuration interface is shown below.

Windows quarantine management.




Linux quarantine management.



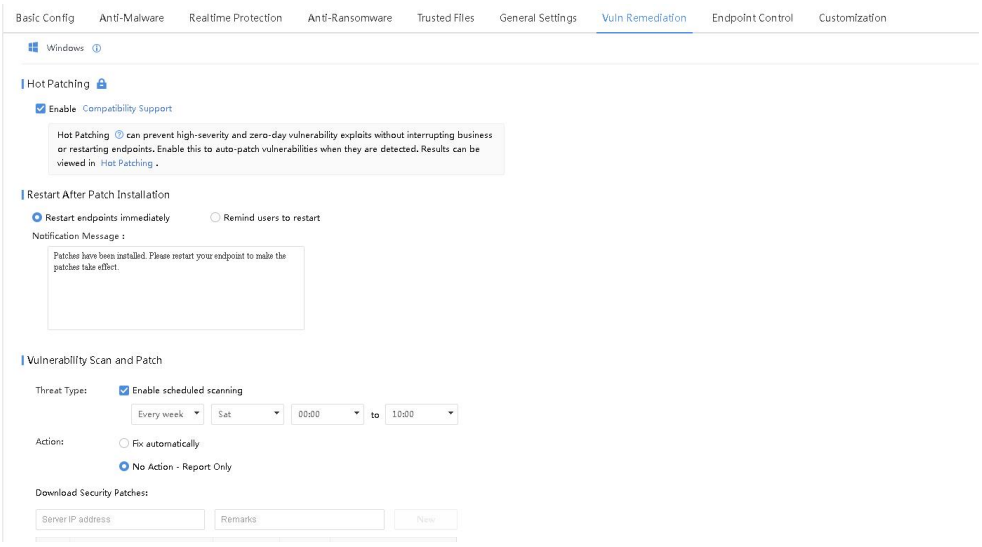

**NOTE**

1. MAC endpoint does not support quarantine management.

2. Windows endpoint supported to set quarantine management on end.

## 3.3.4.7 Vuln Remediation

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




**NOTE**

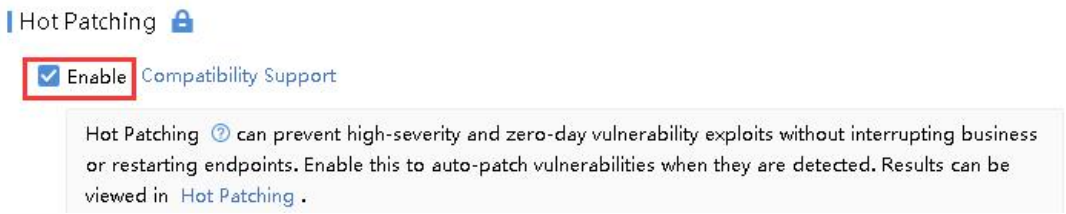
This function is supported only on Windows endpoints that can access the Internet.

### 3.3.4.7.1 Hot Patching

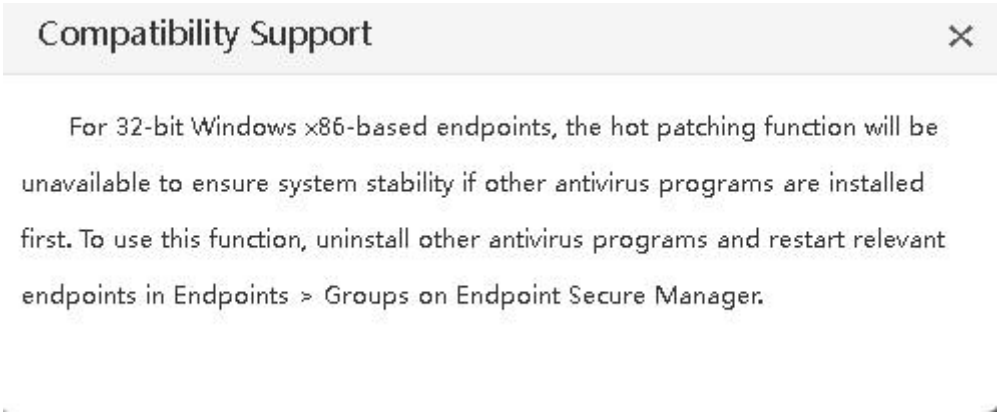
Hot patching is lightweight and has no impact or interference on the business system. It can prevent high-risk and zero-day vulnerability exploits without interrupting business or restarting endpoints. Hot patching does not involve compatibility issues and features a lightweight process, fast rectification,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

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

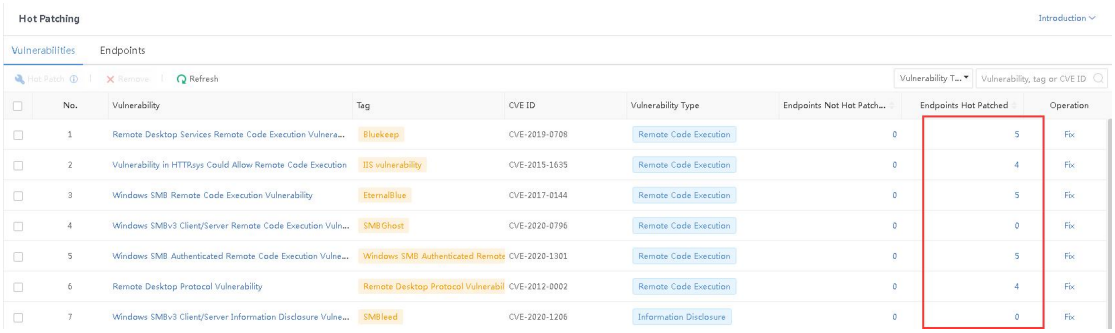
indicates that users are not allowed to modify hot patching settings on the Agent, and the settings on the Manager prevail. indicates that users are allowed to modify hot patching settings on the Agent, and the settings on the Agent prevail.




Click **Compatibility Support** in the above picture. The compatibility support is as follows:



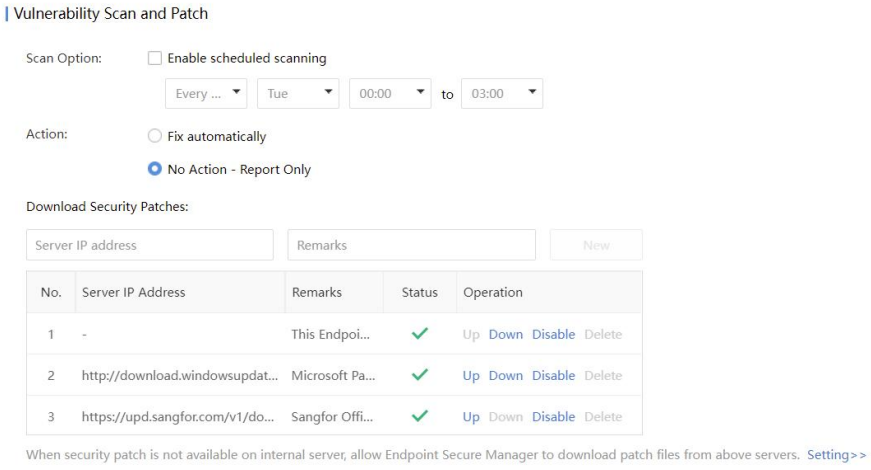

When the hot patching function is enabled, the computer with the corresponding vulnerability will be automatically patched. Open **Response > Remediation > Hot Patching**, as shown below:




When the endpoint does not need to be patched to a particular vulnerability, as shown in the figure above, select the vulnerability and click **Remove.**

### 3.3.4.7.2 Vulnerability Scan and Patching

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



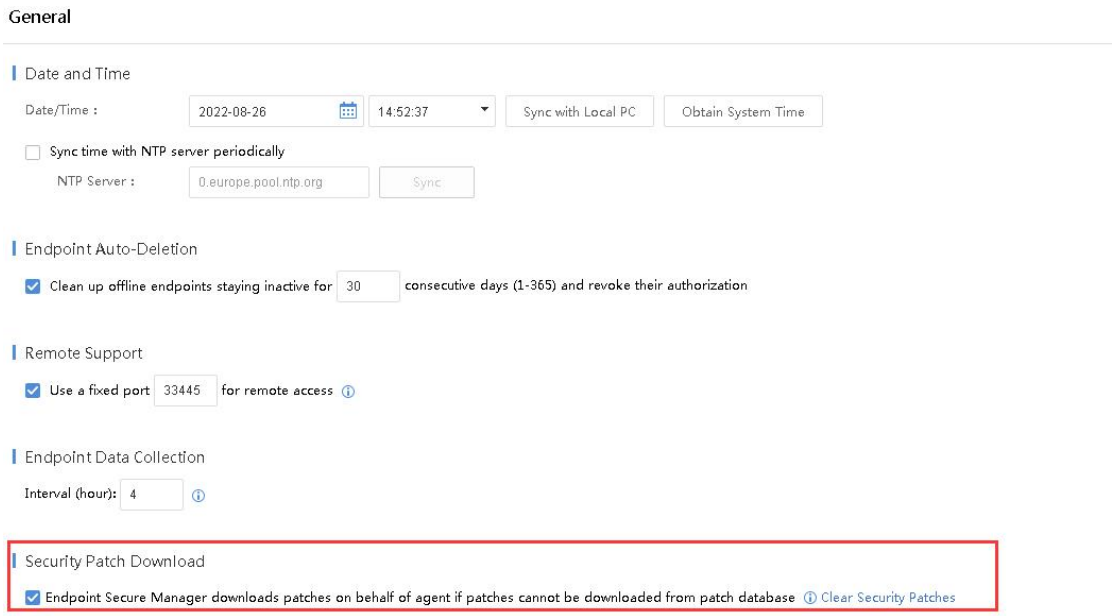

The parameters are as follows:

- **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 ForeNova CDN server, the Microsoft vulnerability patch server, and the NovaGuard Manager.

NOTE

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

When the endpoint cannot connect to the Internet, but the NovaGuard manager can connect to the Internet, the endpoint cannot download the vulnerability patch package from the Internet server. Go to **System** > **System** > **General**, as shown in the figure below, and select **NovaGuard Manager downloads patches on behalf of agent if patches cannot be downloaded from patch database**, then the NovaGuard manager can download the patch package on behalf of the agent to complete the patch repair.




NOTE

When neither the endpoint agent nor the NovaGuard manager has Internet permissions, refer to the **System > System > Tools** to download the vulnerability patch through an offline tool to complete the vulnerability repair.

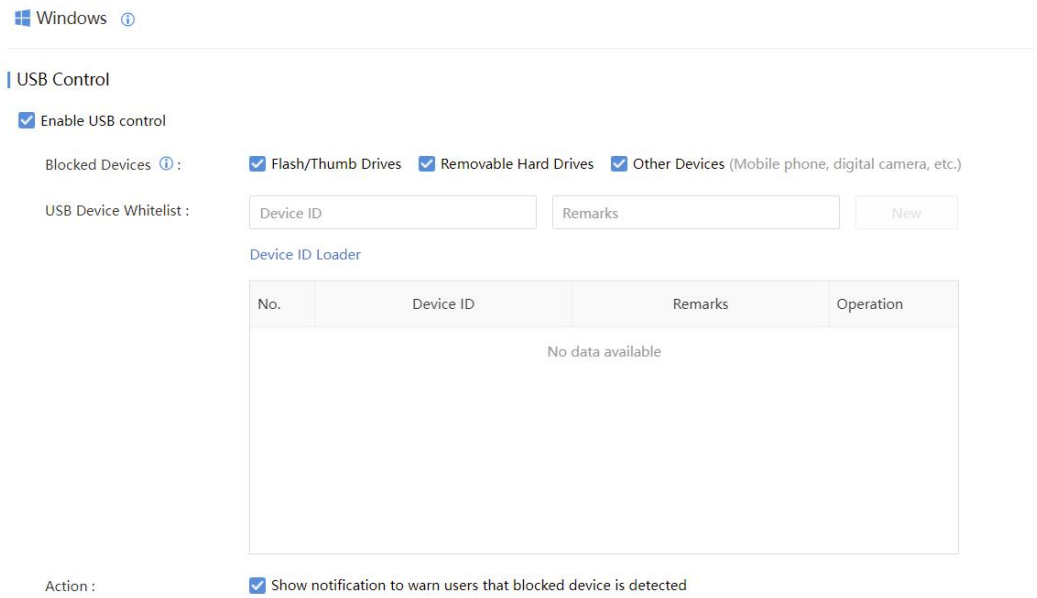
## 3.3.4.8 Endpoint Control

### 3.3.4.8.1 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 other devices(mobile phones, digital cameras, etc.) and set the Agent to show notifications to warn users. It helps reduce risks caused by insufficient USB device control.

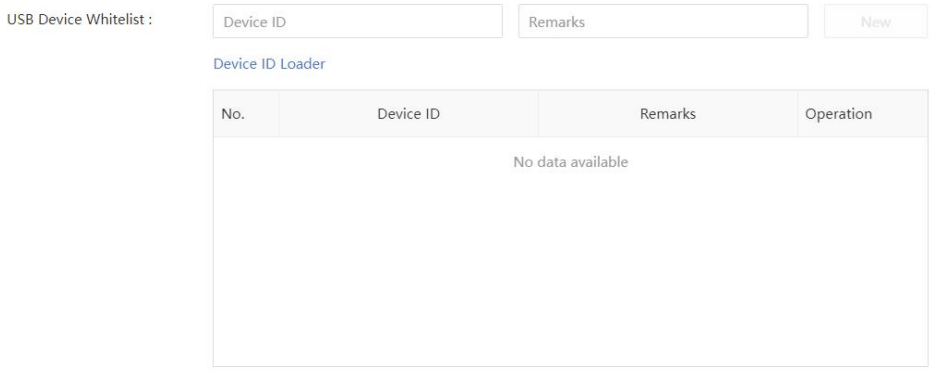
Select **Enable USB control** on the USB Control tab to enable the USB control function. The following figure shows the configuration page.




1. Define blocked USB devices.

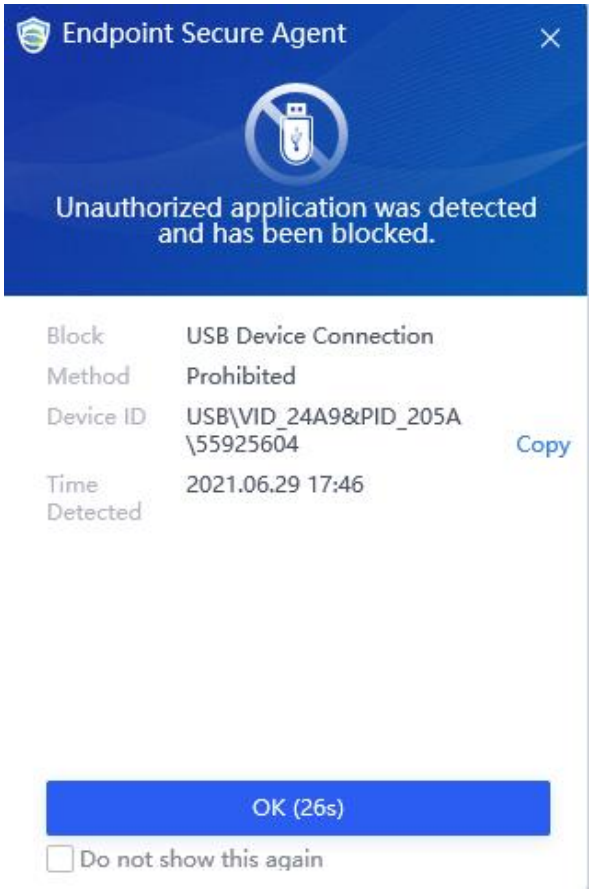
**Blocked Devices**: Only USB devices with the storage function will be blocked. Mouses and keyboards will not be blocked. Common USB devices include USB flash drives, removable hard disks, and portable devices (such as mobile phones and digital cameras).

- 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 **the Show notification to warn users that 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.

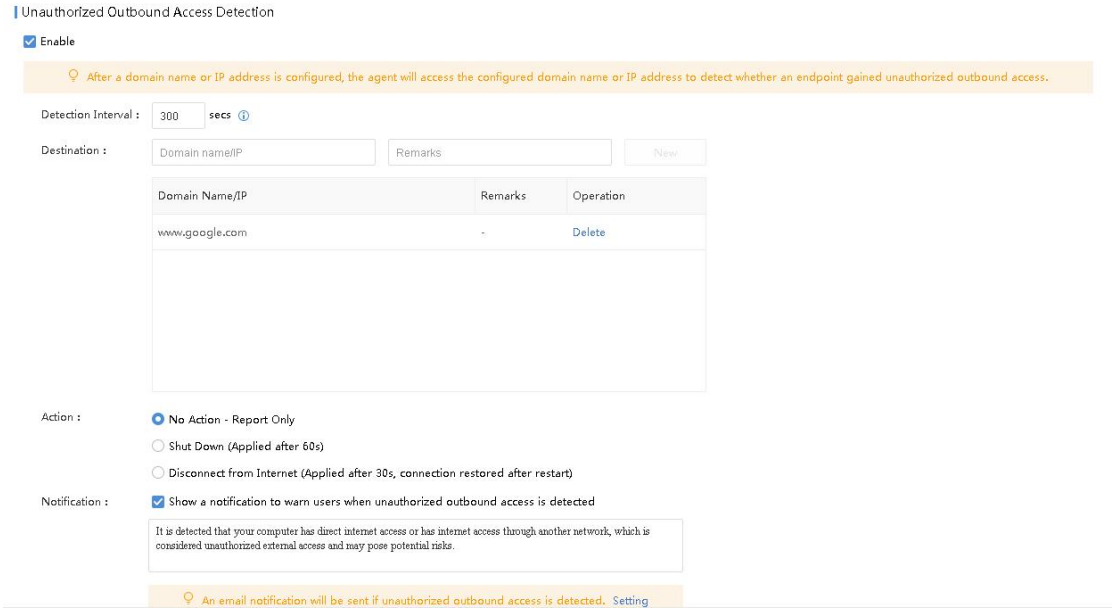


### 3.3.4.8.2 Unauthorized Outbound Access Control

Unauthorized outbound access control is only for Windows, not Linux endpoints. Direct access to the Internet and access through another network from internal computers and dedicated network devices are regarded as unauthorized external access. Hackers can bypass the firewall, gateway, and other protection measures to intrude on 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. The network disconnection effect is similar to endpoint isolation for endpoints running Windows Vista or later. Except for communications with the NovaGuard 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.

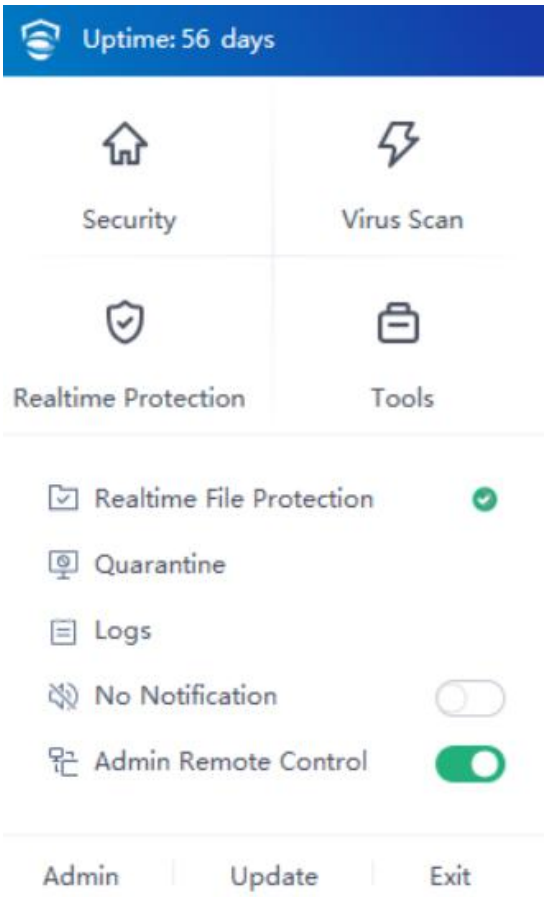
4. **Notification**: When an endpoint conducts unauthorized external access, a pop-up window will be displayed in the lower right corner of the desktop to warn users. You can set the notification content in the text box in this area.
5. **Email**: When an endpoint conducts unauthorized external access,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

#### 3.3.4.8.3 Remote Support Control

When the controlled endpoints fail, the admin can remotely control endpoints through the remote support function and respond to the endpoint's problems safely and quickly.

**Prerequisites:**

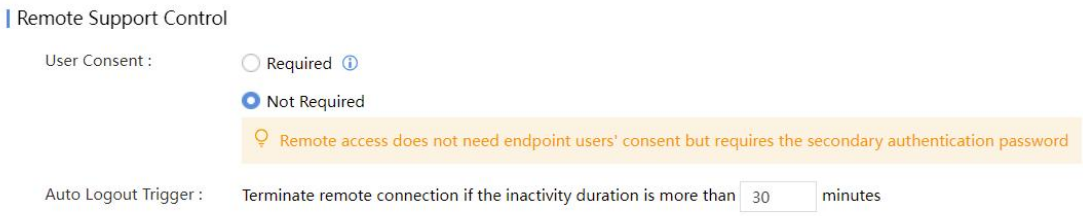
The admin's prerequisite to remotely managing endpoints is that the agent has enabled **Admin Remote Control,** as shown in the figure below. This function is disabled by default. Suppose the Admin Remote Control is turned off. The administrator cannot assist the Endpoints management through NovaGuard remotely.




**Scenario 1: Do not need Endpoint's confirmation. Directly remote Endpoint's computer.**

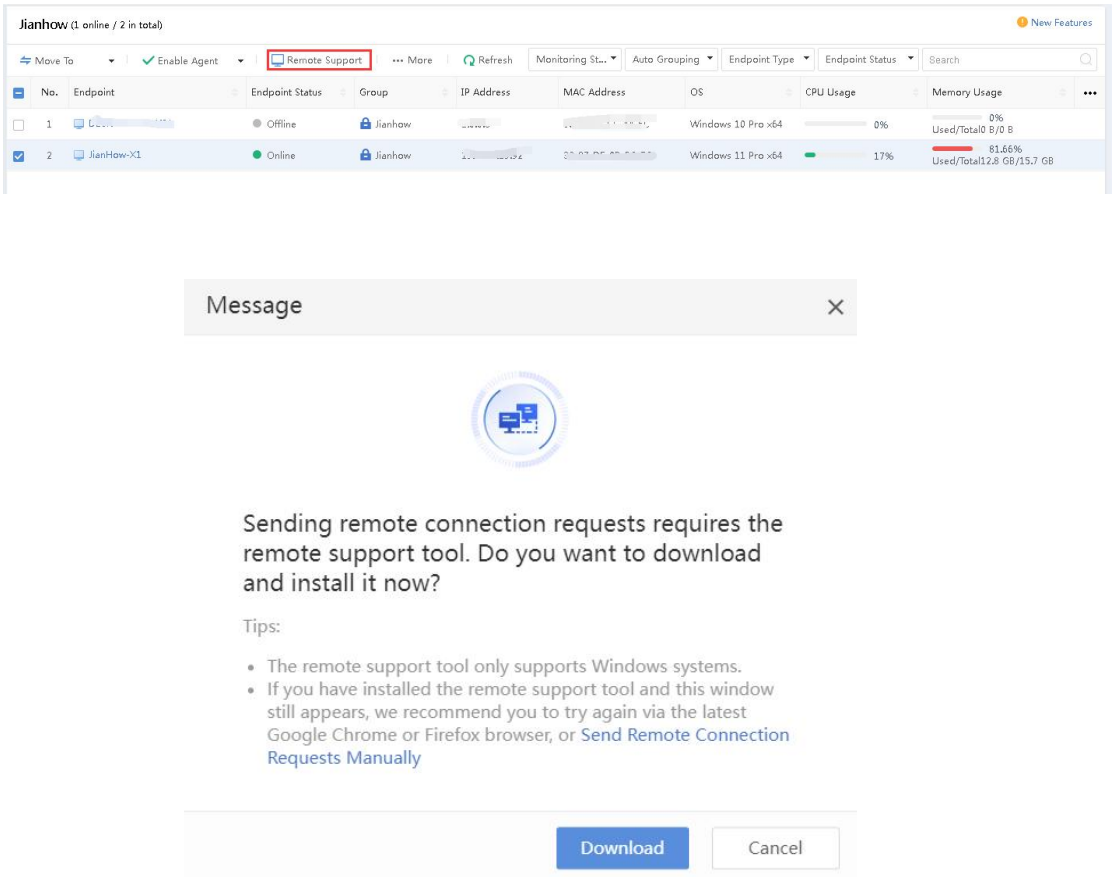
Without user confirmation, the administrator can directly remote the endpoint computer, which is suitable for unattended endpoint scenarios.

Go to **Endpoints > Security Protection** and select the group that needs confirmation for remote support control. Open the **Endpoint Control > Remote Support Control.** Select **Not required** in User Consent.




Go to **Endpoints > Groups** Administrator, select the endpoint that needs to be remote, and

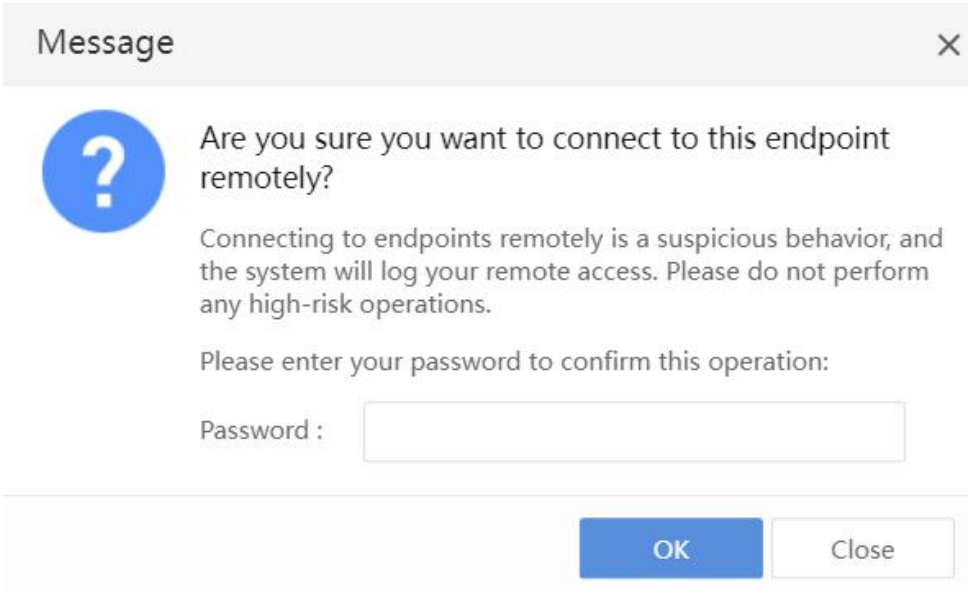
initiate remote assistance, as shown in the figure below.



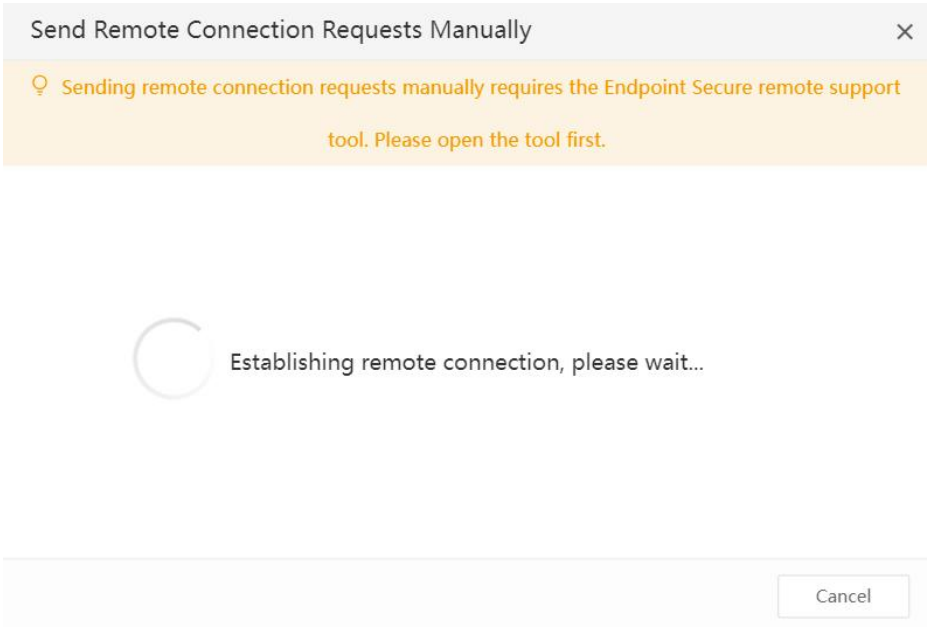

When using remote support for the first time, you need to download the VNC client remote tool and click **Download** to download and install the VNC client remote tool, as shown in the figure below.

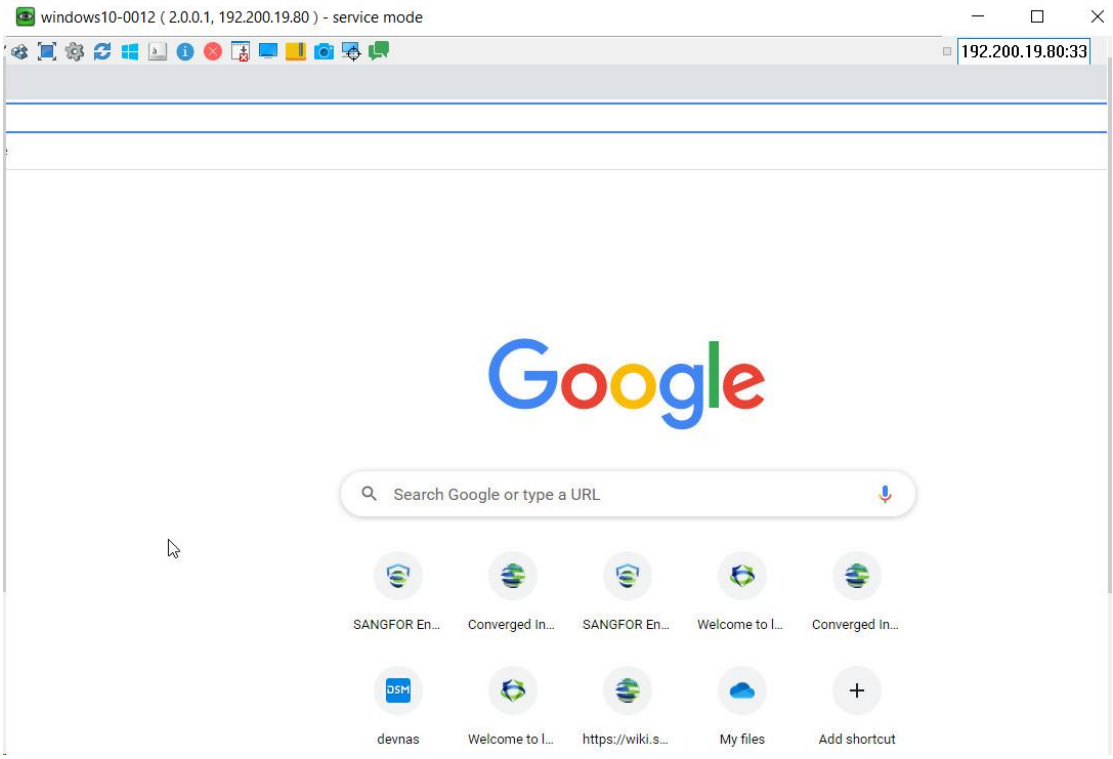



After installing the VNC client remote tool, initiate a remote to endpoints again, as shown in the figure below.




To confirm that an admin operates it, you need to enter the current admin account password, enter the admin password, and click **OK** to establish a remote connection and successfully remotely control the computer, as shown in the figure below.

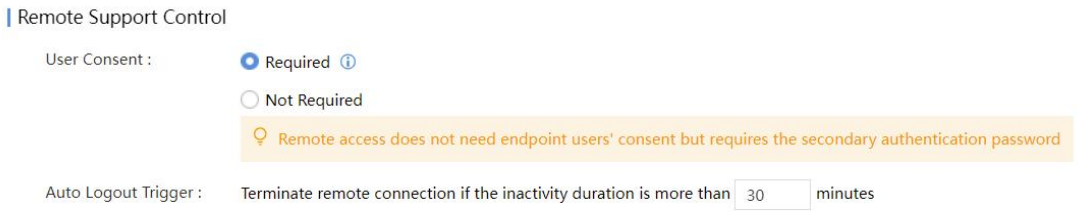




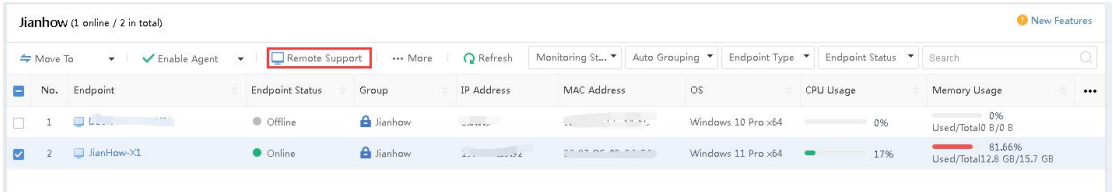

**Scenario 2: Endpoint confirmation is required before the remote Endpoint computer can be used.**

It requires endpoint confirmation so an admin can remote Endpoints computers, suitable for scenarios where people are on duty and sensitive to remote operations.

Go to **Endpoints > Security Protection** and select the group that needs confirmation for remote support control. Open the **Endpoint Control > Remote Support Control.** Select **Required** in User Consent.



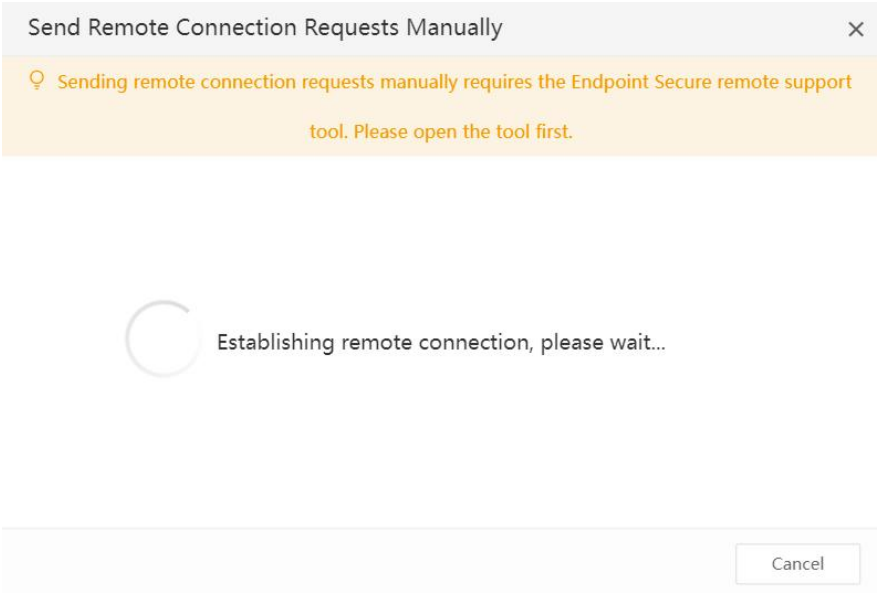

Go to **Endpoints > Groups** Administrator, select the endpoint that needs to be remote, and initiate remote assistance, as shown in the figure below.



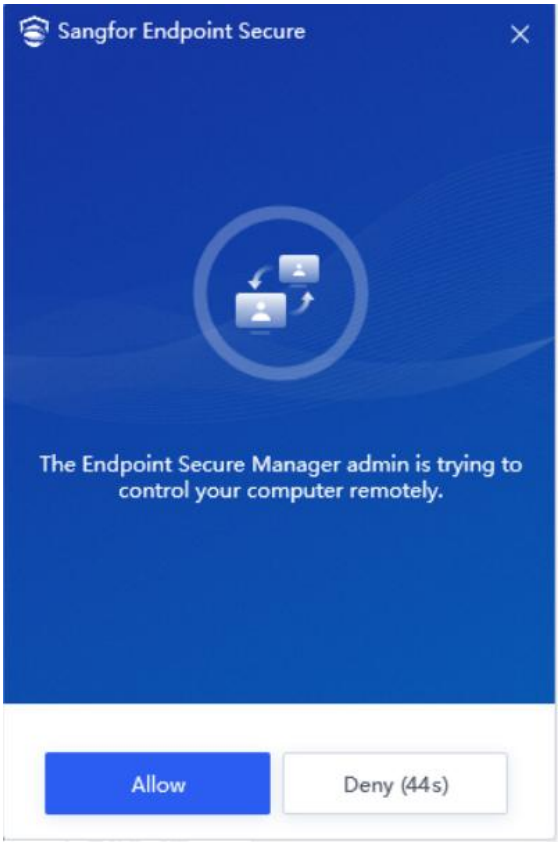

When using remote assistance for the first time, you need to download the VNC client remote tool and click **Download** to download and install the VNC client remote tool, as shown in the figure below.




After installing the VNC client remote tool, initiate a remote to endpoints again, as shown in the figure below.

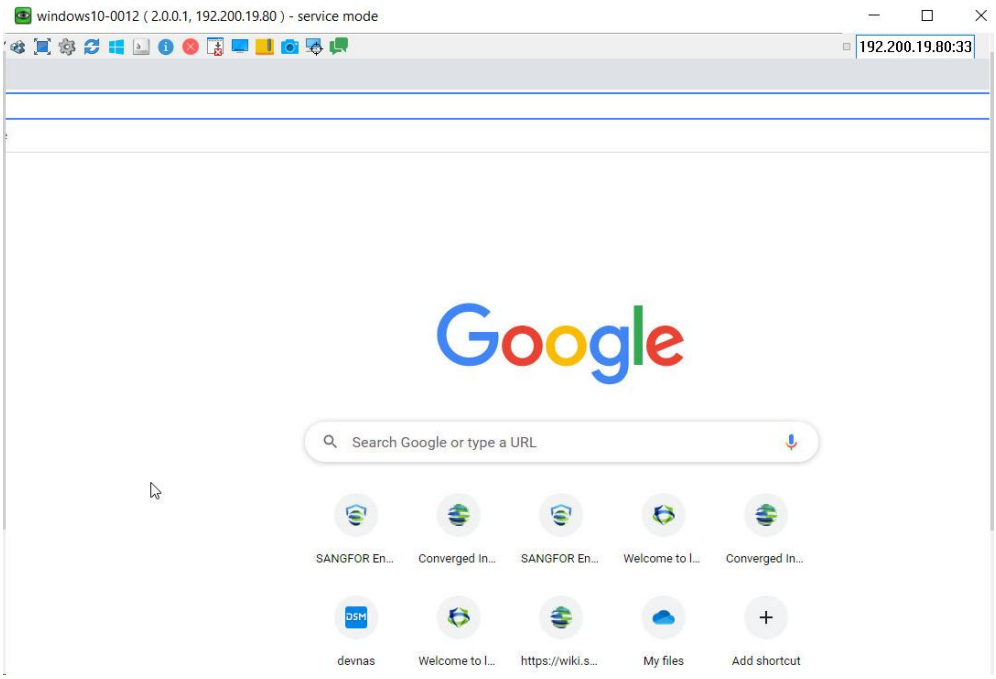



A prompt pop up on the NovaGuard client tray of the endpoint computer.




When the Endpoints user clicks **Allow, the** admin can remotely control the Endpoints computer.

To confirm that an admin operates it, you need to enter the current admin account password, enter the admin password, and click **Confirm** to establish a remote connection and successfully remotely control the computer, as shown in the figure below.




**NOTE**

1. Only the admin and the security operator have permission to remote control, and the entire communication process is encrypted.
2. Remote assistance uses the random port to control the computer remotely. The fixed port can be set in advance through the **Remote Support Setting** in **System System > General,** and the computer can be controlled remotely through the fixed port.
3. The remote support function currently supports win7/win10/XP /win8/win8.1 system.

## 3.3.4.9 Security Policies Supported by Different Operating Systems

| Security Protection | Windows PC | Windows Server | Linux | MAC |
|---|---|---|---|---|
| Basic Config | √ | √ | × | × |
| Virus Scan | √ | √ | √ | × |
| Realtime Protection | √ | √ | √ | × |
| WebShell Detection | × | √ | √ | × |
| Ransomware Protection | √ | √ | × | × |
| Brute-Force Attack Protection | √ | √ | √ | × |
| Fileless attack protection | √ | √ | × | × |
| Enhanced Server Protection | × | √ | × | × |
| Trusted Files | √ | √ | × | × |
| Quarantine Management | √ | √ | √ | × |
| Vulnerability Remediation | √ | √ | × | × |
| Unauthorized Outbound Access Detection | √ | √ | × | × |
| USB Control | √ | √ | × | × |
| RDP Secondary Authentication | × | √ | × | × |

Table 5: Security policies supported by Windows PC, Windows Server, Linux, and Mac systems

NOTE

Mas OS currently only supports trigger virus scan from NovaGuard Manager.

# 3.4 Micro-Segmentation

The **Micro-Segmentation** module allows you to enable necessary server/endpoint ports, 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.

<table>
<tr><td rowspan="8">Object</td><td rowspan="2">Business assets</td><td>Business Asset Name</td><td>Endpoint Group</td><td>Contained Endpoints</td><td>-</td></tr>
<tr><td>All</td><td>User zone 1, user zone 2, user zone 3, server zone 1, and server zone 2</td><td>PC1\PC2 Sever1 and Server2</td><td>-</td></tr>
<tr><td rowspan="2">IP groups</td><td>IP Group Name</td><td>IP Address Range</td><td>IP Group Type</td><td>-</td></tr>
<tr><td>Office endpoints</td><td>172.16.200.1-172.16.200.254</td><td>Internal network</td><td>-</td></tr>
<tr><td rowspan="3">Services (Clarify custom policies only.)</td><td>Service Name</td><td>Protocol</td><td>Port</td><td>Traffic Type</td></tr>
<tr><td>SMB</td><td>TCP</td><td>135\136\137\139\445</td><td>Business traffic</td></tr>
<tr><td>RTP</td><td>TCP</td><td>3389</td><td>Maintenance traffic</td></tr>
<tr><td rowspan="2">Access Relationship Between</td><td rowspan="2">Access relationship</td><td>Source</td><td>Destination</td><td>Service</td><td>Action</td></tr>
<tr><td>IP group: Internet by</td><td>Business asset: All</td><td>SMB and RTP</td><td>Deny</td></tr>
</table>

| | | | | | |
|---|---|---|---|---|---|
| **Objects** | | default | | | |

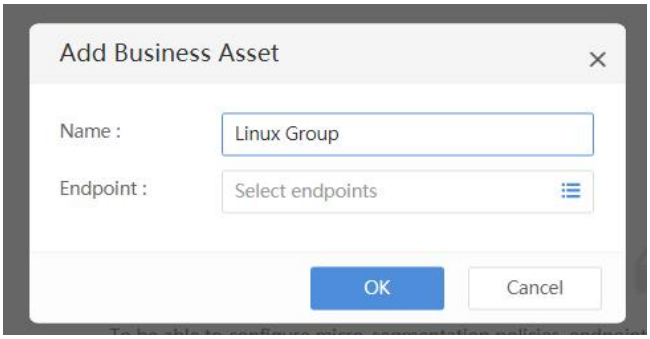
Table 6: Relationship between business assets

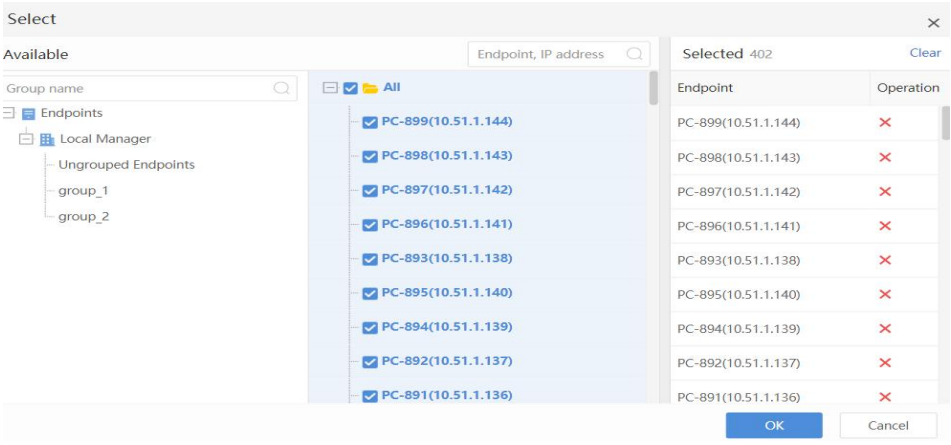
## 3.4.2 Creating Business Assets, Roles, IP Groups, and Services

### 3.4.2.1 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.




**NOTE**

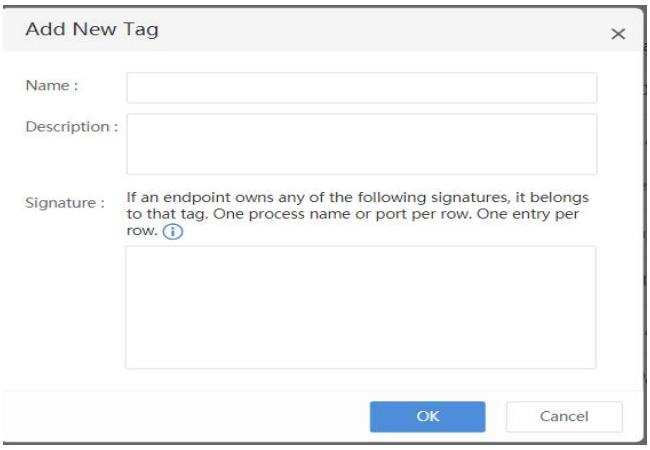
One server endpoint can only join one business asset. The endpoint only supports the selection of the server endpoint.

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.

### 3.4.2.2 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 NovaGuard 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** > **Roles** 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.

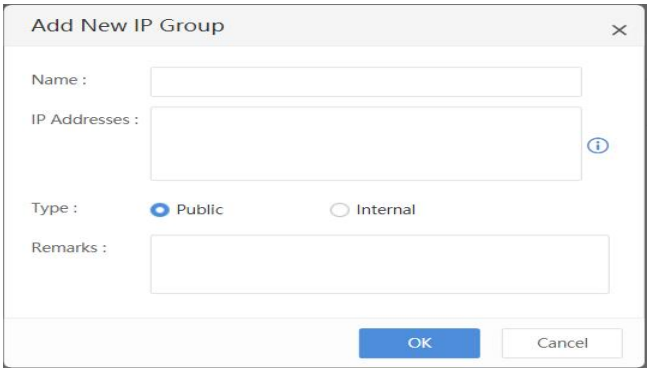
2. After editing the information, click **OK** to complete the creation. You can specify tags for server endpoints on the **Business Assets** page to better invocate micro-segmentation policies and display traffic statistics.

### 3.4.2.3 Creating an IP Group

The **IP Groups** page allows you to classify internal and public IP addresses to corresponding IP groups. The NovaGuard 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 the 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.

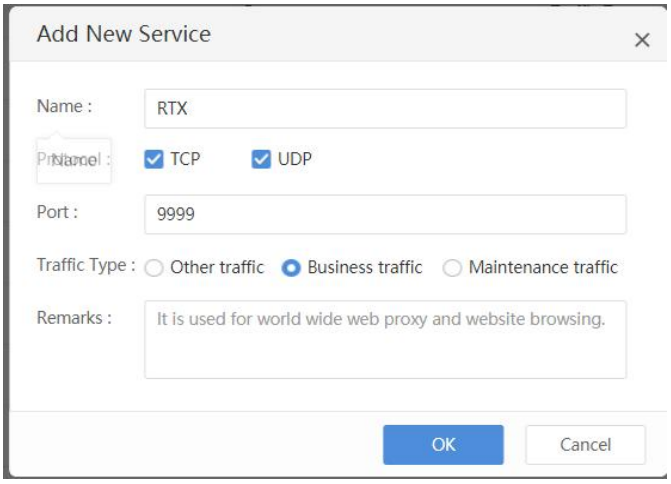
### 3.4.2.4 Creating a Service

You can define service ports on the **Services** page for invoking micro-segmentation policies. The NovaGuard 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

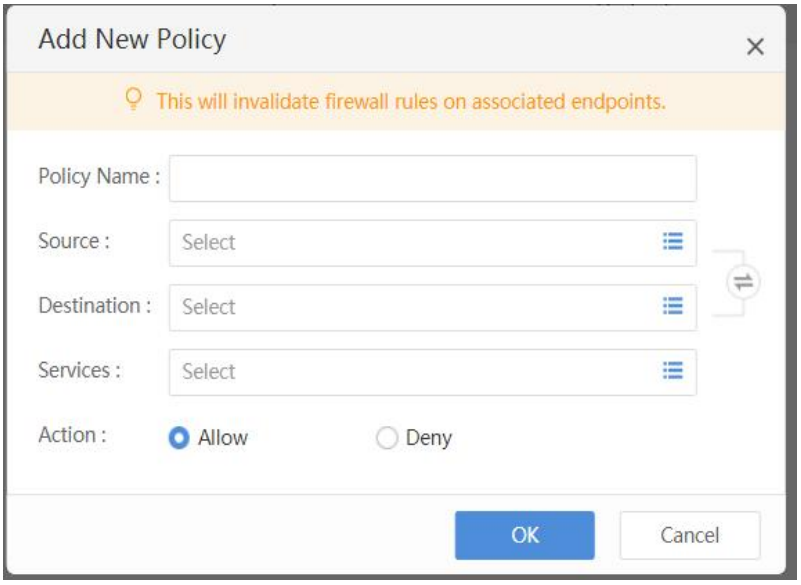
type to display the corresponding traffic statistics.

2. After the 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 enable or disable the function globally. 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**.

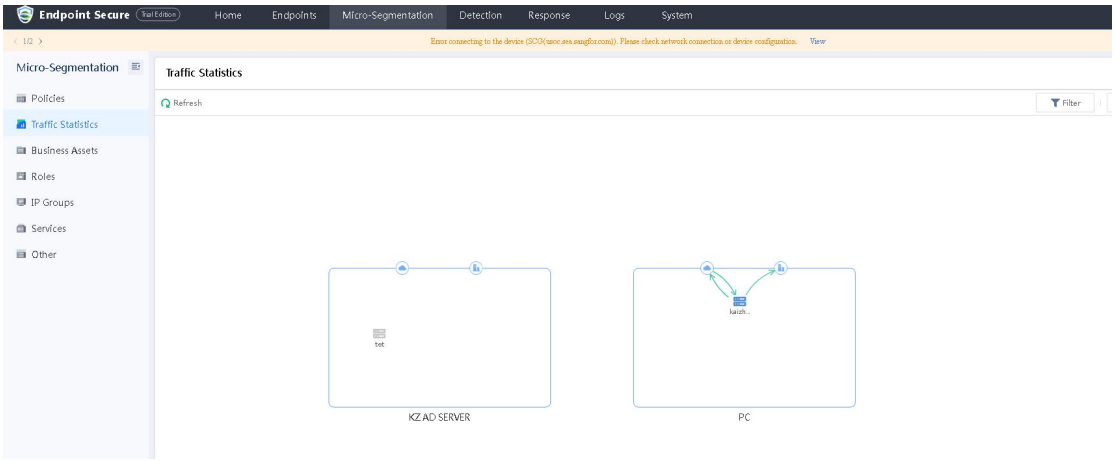
NOTE

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.

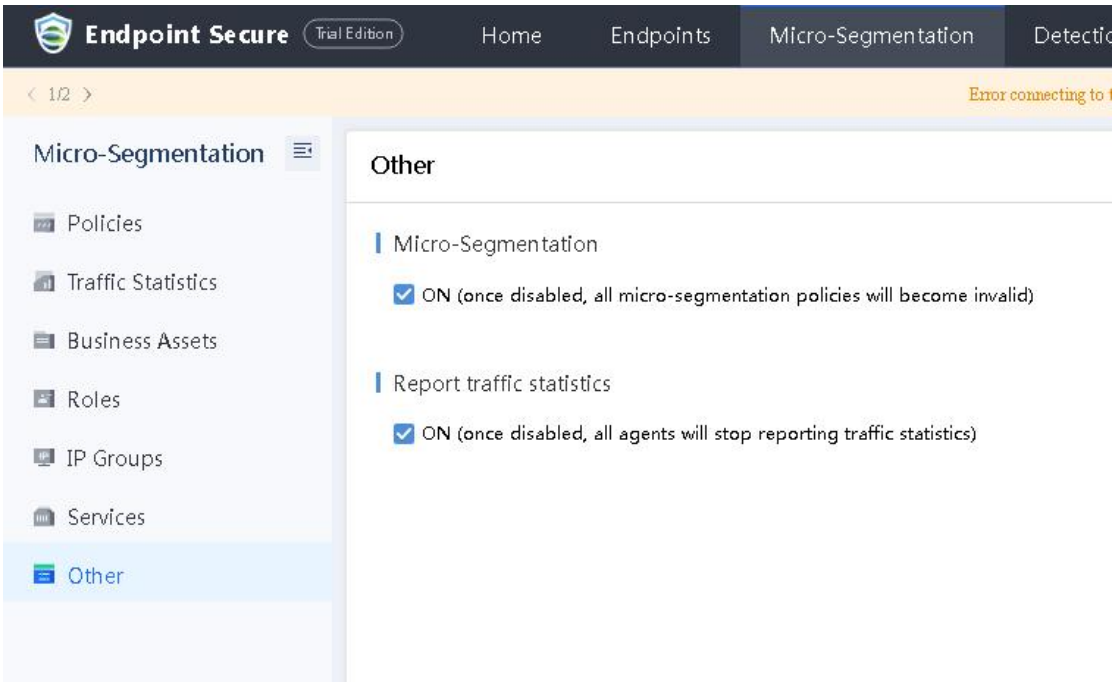



The options for **Filter** are as follows:

- **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 NovaGuard Manager. It scans malicious files of endpoints using the local file reputation database, Engine Zero, Behavioral Analysis Engine, Gene Analysis Engine, and Cloud-Based Engine.

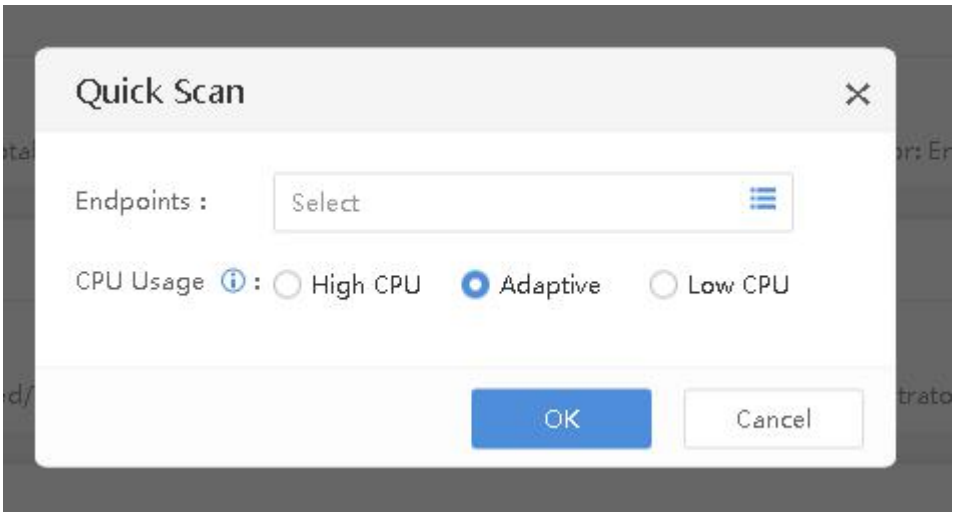
Virus scan modes include **Quick Scan, Full Scan,** and **Forced Scan**. You can click the

triangle pointer next to **Quick Scan** to select a scan mode from the drop-down list. The following table describes the differences between quick scan, full scan, and forced scan.

| | |
|---|---|
| **Full Scan** | Scan all disk files of an endpoint. |
| **Quick Scan** | Scan critical directories in the system disk. Critical directories include:<br>Windows:<br>/Windows and Windows/system32<br>/Windows/system32/drivers and its subdirectories<br>Linux:<br>/bin, /sbin, /usr/sbin, /usr/bin, /lib, /lib64<br>/usr/lib/usr/lib64, /usr/local/lib, /usr/local/lib64,<br>/tmp, /var/tmp, /dev, /proc<br>MacOS:<br>/private/tmp, /Users/″ Username″ /Downloads, /Users/″ Username″ /Desktop, /Users/″ Username″ /Documents |
| **Forced Scan** | For some customer scenarios where it is difficult to deal with stubborn viruses, you can issue special killing tools in batches on the NovaGuard Manager platform to help customers respond quickly when large-scale infections are challenging to handle.<br>Currently only supports Windows systems. |

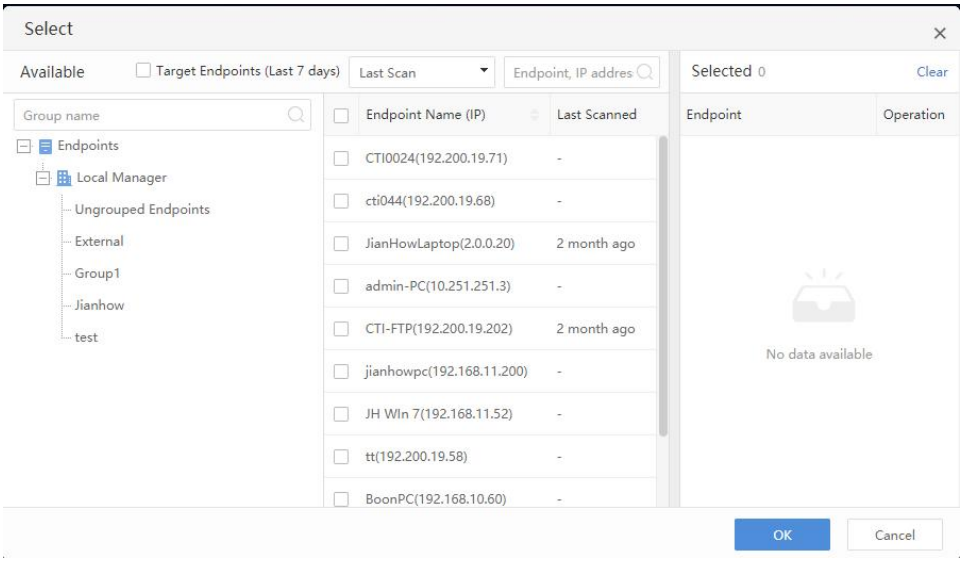
Table 7: Differences between Full scan, Quick scan, and Forced Scan

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.

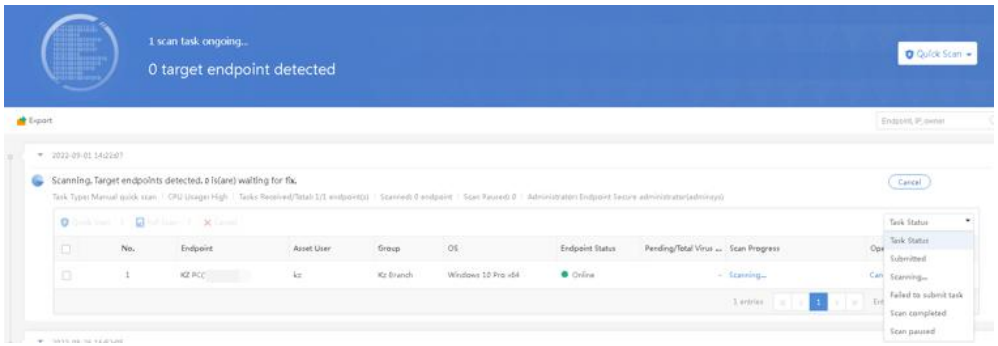


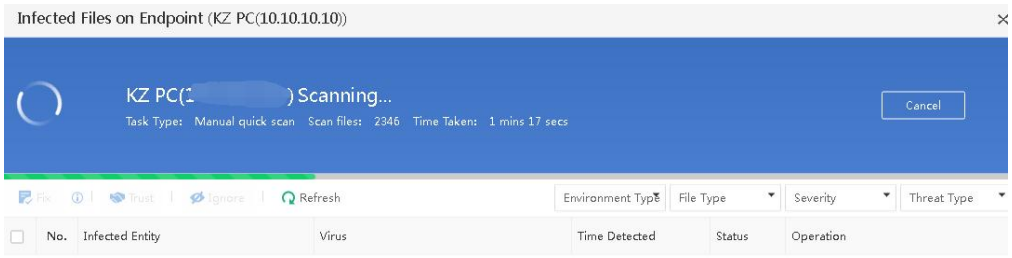

**CPU Usage**: The options include **High**, **Adaptive**, and **Low**. Their differences are as follows:

- **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%.)
- **Adaptive**: During scanning, the CPU usage is intelligently adjusted according to the endpoint usage to ensure that endpoint services are not stuck.

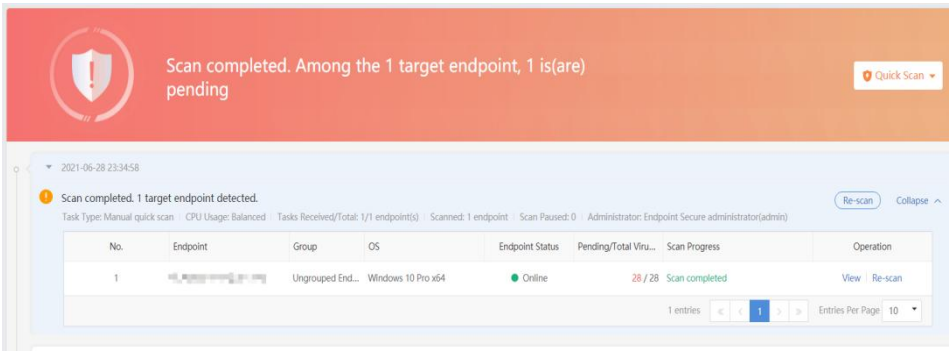
- **Low**: Fewer CPU resources are occupied during scanning, and the CPU usage cannot exceed 10%. (In resource optimization mode, the CPU usage does not exceed 5%.)

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.

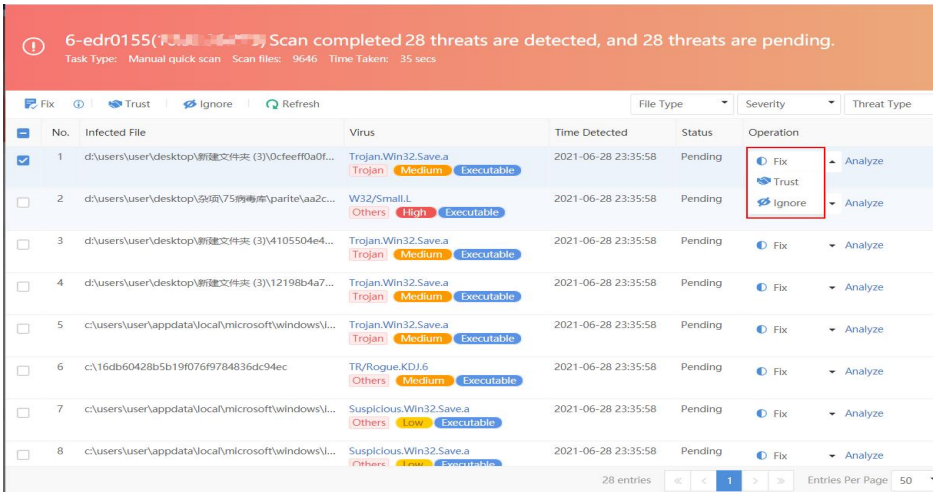


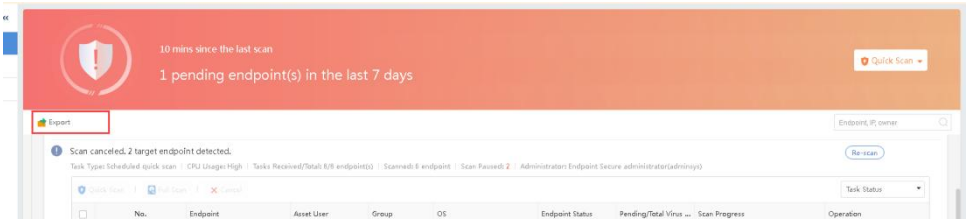

3. After the virus scan is complete, you can view the scan result. The displayed information includes the task type, scan mode, task received/total endpoints, scanned endpoints, scan paused endpoints, endpoint name, IP address, group, operating system, status, pending viruses, total viruses, and scan 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, click the drop-down list icon next to Fix, and select **Fix**, **Trust**, or **Ignore** for a virus, as shown in the following figure.




5. You can export the virus scan record, as shown below:




**Virus Scan Task Records**

| | |
|---|---|
| **Summary** | 1 out of exported 1 entries are found and exported. |
| | **Filter** |
| **Time** | - |
| **Sort by time** | Descending |
| **Period** | Export the records of the last 1 task(s) (Note: Only a maximum of 100, 000 records can be exported) |
| | **Result** |

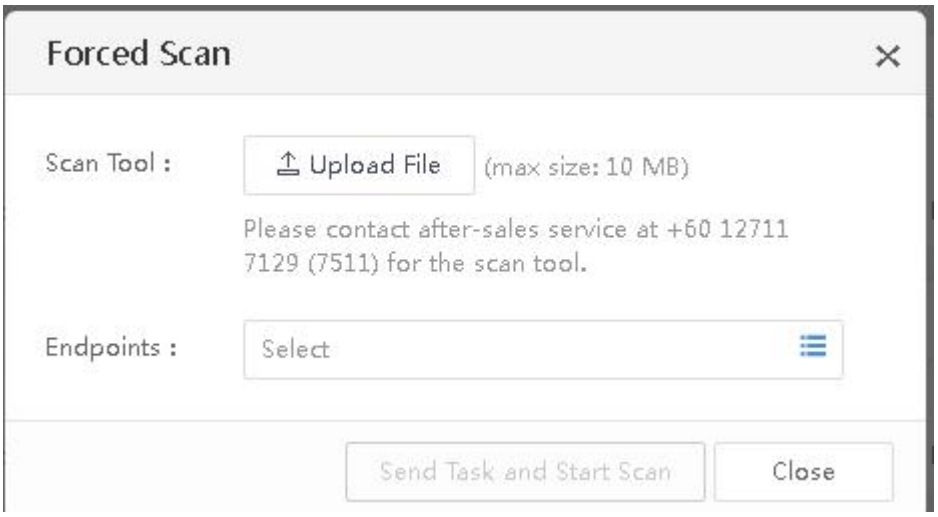
| No. | Time Sent | Endpoint | Owner | Group | OS | Endpoint Status | Pending/Total Viruses | Scan Progress | Task Type | Scan Mode |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2022-09-01 14:22:07 | KZ PC(10.10.10.10) | kz | Kz Branch | Windows 10 Pro | Online | 0/0 | Scan completed | Manual Quick Scan | High CPU |

## 3.5.1.1 Forced Scan

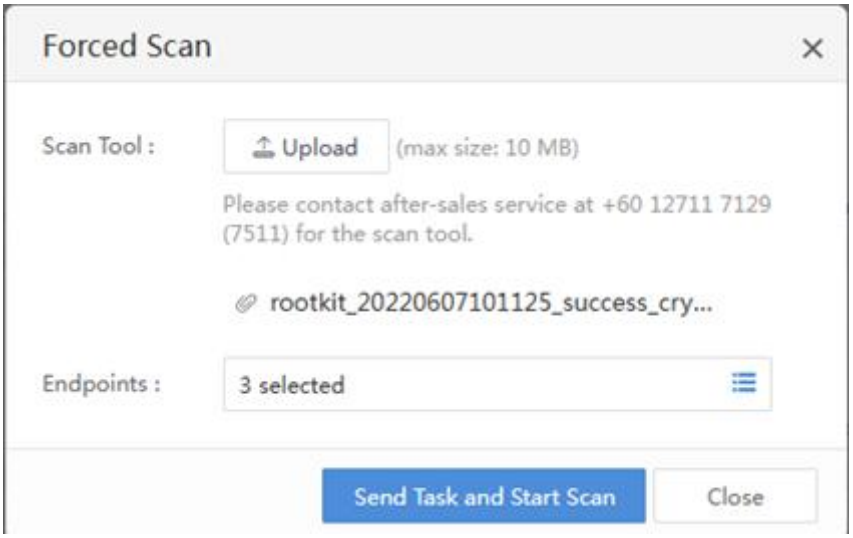
For some customer scenarios where it is difficult to deal with stubborn viruses, anti-virus tools can be distributed in batches to the NovaGuard Manager to help customers quickly respond to large-scale infections of difficult-to-handle viruses. Only Windows systems are supported for the time being.

Click **Forced Scan** to enter the configuration interface, as shown in the figure below.

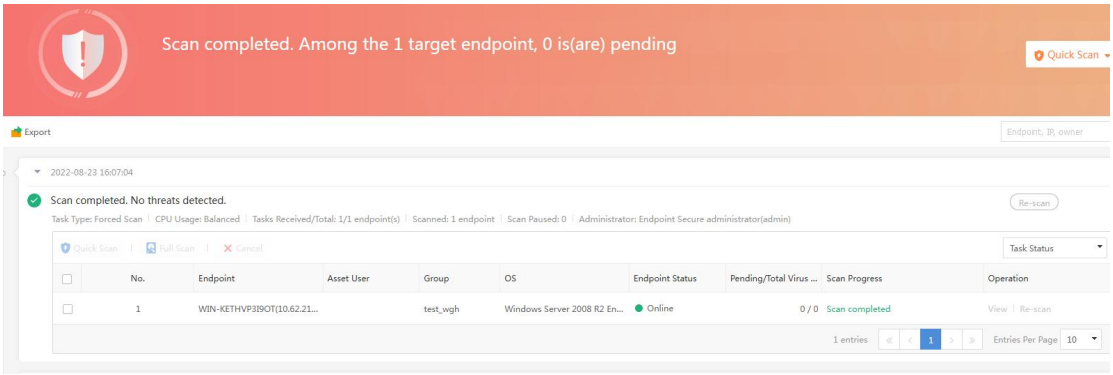





Upload the scan tool, select the Windows endpoint to be distributed, and click **Send Task and Start Scan.**




If the status of the scan progress is **Scan completed**, indicating that the execution of the scanning tool is complete.

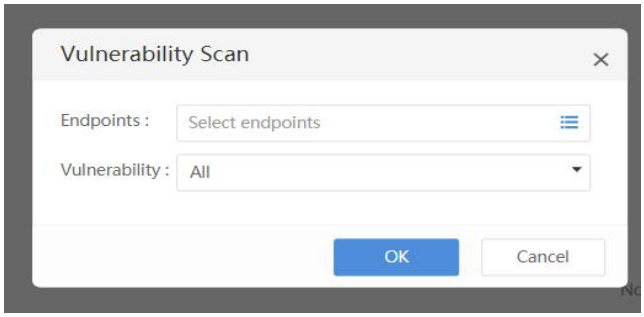


## 3.5.2 Vulnerability Scan

The **Vulnerability Scan** can detect Windows endpoint system vulnerabilities, Linux endpoint system vulnerabilities, and application vulnerabilities. It supports the patching of Windows endpoint system vulnerabilities, and for Linux, it only provides repair suggestions for Linux endpoint system vulnerabilities and application vulnerabilities currently.

### 3.5.2.1 Windows Vulnerability Scanning and Patching

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

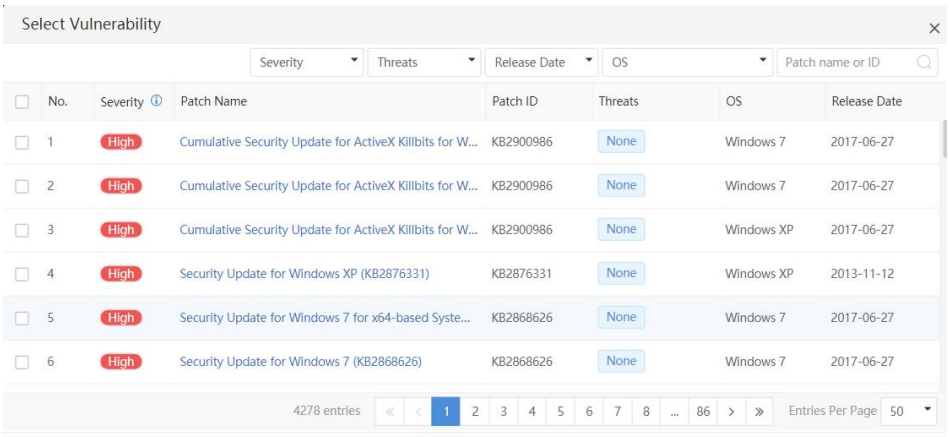



The parameters are as follows:

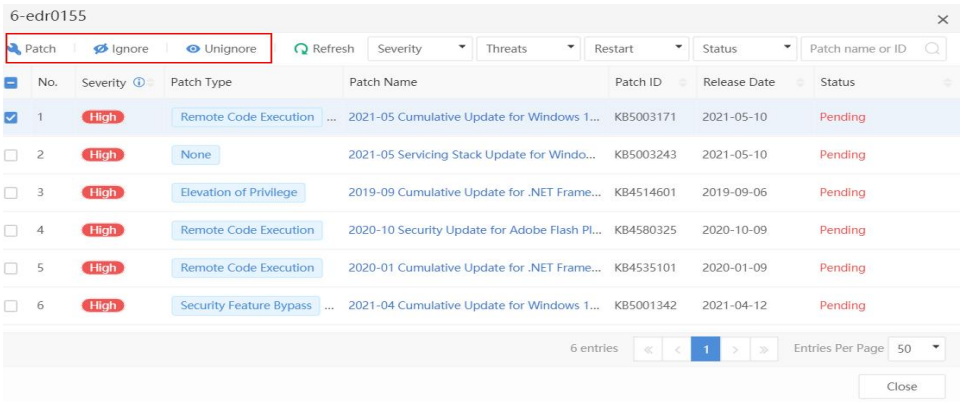
**Endpoints**: On the **Select** page, you can view endpoints not scanned in the last week, last month, or last three months, and the last scanning time to filter endpoints that need to be scanned. You can also enter an endpoint name or IP address in the search box to search for the specific endpoint.

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

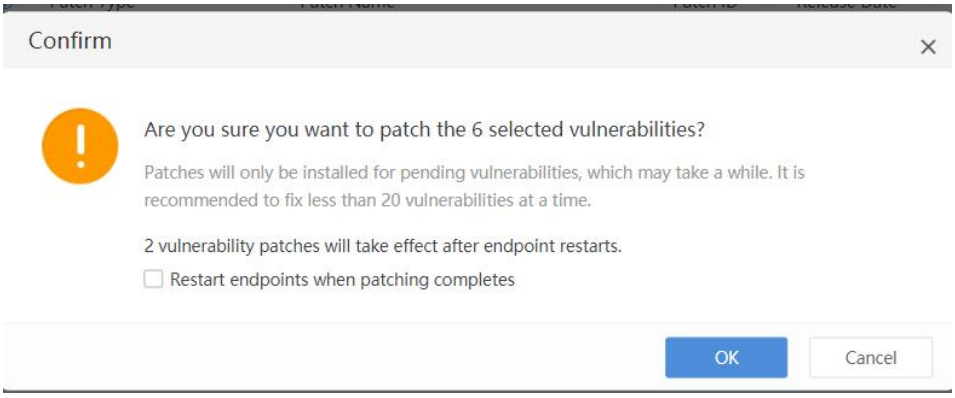
- **All**: Scan and fix the RCE, DoS, privilege escalation, security feature bypass, and information leakage vulnerabilities.
- **High**: Scan and fix only high-severity vulnerabilities. Select **High** from the vulnerability severity drop-down list box on the **Select Vulnerability** page for details 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**. A prompt shown in the following figure will be displayed when patching starts if a restart is required for the patch to take effect. Select **Restart endpoints after patching completes** 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 during the off-work time.

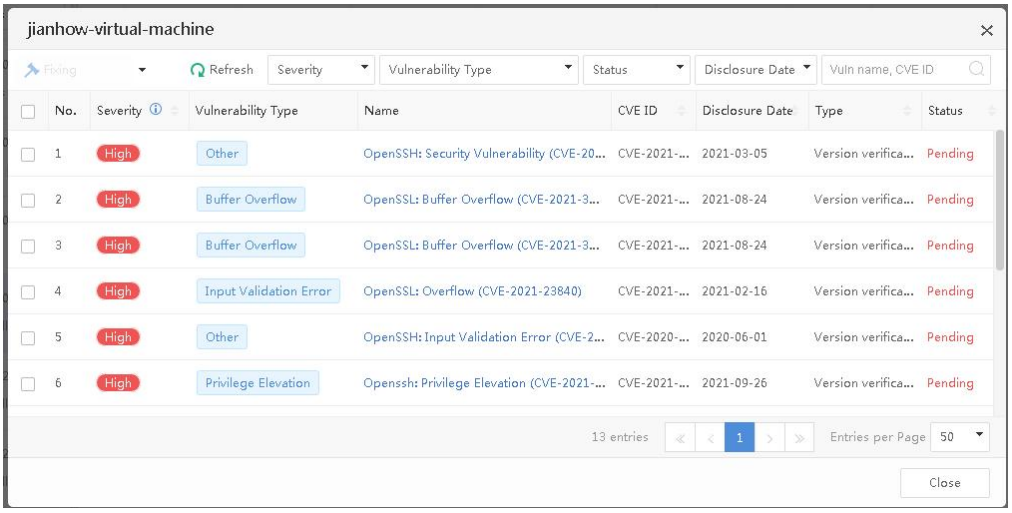



NOTE

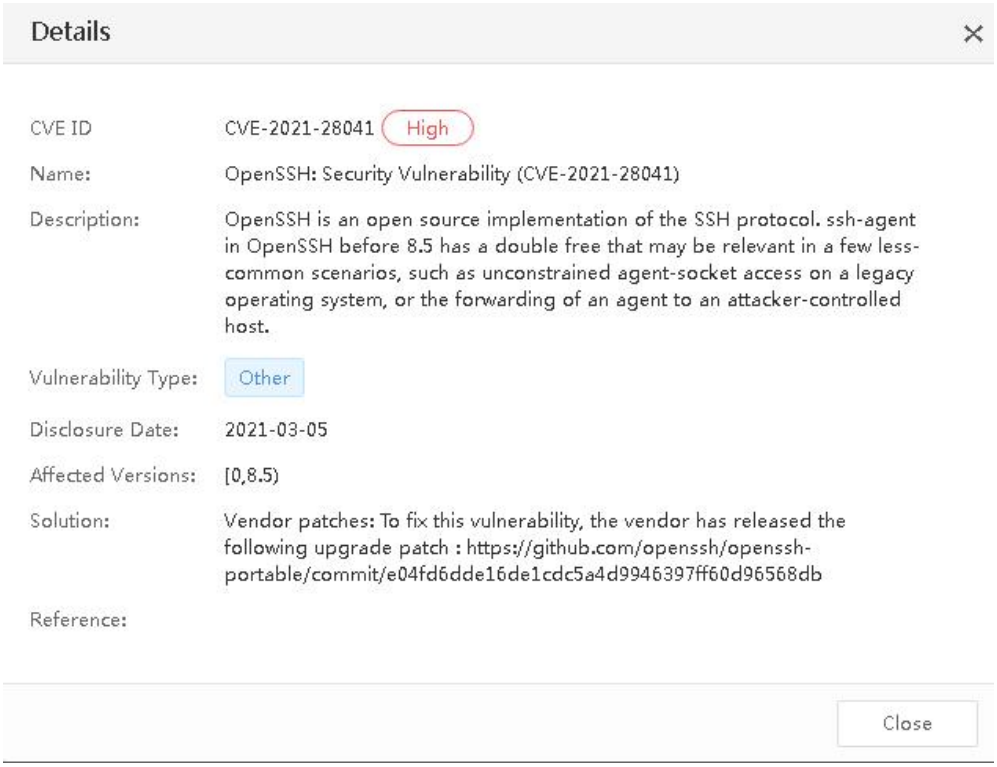
Vulnerability patching mentioned in this section requires endpoint PCs to be able to access the Internet. If an endpoint PC cannot access the Internet, patch vulnerabilities by referring to Chapter 3.6.5 Remediation.

### 3.5.2.2 Linux Vulnerability Scanning

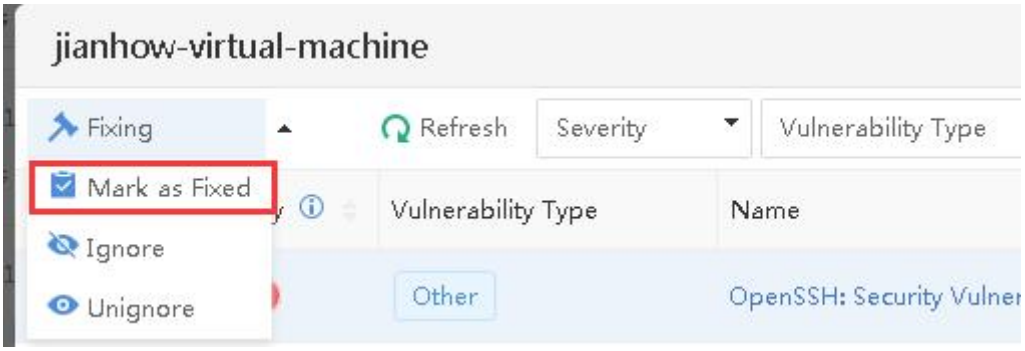
Create a Linux vulnerability scan task by referring to Windows vulnerability scanning, as shown in the following figure, for details of Linux vulnerability scanning.




Click the vulnerability name to view the vulnerability details and solution, as shown in the figure below.




After the administrator manually confirms or fixes the Linux vulnerability, if the status still shows **Pending**, you can click **Mark as Fixed** to manually mark them as handled, ignore or unignore operation.




**NOTE**

NovaGuard supports Linux systems and Linux application vulnerability scanning. It does not support Linux systems and Linux application vulnerability automatic patching. Administrators can manually repair according to the vulnerability solution. NovaGuard supports Windows system vulnerability scanning and solution.

## 3.5.3 Security & Integrity Check

The **Security & Integrity Check** module is for compliance checks of endpoints. The check

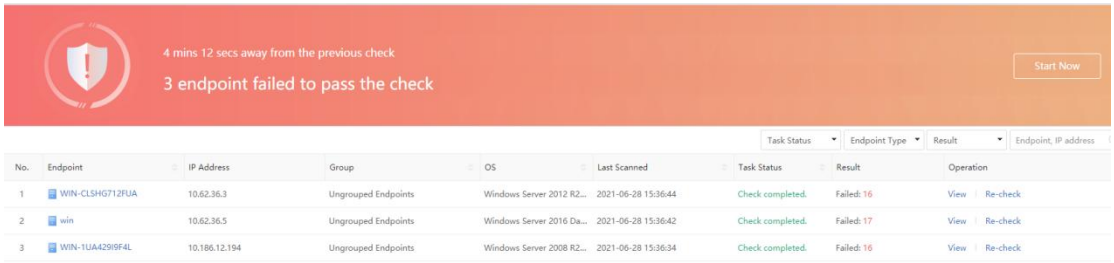
content varies depending on the endpoint operating system.

**Windows endpoints**: identity identification, access control, security audit, history information protection, intrusion prevention, and malicious code prevention

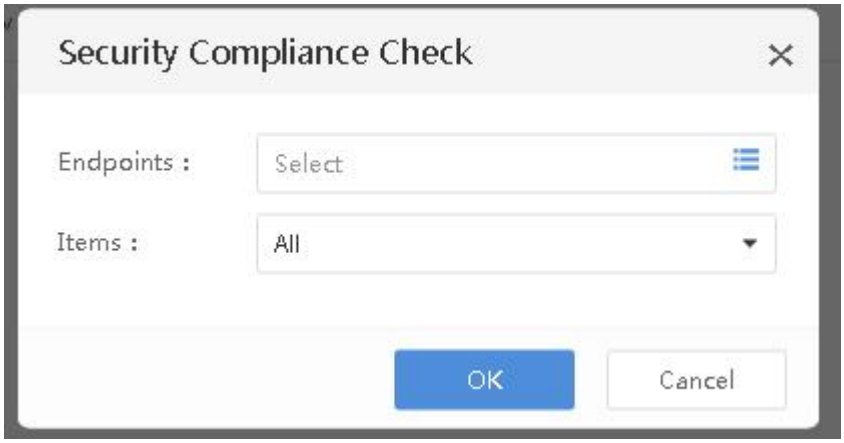
**Linux endpoints**: identity identification, access control, security audit, SSH policy detection, intrusion prevention, and malicious code prevention

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

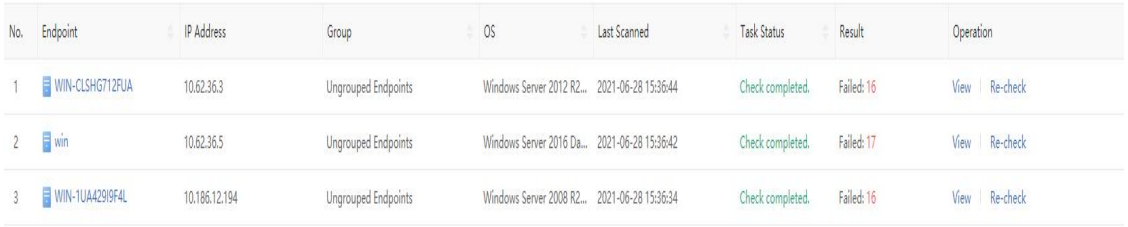
The following figure shows the configuration page.



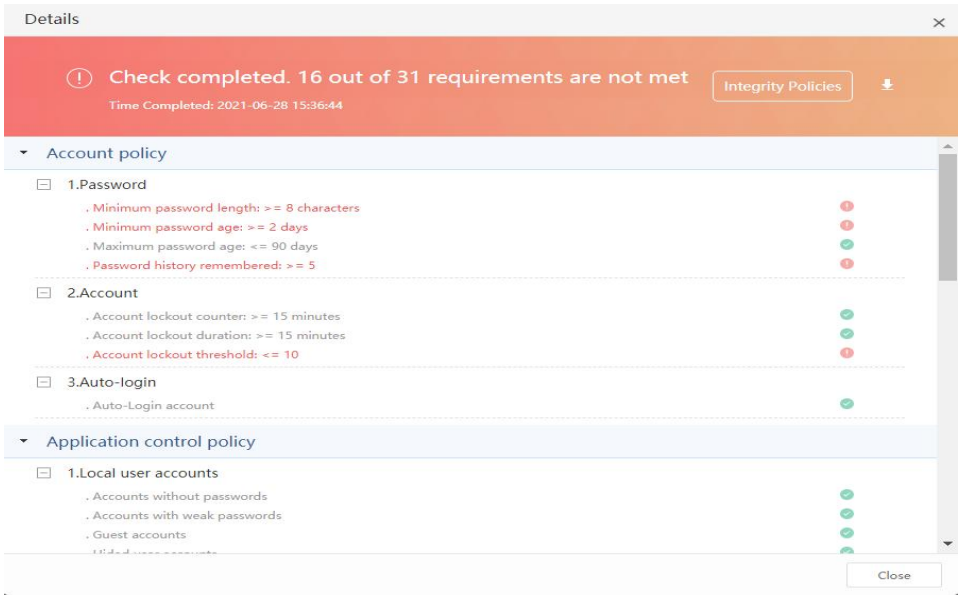

Click **Start Now** and select endpoints for which a compliance check is required, as shown in the following figure.




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




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




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




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

You can click  to download the compliance check report.

---

**WARNING**

Pay attention to compliance check items in orange.

---

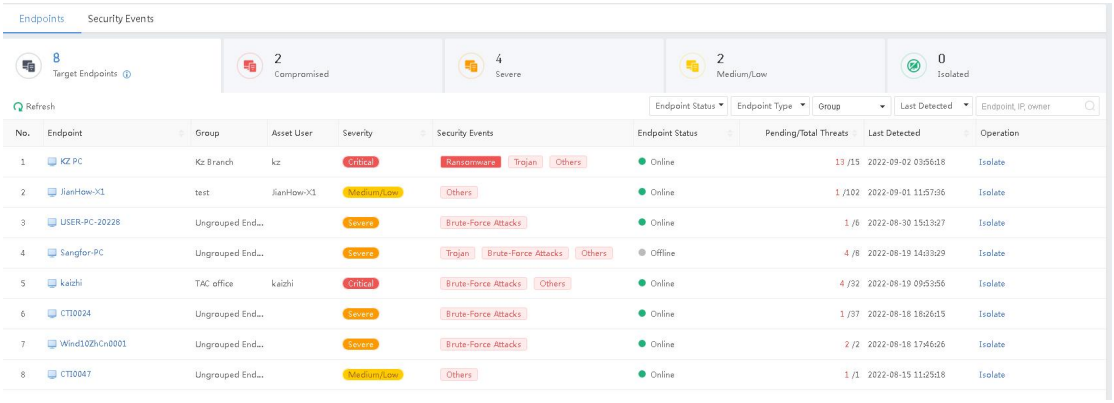
# 3.6 Response

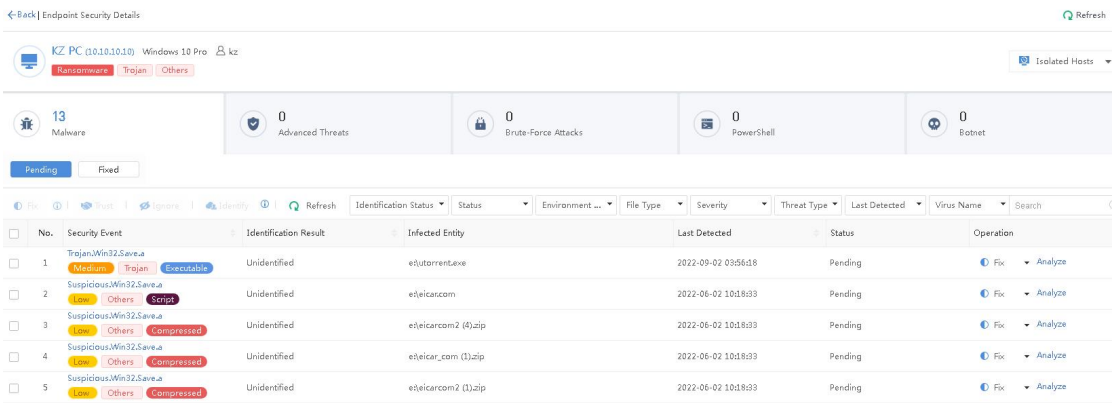
## 3.6.1 Threat Response

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 Status, 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 filter endpoints by **Endpoint Status, Endpoint Type**, **Group**, and **Last Detected**. On the **Endpoints** tab, you can click the endpoint name to jump to the **Endpoint Security Details**, handle the threat, and isolate the endpoint. The **Endpoints** and **Endpoint Security Details** are as follows.



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, WebShell backdoors, suspicious parameters execution, 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**. Select infected files/processes and click **Fix**, **Trust**, or **Ignore** on the displayed page. 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

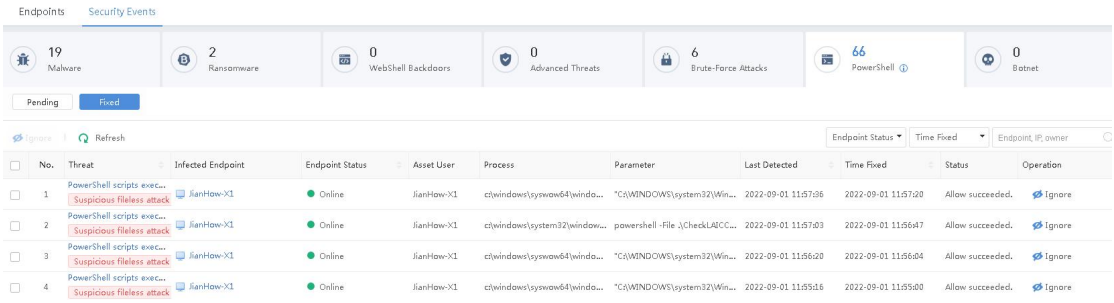
To ensure security, **Fix** is not available for brute-force attacks, and brute-force attacks need to be added to the blacklist manually.

## 3.6.3 Security Events

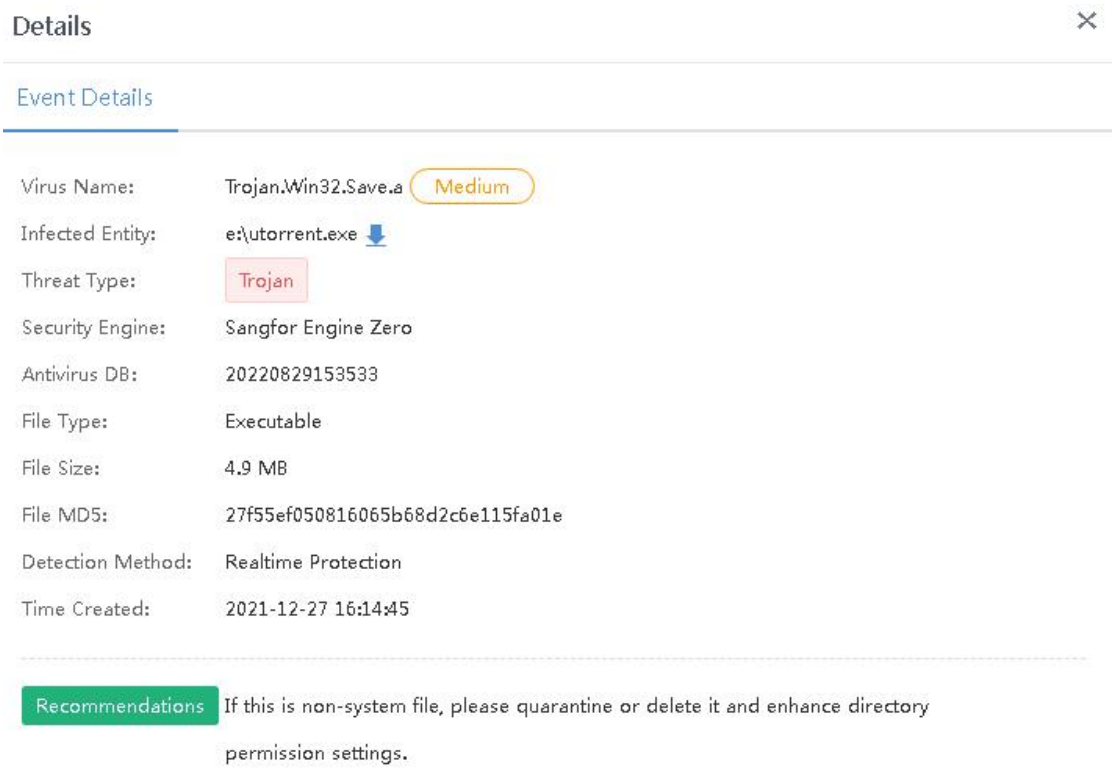
On the **Security Events** tab, you can select a security event type (including Anti-**Malware**, **Ransomware**, **Brute-Force Attacks, Botnet, WebShell Backdoors**, and **Advanced Threats**) to view the corresponding security event names, infected endpoints, infected files, detection time, and handling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

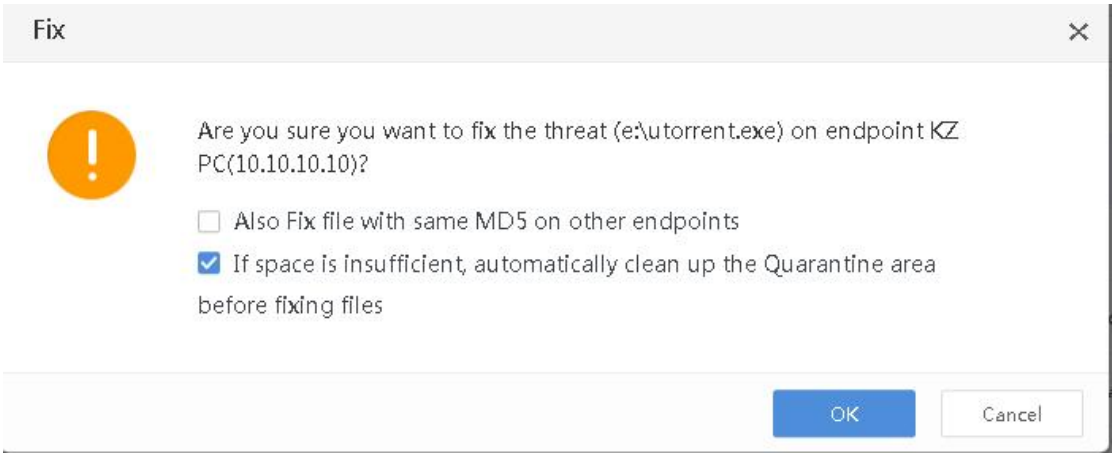
You can filter security events by handling status and severity. You can also select multiple security events for batch operations.

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 the security event to view the details, such as the virus name, infected file, virus type, detection engine, and handling suggestions.




**NOTE**

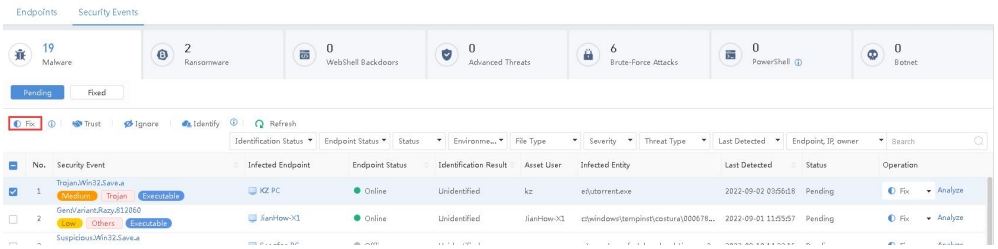
For the **Fix** and **Trust** operations, you can select **Also fix file with the same MD5 on other endpoints** to batch process the same files on other endpoints.

Select **If space is insufficient, automatically clean up the Quarantine area before fixing files**. If the endpoint quarantine area is detected full, the files in the quarantine area will be automatically cleaned up and then quarantined.

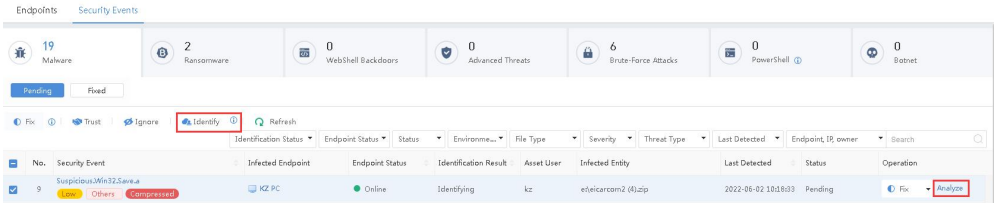
When **If space is insufficient, automatically clean up the Quarantine area before fixing files** is selected. 50% of the files in the endpoint quarantine area will be automatically cleaned up in the order of the quarantined files.

### Pending Status

The tab shows all detected open threat events. You can select **Fix**, **Trust**, or **Ignore** for specific threat events. Select the threat file to be quarantined and click **Fix**, as shown in the figure below.

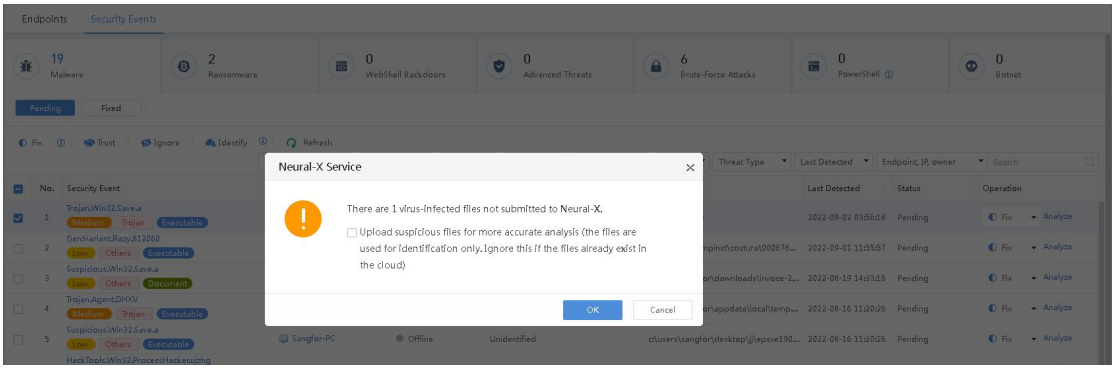



If you are unsure whether the file is malicious, you can use the **Identify** or click **Analysis** for further analysis and judgment by the intelligence center.

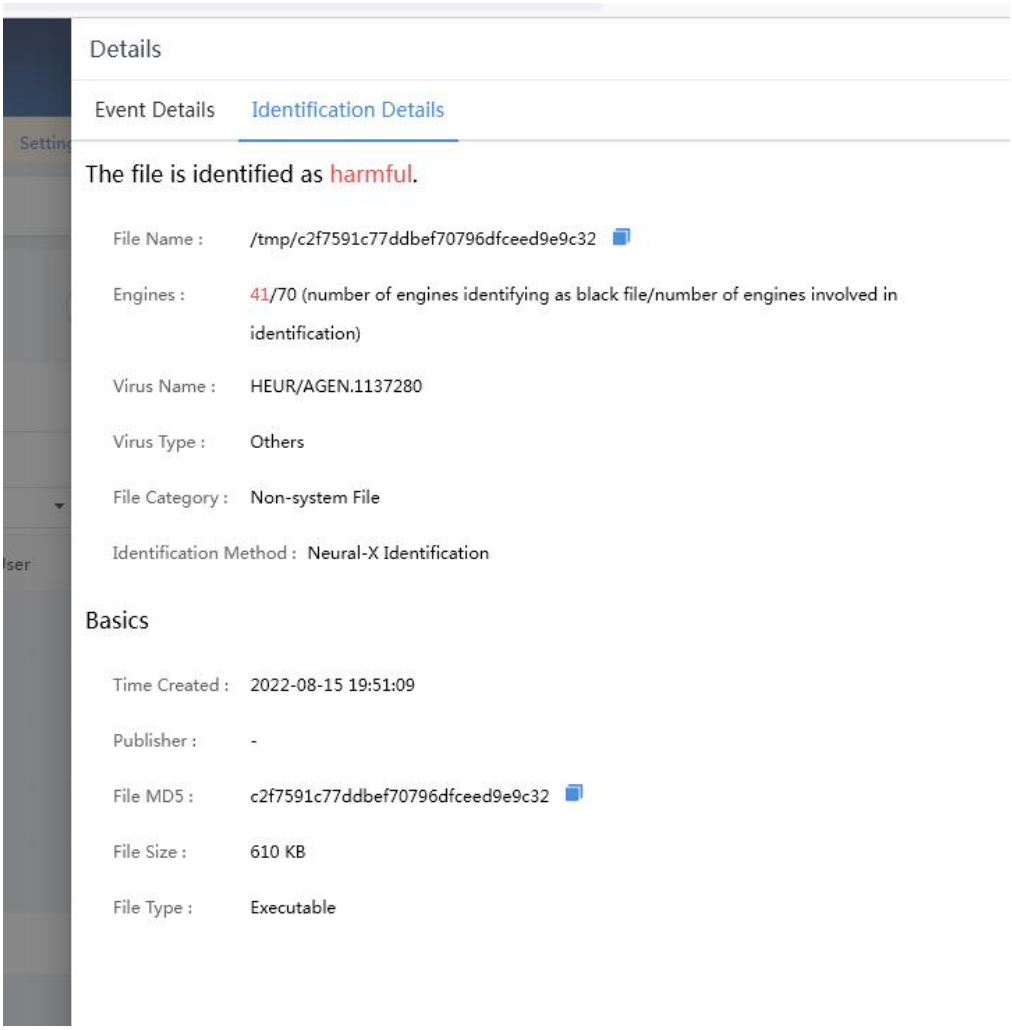



The Neural-X service provides file identification capabilities enabled by security experts, sandboxes, and engines. In addition, it analyzes files using the Cloud-Based Engine and intelligence. It filters out fuzzy matches and only provides identification results of confirmed black or white files, providing you with more accurate identification results so that event handling can be closed-loop.

When the NovaGuard manager can connect to the Internet, the detected threat files will be automatically sent to the cloud and identified, and return the identification results. For unidentified files, manual cloud identification can be performed.

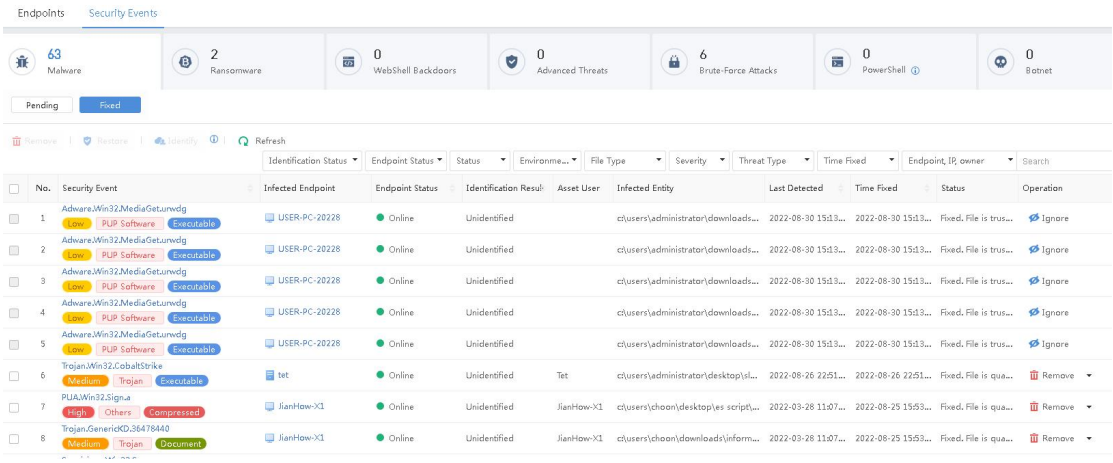



After identification is complete, you can click the **View** button to view the detailed results of the identification.

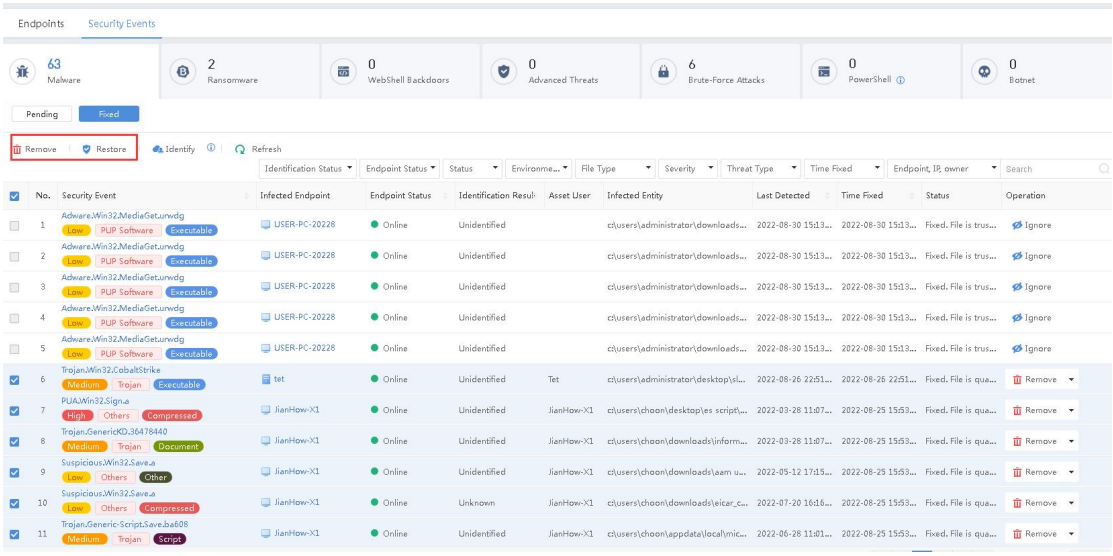



**Fixed Status**

The tab displays all threat files added to the quarantine area, and you can completely remove or restore the files, as shown in the figure below.




Select the threat file and click **Remove** to delete the endpoint quarantine files in batches, and click **Restore** to restore the quarantined files in batches, as shown in the figure below.




It supports the removal of 10,000 threat files at a time.

## 3.6.4 Advanced Threats

**Applicable scenario:**

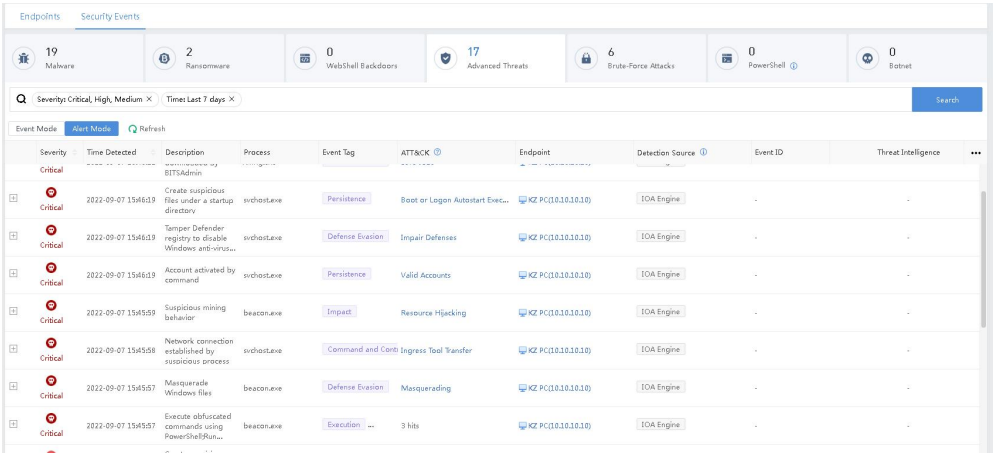
For new threats, offensive and defensive confrontation scenarios, such as ransomware attacks, phishing emails, etc., where the office network is used to break through the intranet, the IOA rules can be used to match the abnormal behaviors of related attacks such as ransomware and phishing (refer to att&ck, such as abnormal injection, stealing credentials, privilege escalation, etc.)

Provide timely alert threat information and intercept high-risk actions. At the same time, trace the process chain where the attack threat program is located, aggregate all abnormal behaviors to form accurate security events, assist in finding the source of the attack, and provide closed-loop to startup item ability to ensure it is cleaned up.

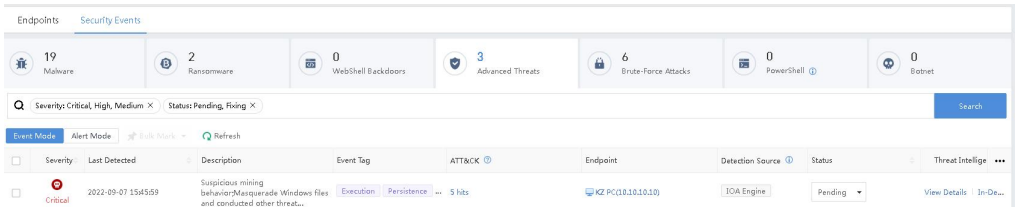
**Case Study:**

The following is a case of mining incidents to describe the use of advanced threats.

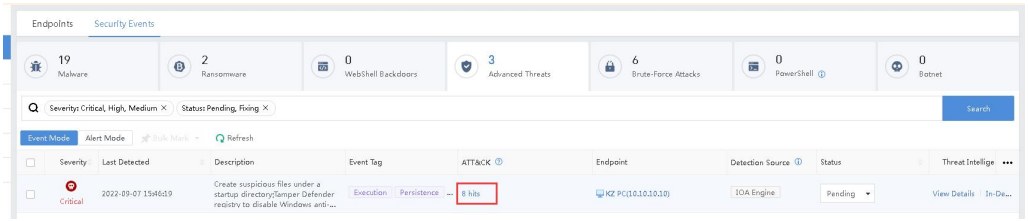
During the routine operation and maintenance process, the security administrator found that the NovaGuard advanced threat detected multiple alerts of suspicious behaviors such as mining behavior, account activation, and suspicious file creation, as shown in the figure below.



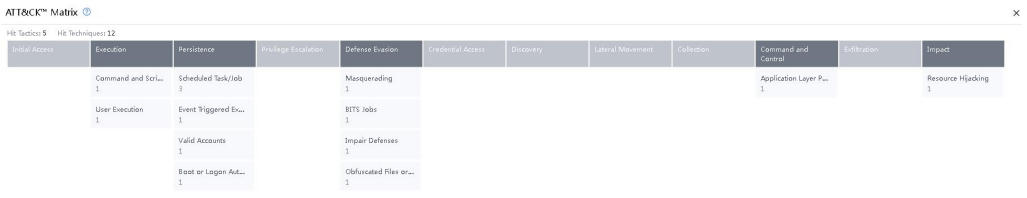

View the security events, NovaGuard detected a security event with a Critical threat level, as shown in the following figure. NovaGuard aggregates multiple suspicious behaviors of the endpoint into a complete attack event for display.



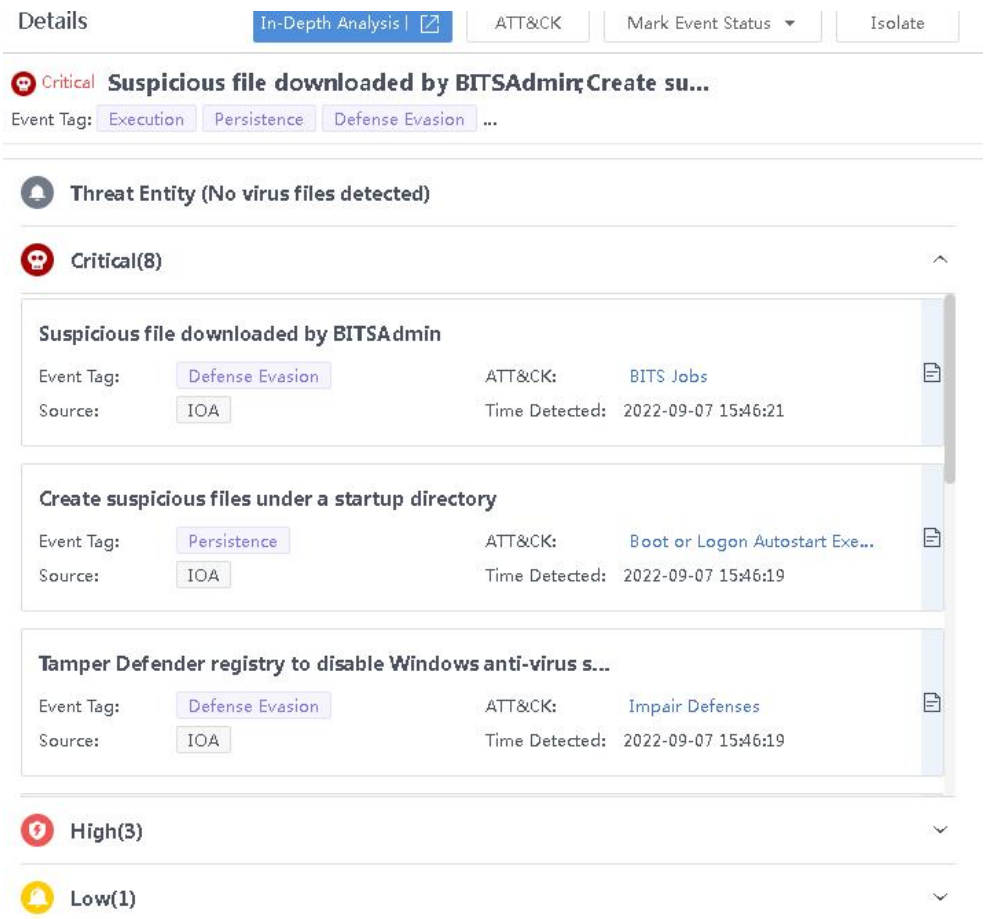

View the security events, and many matches the ATT&CK threat matrix model, as shown in the following figure.




Attacks repeatedly hit tactics such as execution, persistence, defense evasion, command and control, and impact in the ATT&CK threat model.




Click the security event **View Details** to view the threat entity and abnormal behavior report of the security event.

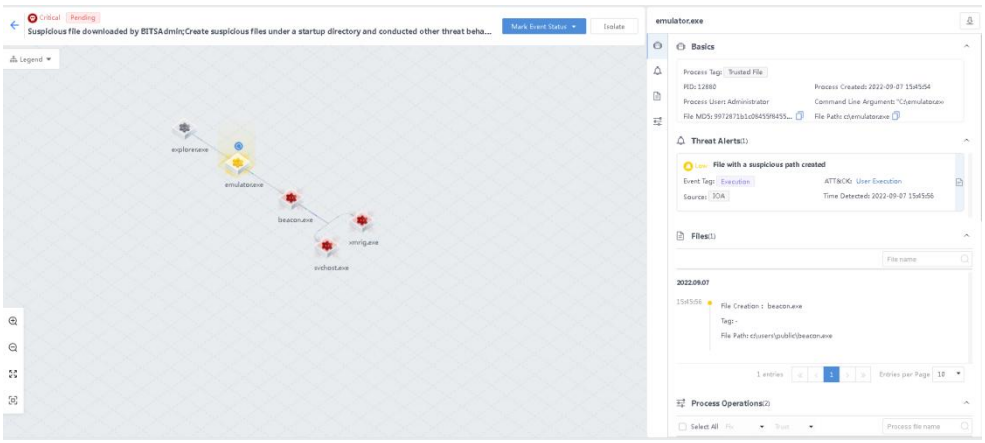



Click the **In-Depth Analysis** to perform a visual traceability analysis of the process attack chain.



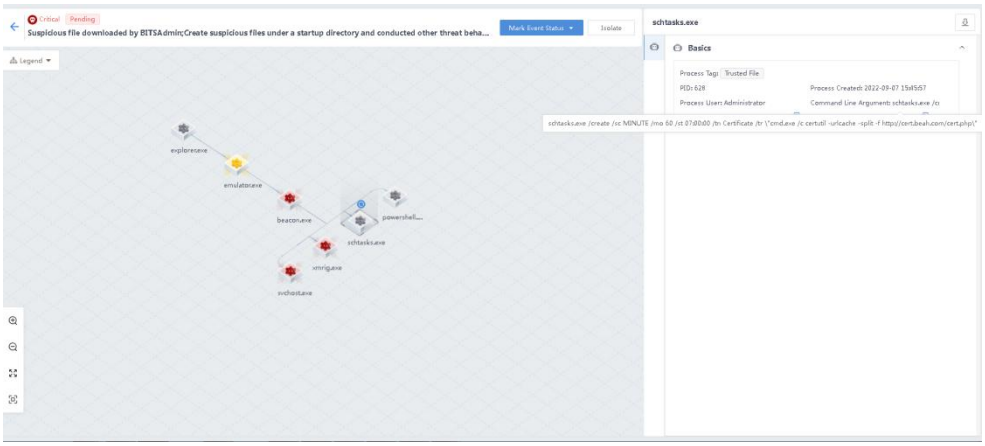

1. Attack entrance

The attacker logs in through the remote desktop to obtain the permission of the test machine and drops the attack sample emulator.exe. The beacon.exe file and process are automatically created after the sample is executed.



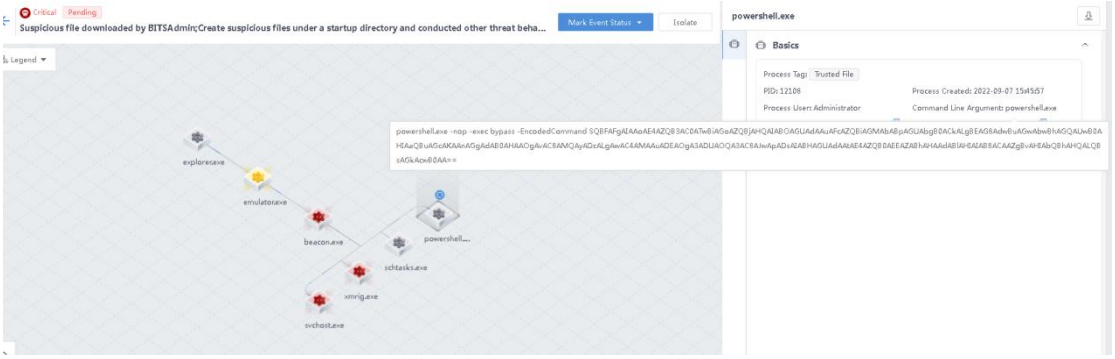
2. Create suspicious task plans to achieve persistent attacks

beacon.exe creates the schtasts.exe process and a suspicious task plan through the schtasts.exe process to implement persistent attacks.



3. Execute obfuscated PowerShell commands to bypass security protection and implement attacks.

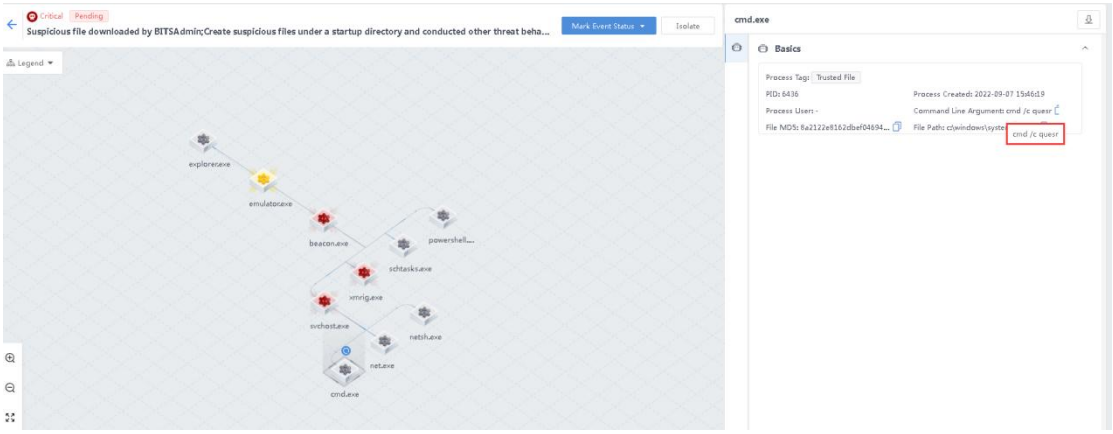
beacon.exe creates the powershell.exe process, which bypasses security protection and implements attacks by executing obfuscated PowerShell commands.



4. Detect host users to collect information

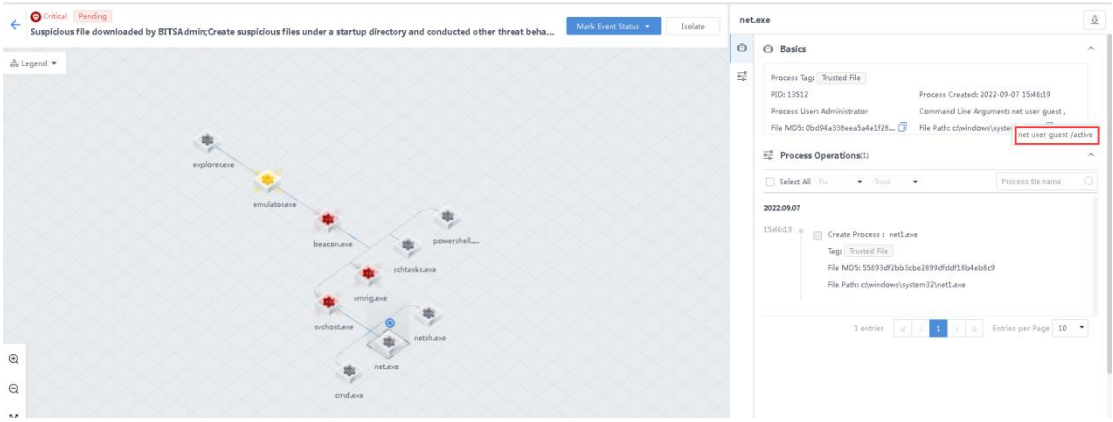
beacon.exe creates the svchost.exe process and invokes the command cmd /c quser to detect

the host user information to achieve information collection.



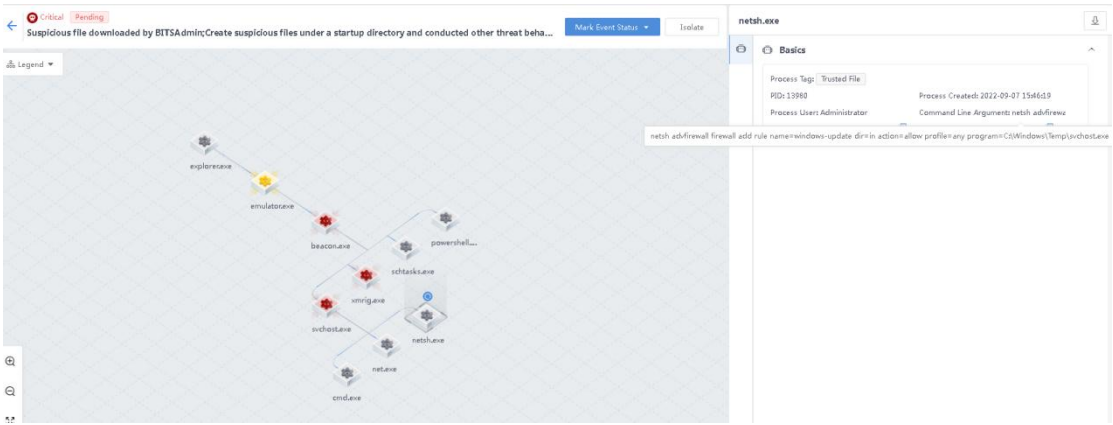

5. Activating the host-guest user to implement persistent attacks.

beacon.exe creates the svchost.exe process and invokes the command net user guest /active to activate the host-guest user to implement persistent attacks.




6. Create a suspicious firewall bypass list via netsh

beacon.exe creates the svchost.exe process, invokes the command **netsh** to add firewall whitelist rules, establishes suspicious connections, and attempts to bypass the firewall security protection.

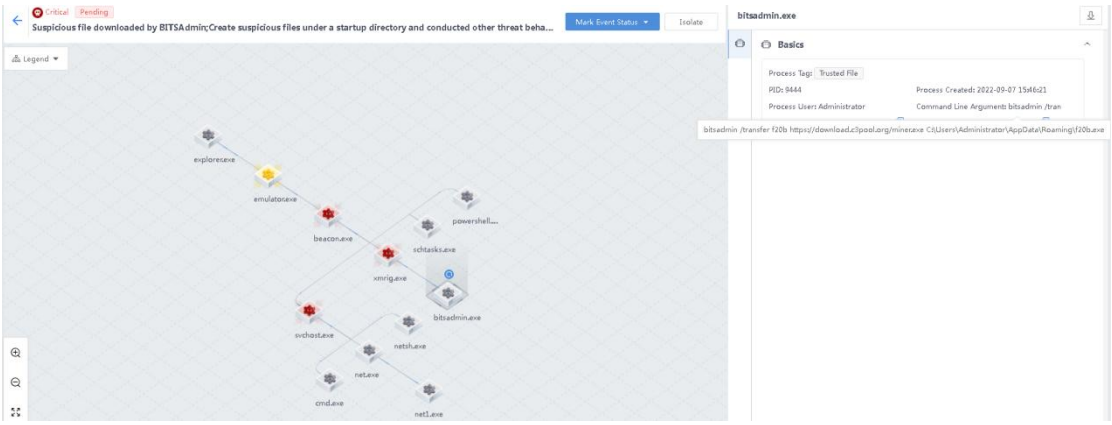


7. View current user permissions and collect sensitive information.

beacon.exe creates the xmrig.exe file and process, invokes the command cmd /c whoami to view the current user permissions, and collects sensitive information.

8. Download mining virus for mining

beacon.exe creates the xmrig.exe file and processes, and calls bitsadmin.exe to download the virus for mining.



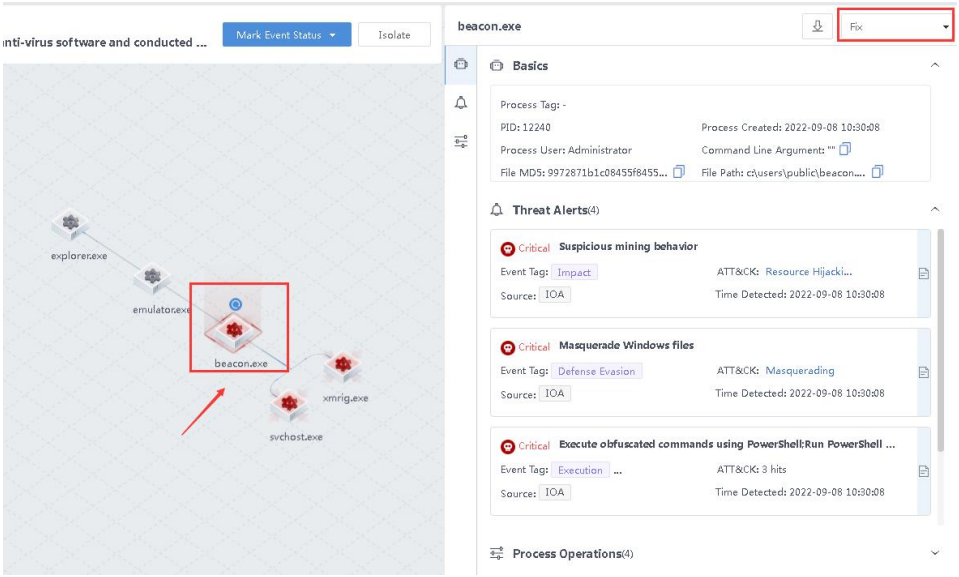

**Attack incident handling**:

1. Traceability summary:

The test machine was infected with a mining virus. The attack sample emulator.exe creates malicious files beacon.exe and xmrig.exe and pulls up multiple processes to complete attack behaviors such as execution, persistence, defense evasion, credential access, detection, and command and control.

2. The solution is as follows:

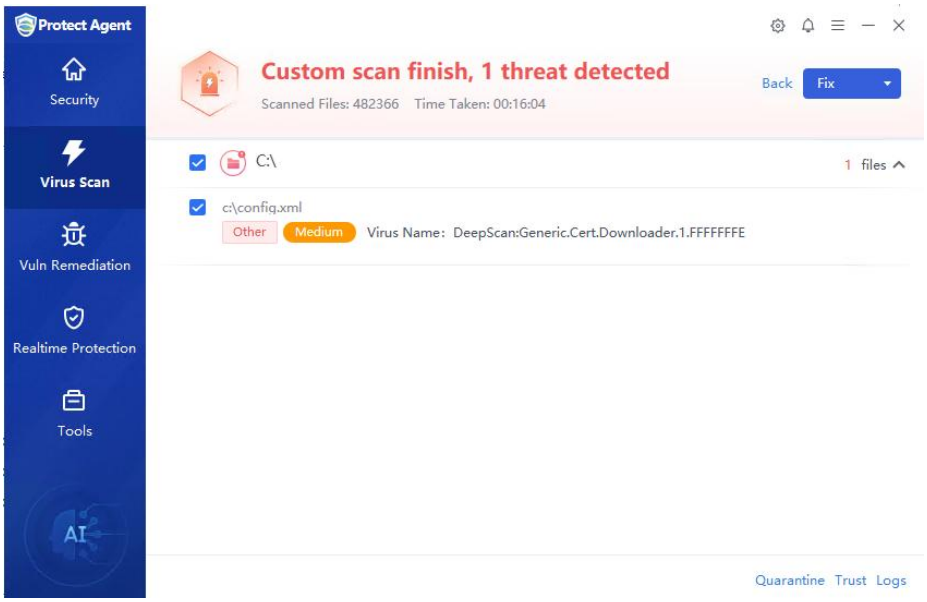
- Isolate malicious files emulator.exe, beacon.exe, xmrig.exe.




- Isolate the endpoint, isolate the endpoint without affecting the business, and avoid the horizontal spread of the threat.




- The threat endpoint conducts a comprehensive virus scanning and fixing and removes the residual items.




3. The attacker obtains permissions and implants viruses through remote desktop

login/brute force. The following reinforcement measures are recommended.

- Close unnecessary remote ports.
- Enables remote desktop login secondary authentication and brute force detection on NovaGuard.
- Update system security patches in time.

## 3.6.5 Remediation

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

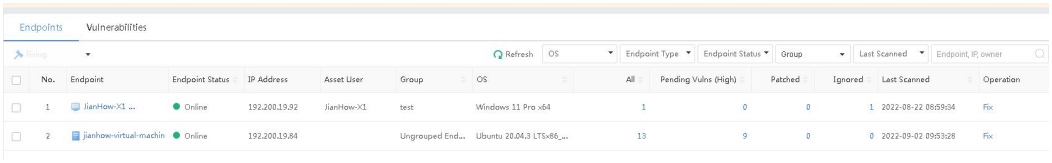
NOTE

Vulnerability patching can be performed after vulnerability detection is complete.

### 3.6.5.1 Vulnerabilities

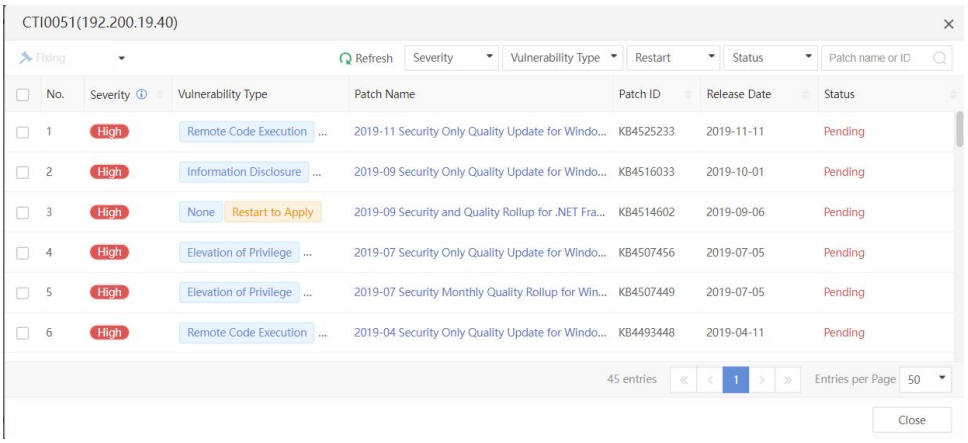
#### 3.6.5.1.1 Endpoints View

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



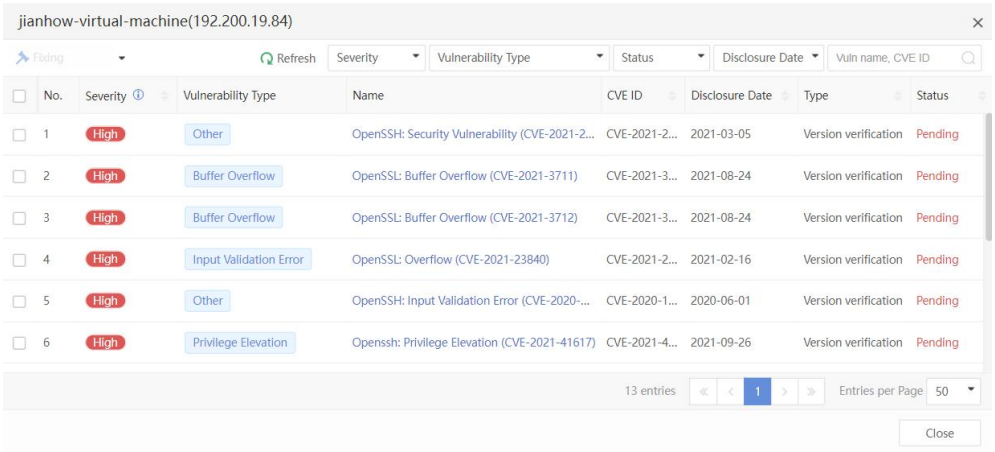

Click the **Fix** button under Operation for the Windows endpoints:

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.




Click the **Fix** button under Operation for the Linux endpoints:

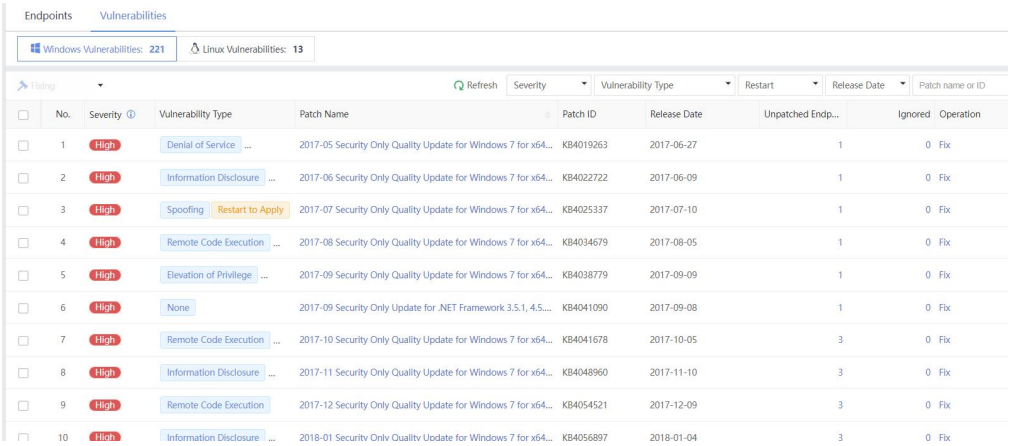
1. View a specific terminal's corresponding vulnerability severity, patch-related information, and repair status. You can filter by vulnerability severity, patch name, patch ID, Status, etc.
2. Check multiple patch information to perform a one-click patch or ignore it.



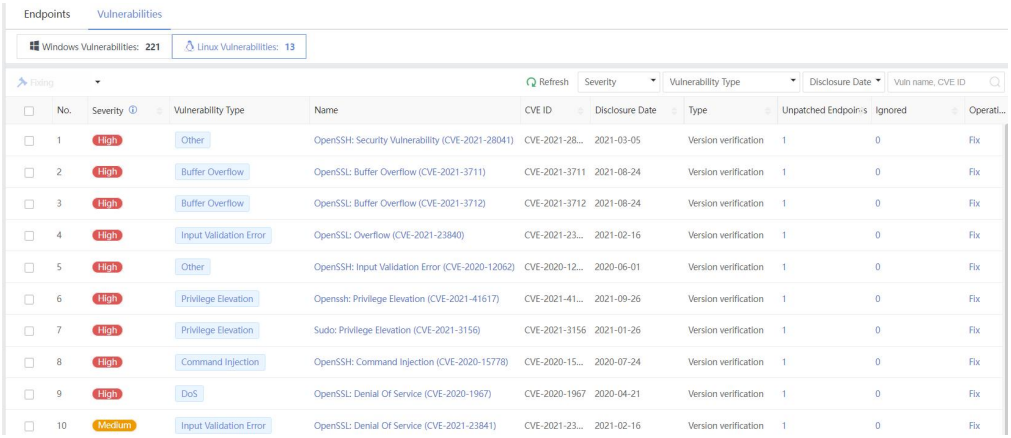

### 3.6.5.1.2 Vulnerabilities View

The **Vulnerabilities** tab is divided into Windows vulnerabilities and Linux vulnerabilities. NovaGuard can respond to vulnerabilities for specific vulnerabilities, you can view the vulnerabilities to be disposed of and patch information on the disposition page, and you can fix or mark them as disposed of for single/multiple vulnerabilities. The disposition page is shown below.

Windows Vulnerabilities




Linux Vulnerabilities




## 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.

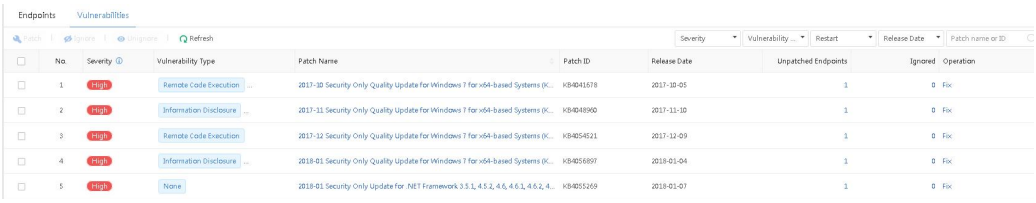



The **Hot Patching** page displays endpoints patched against all vulnerabilities on its **Endpoints** and **Vulnerabilities** tab pages by endpoint and vulnerability.

### 3.6.5.2.1 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 patch name 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.

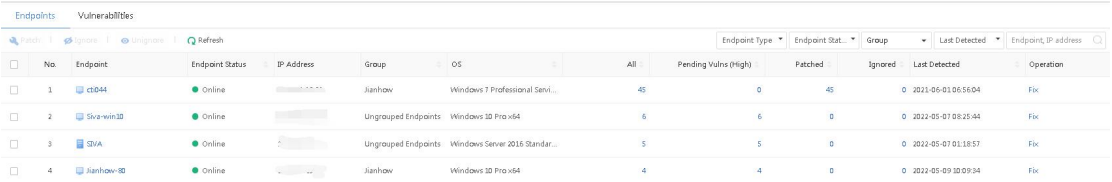
**NOTE**

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.

### 3.6.5.2.2 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.

## 3.6.6 Threat Hunting

When new threat intelligence is known to customers or obtained externally, the relevant intelligence information can be retrieved through a simple combination of criteria (such as IP, domain name, behavior, etc.). You can initiate threat hunting for all endpoints on the entire network, locate the hosts, processes, and other related information about potential threats, and help customers discover new threats or troubleshoot potential risks on the entire network.

### 3.6.6.1 Single Condition Search

Single condition search includes domain name access query, network connection query, executable file hash query, and file name query.

**Domain Name Access Query**

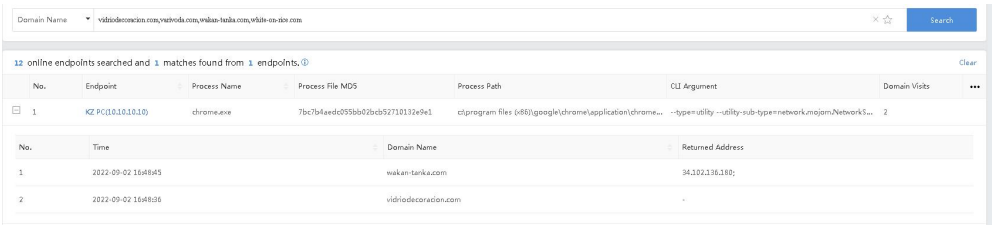
Enter single or multiple domain names, separated by "," (English commas), to retrieve any device that has the behavior of communicating with the associated domain name. The domain name supports fuzzy queries using the "*" wildcard.

**Example**: The domain name related to the Emotet virus was known. Therefore we can query the endpoint that may be infected with the Emotet virus and the corresponding process information that communicates with the Emotet virus domain name.

**Query**:

vidriodecoracion.com,varivoda.com,wakan-tanka.com,white-on-rice.com

The query result is shown below.



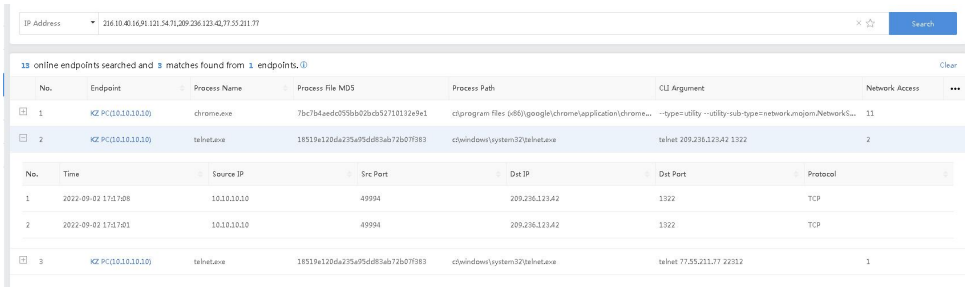

**Network Connection Query**

Enter single or multiple IP addresses, separated by "," (English comma), to retrieve the endpoint and corresponding process information that contains the network connection behavior of the retrieved address in the source IP or destination IP.

**Example**: IP information related to the Emotet virus was known, we can query the endpoint that may be infected with the Emotet virus and process information that communicates with the IP address of the Emotet virus

**Query**: 216.10.40.16,91.121.54.71,209.236.123.42,77.55.211.77

The query result is shown below.




**Executable File Hash Query**

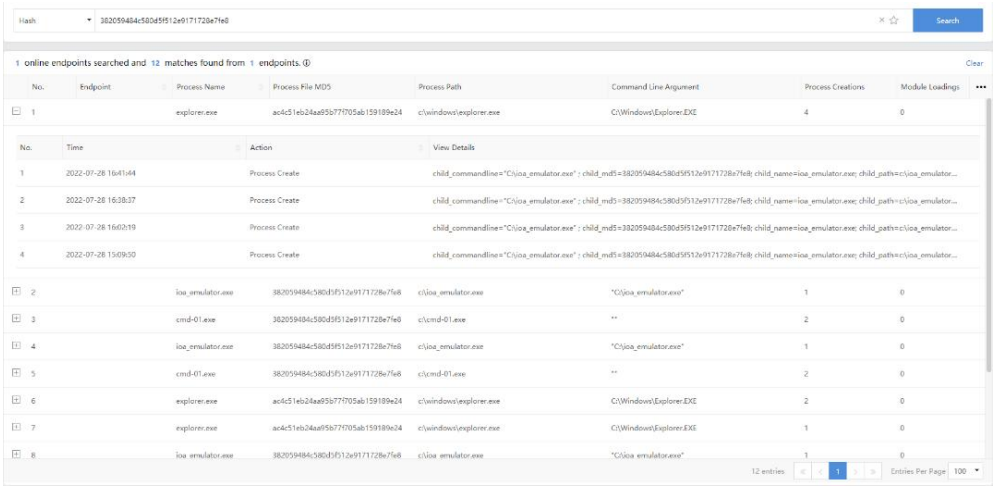
Enter the MD5 or SHA256 value of one or more suspicious program files to be queried, separated by "," (English comma), to retrieve the endpoint and corresponding process that match the input file hash in process operation events and loaded module events information.

**Example**: The SHA256 of files related to the Emotet virus was known. We can query endpoints that may be infected with the Emotet virus.

**Query**:

382059484c580d5f512e9171728e7fe8

The query result is shown below.



**File Name Query**

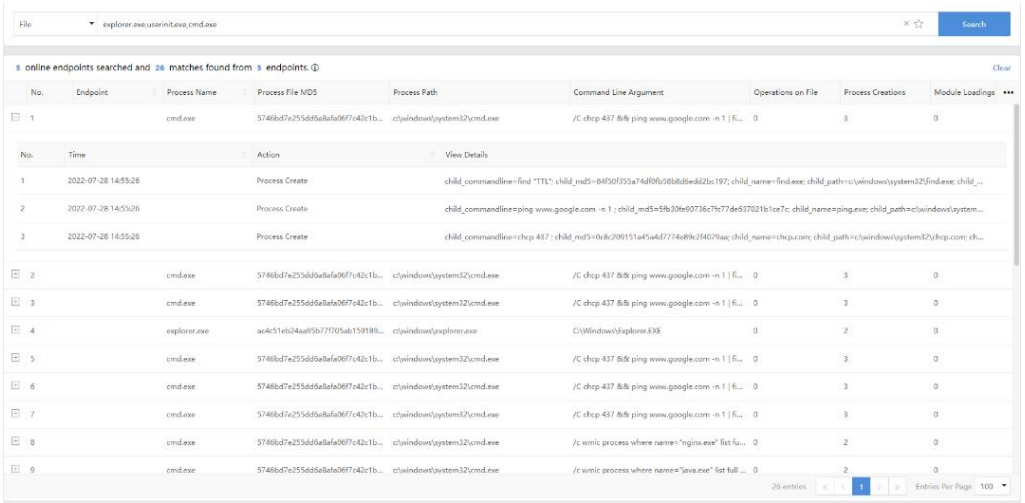
Enter the file names of single or multiple suspicious files to be queried, separated by "," (English comma), to retrieve the endpoints and events related to the entered file names. The file name supports the "*" wildcard for the fuzzy query.

**Example**: The name of the Emotet malicious file was known, and we can query the endpoints that may be infected with the Emotet virus.

**Query**:

explorer.exe,userinit.exe,cmd.exe

The query result is shown below.



## 3.6.6.2 Group Conditions Search

**Group Conditions Search Query**

The search statement consists of **search object**, **field name**, **value**, **comparison operator**

and **logical operator**, as shown in the following figure.

| | | | | | | |
|---|---|---|---|---|---|---|
| Network.src_ip | = | "1.1.1.1" | OR | Process.process_name | = | "Powershell*" |

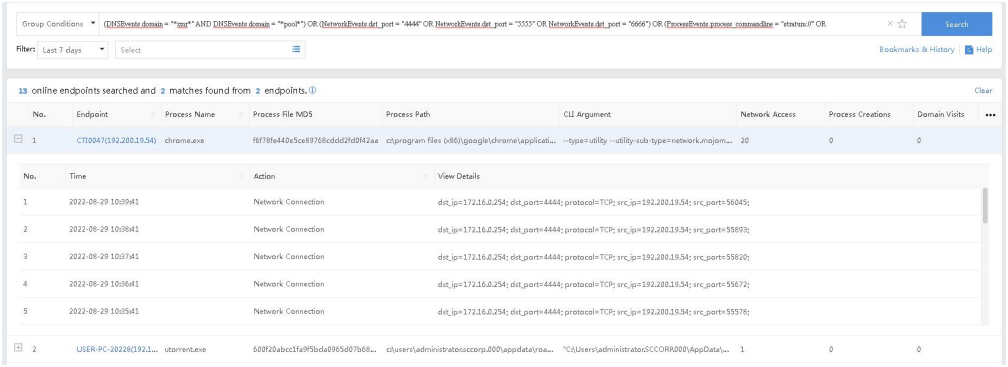
**Example**: Mining virus detection

**Query**: (DNSEvents.domain = "*xmr*" AND DNSEvents.domain = "*pool*") OR (NetworkEvents.dst_port = "4444" OR NetworkEvents.dst_port = "5555" OR NetworkEvents.dst_port = "6666") OR (ProcessEvents.process_commandline = "stratum://" OR ProcessEvents.process_commandline = "cpu-priority")

**NOTE**

The search query is not case-sensitive.

The query result is shown below.




**Object and Field Descriptions**

Retrievable objects include domain name access, network connections, process operations, file operations, loaded modules, and device information. The specific objects and corresponding fields are as follows.

Domain access fields:

| Field | Description | Example |
| --- | --- | --- |
| timestamp | Time Detected | 2021-06-14 12:12 |
| device_name | Endpoint | edr0043(10.32.36.52) |
| action_type | Action | Access Domain Name |
| domain | Domain Name Queried | baidu.com |
| return_ip | Returned Address | 39.156.69.79,220.181.38.148 |
| process_id | Process ID | 4305 |
| process_name | Process Name | PING.EXE |
| process_md5 | Process File MD5 | f926bedd777fa0f4f71dd2d28155862a |
| process_SHA256 | SHA256 | 1d35014d937e02ee090a0cfc903ee6e6b1b65c8326945... |
| process_path | Process Path | C:\WINDOWS\system32\PING.EXE |
| process_commandline | Process Execution Command | C:\WINDOWS\system32\PING.EXE |
| process_user | Process User | NT AUTHORITY\SYSTEM |

## Network Connection Fields

| Field | Description | Example |
| --- | --- | --- |
| timestamp | Time Detected | 2021-06-14 12:12 |
| device_name | Endpoint | edr0043(10.32.36.52) |
| action_type | Action | Network Access |
| src_ip | Source IP | 1.1.1.1 |
| src_port | Src Port | 22345 |
| dst_ip | Dst IP | 192.168.1.1 |
| dst_port | Dst Port | 80 |
| protocol | Protocol (TCP/UDP) | tcp |
| process_id | Process ID | 4305 |
| process_name | Process Name | PING.EXE |
| process_md5 | Process File MD5 | f926bedd777fa0f4f71dd2d28155862a |
| process_SHA256 | SHA256 | 1d35014d937e02ee090a0cfc903ee6e6b1b65c8326945... |
| process_path | Process Path | C:\WINDOWS\system32\PING.EXE |
| process_commandline | Process Execution Command | C:\WINDOWS\system32\PING.EXE |
| process_user | Process User | NT AUTHORITY\SYSTEM |

## File Operation Fields

| Field | Description | Example |
| --- | --- | --- |
| timestamp | Time Detected | 2021-06-14 12:12 |
| device_name | Endpoint | edr0043(10.32.36.52) |
| action_type | Action | Create a file |
| file_name | File Name | sss.php |
| file_md5 | File MD5 | f926bedd777fa0f4f71dd2d28155862a |
| file_sha256 | File SHA256 | 93d48bf194d87b190dc1fb9b8837011a58dc1f742871... |
| file_path | File Path | E:\www\sss.php |
| prev_file_name | Original File Path | E:\www\shell.php |
| is_exist | File Exists | Yes/No |
| process_id | Process ID | 4305 |
| process_name | Process Name | PING.EXE |
| process_md5 | Process File MD5 | f926bedd777fa0f4f71dd2d28155862a |
| process_SHA256 | SHA256 | 1d35014d937e02ee090a0cfc903ee6e6b1b65c8326945... |
| process_path | Process Path | C:\WINDOWS\system32\PING.EXE |
| process_commandline | Process Execution Command | C:\WINDOWS\system32\PING.EXE |
| process_user | Process User | NT AUTHORITY\SYSTEM |

## Process Operation Fields

| Field | Description | Example |
| --- | --- | --- |
| timestamp | Time Detected | 2021-06-14 12:12 |
| device_name | Endpoint | edr0043(10.32.36.52) |
| action_type | Action | Create Process |
| child_id | Child Process ID | 4305 |
| child_name | File Name of Child Process | SearchFilterHost.exe |
| child_md5 | File MD5 of Child Process | f926bedd777fa0f4f71dd2d28155862a |
| child_sha256 | File SHA256 of Child Process | 0ba37d0db6d5d74e9b1d8ebc540c1acd4a471386d683... |
| child_path | Child Process Path | C:\WINDOWS\system32\SearchFilterHost.exe |
| child_commandline | Child Process Execution Command | 0 812 816 824 8192 820 |
| child_user | Child Process User | NT AUTHORITYSYSTEM |
| process_id | Process ID | 29733 |
| process_path | Process Path | C:\Windows\system32\services.exe |
| process_md5 | Process File MD5 | f926bedd777fa0f4f71dd2d28155862a |
| process_name | Process Name | services.exe |
| process_SHA256 | SHA256 | 1d35014d937e02ee090a0cfc903ee6e6b1b65c8326945... |
| process_commandline | CLI Argument | C:\Windows\system32\services.exe |
| process_user | Process User | NT AUTHORITY\SYSTEM |

## Module Loading Fields

| Field | Description | Example |
|---|---|---|
| timestamp | Time Detected | 2021-06-14 12:12 |
| device_name | Endpoint | edr0043(10.32.36.52) |
| action_type | Action | Loaded Module |
| file_name | Loaded File Name | kernel32.dll |
| file_path | File Path | C:\Windows\System32\kernel32.dll |
| file_md5 | Loaded File MD5 | e1ff9d65e6b86f7ebb531ae36c5af635 |
| file_sha256 | Loaded File SHA256 | 92981d598dc950c191b0320955dd777fbac7bbee1c17… |
| process_id | Process ID | 4305 |
| process_name | Process Name | PING.EXE |
| process_md5 | Process File MD5 | f926bedd777fa0f4f71dd2d28155862a |
| process_SHA256 | SHA256 | 1d35014d937e02ee090a0cfc903ee6e6b1b65c8326945… |
| process_path | Process Path | C:\WINDOWS\system32\PING.EXE |
| process_commandline | Process Execution Command | C:\WINDOWS\system32\PING.EXE |
| process_user | Process User | NT AUTHORITY\SYSTEM |

**Device Information Fields**

| Field | Description | Example |
|---|---|---|
| device_name | Endpoint | edr0043(10.32.36.52) |
| host_name | Hostname | sangfor |
| os_name | OS | Windows 7 Professional |
| os_version | OS Version | 6.1.7601 Service Pack 1 Build 7601 |
| mac_address | MAC Addresses | FE:FC:FE:11:98:F2 |
| ipv4_addresses | IPv4 Addresses | 10.62.7.150 |
| ipv6_addresses | IPv6 Addresses | fe80::b0eb:5d89:f3c1:63d2 |
| cpu_total | Total CPU (Hz) | 2.4GHz |
| cpu_used | CPU Used | 1GHz |
| mem_total | Total Memory Size | 4096MB |
| mem_used | Memory Used | 1024MB |
| disk_total | Total Disk Space | 50GB |
| disk_used | Disk Space Used | 20GB |
| user_name | System Account | Administrator |
| group_name | Group | Administrators |
| last_login_time | Last Login Time | 2020-03-16T07:41:16.730Z |

**Value**

Double quotation marks are required when entering the value. Support wildcard search, support single and multiple character wildcard search within a value that uses the "*" sign to indicate multiple character wildcard search and match zero or more characters. The wildcard "*" can only be used in conjunction with the comparators "=" (equal) and "!=" (not equal).

**Example**: Search for the word mongodb or mondodb, which can be written as: mon*

**Comparison operators**

| Operator | Notes |
| --- | --- |
| = | Equal to |
| > | Greater than |
| >= | Greater than or equal to |
| < | Less than |
| <= | Less than or equal to |
| != | Not equal to |

**Logical Operators**

The log lookup system supports three operators: AND, OR, NOT.

1. AND Operator

AND means that both fields must be matched.

2. OR Operator

OR means that at least one field must be matched.

3. NOT Operator

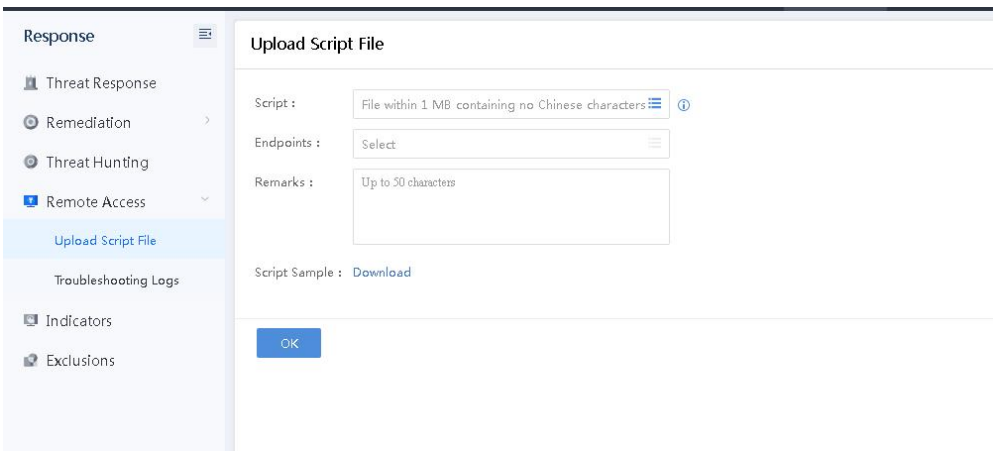
NOT excludes the records containing a single item or phrase following the NOT operator.

## 3.6.7 Remote Access

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

### 3.6.7.1 Upload Script File

The Upload Script File page supports sending scripts to endpoints and executing them on Linux and Windows endpoints.



**Script**: Upload the script files to be sent to the endpoints; their size is no more than 1MB.

**Endpoints**: It specifies endpoints to be sent to the scripts.

NOTE

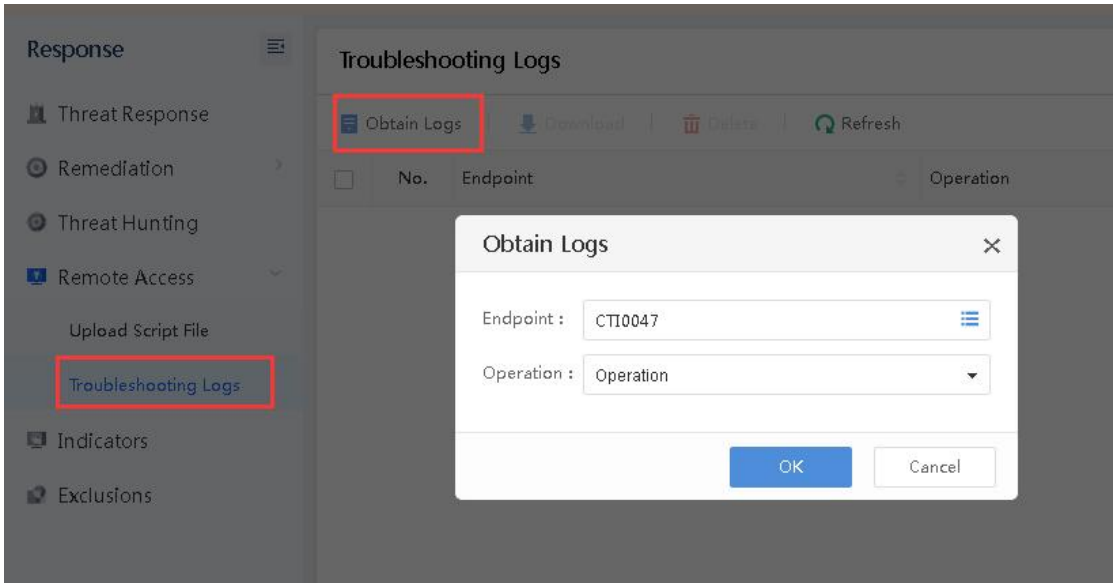
1. Upload script only can select endpoint in online status.

2. To enable this feature, the super administrator account must enable TOTP authentication. Please refer to Chapter **3.8.3.3** for the configuration details.

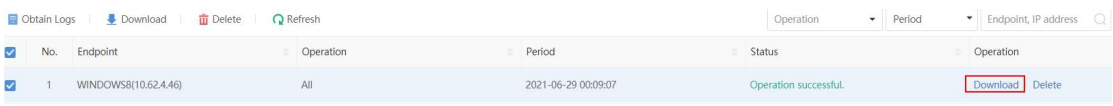
3. Only a super administrator account can use this feature.

## 3.6.6.2 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.



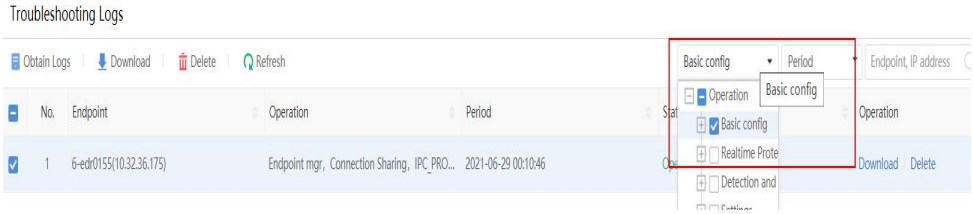

2. Click **OK**. After logs are obtained, click **Download** to download the troubleshooting logs of the endpoint.



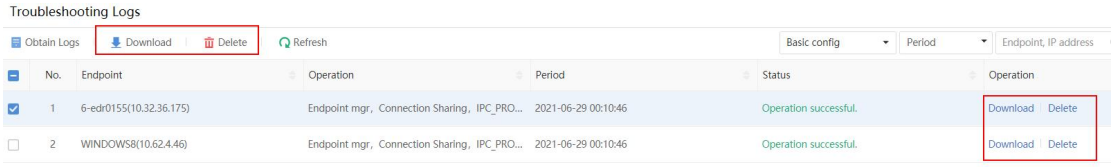

## 3.6.7.3 Troubleshooting Log Management

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.



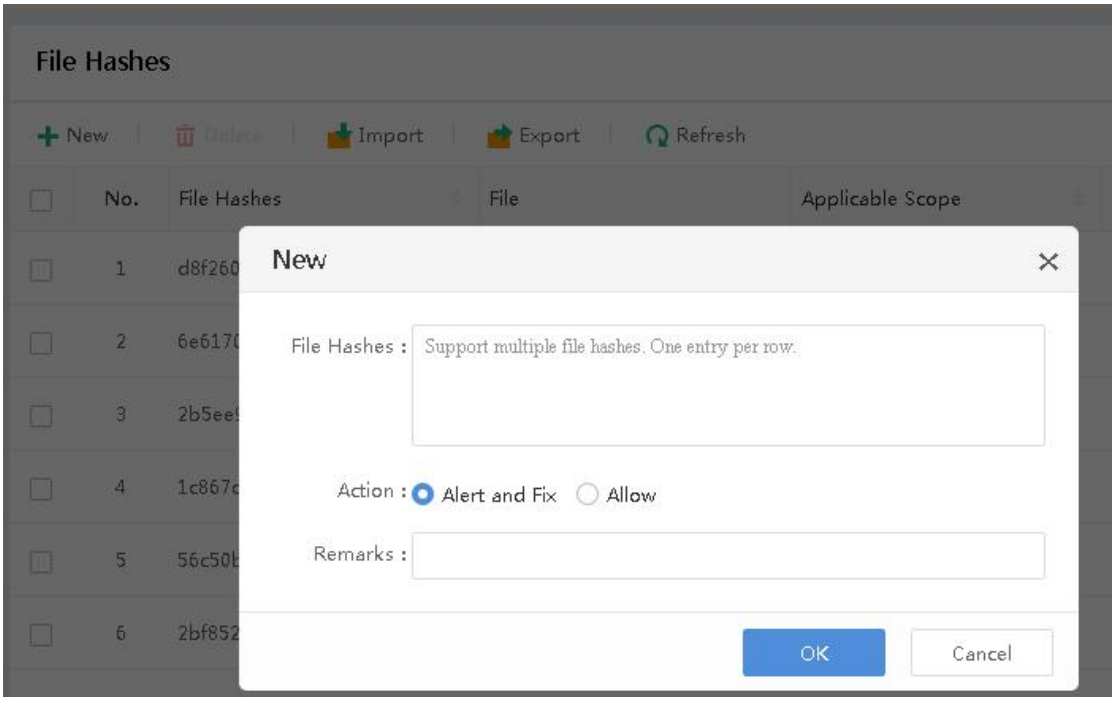

2. You can select one or more logs and click **Download** or **Delete** to download or delete the logs. You can also click **Download** or **Delete** in the **Operation** column of a log to download or delete the log. The following figure shows the **Troubleshooting Logs** page.




## 3.6.8 Blacklist and Whitelist

### 3.6.8.1 Black and White List According to the File MD5

To respond quickly and improve operation and maintenance efficiency in the case of false positives and false negatives, it supports blacklisting and whitelisting according to file hashes. Go to **Response** > **Indicators**, as shown in the figure below. When a malicious file is found to be missed or falsely reported, a black and white list can be set based on the file hash.




Response actions include **Alert and Fix**, **Allow**.

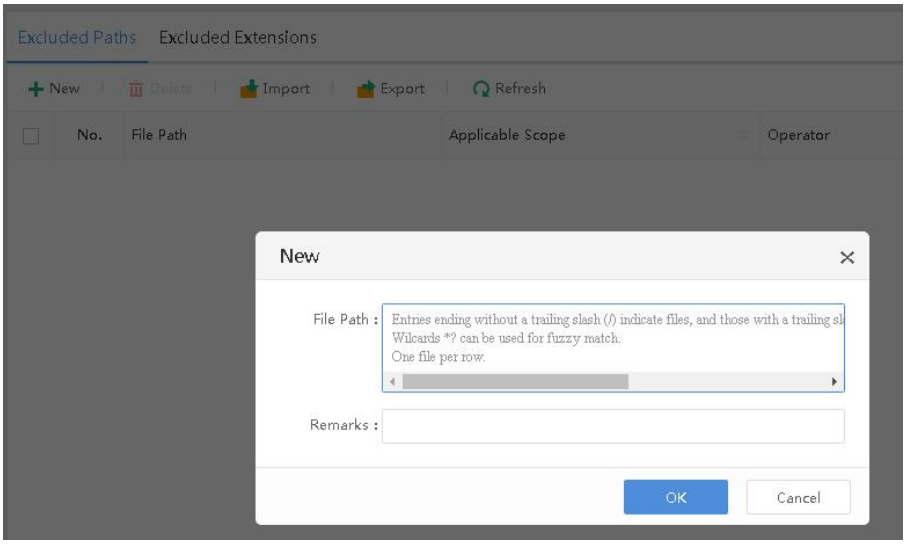
**Alert and Fix**: When a missed report is found, set the response action to alert and fix.

**Allow**: When a false positive is found, set the response action to allow.

### 3.6.8.2 Add Whitelist According to File Directory and Suffix

NovaGuard supports whitelisting by file, directory, and suffix. In addition, it supports fuzzy matching and batch import functions.

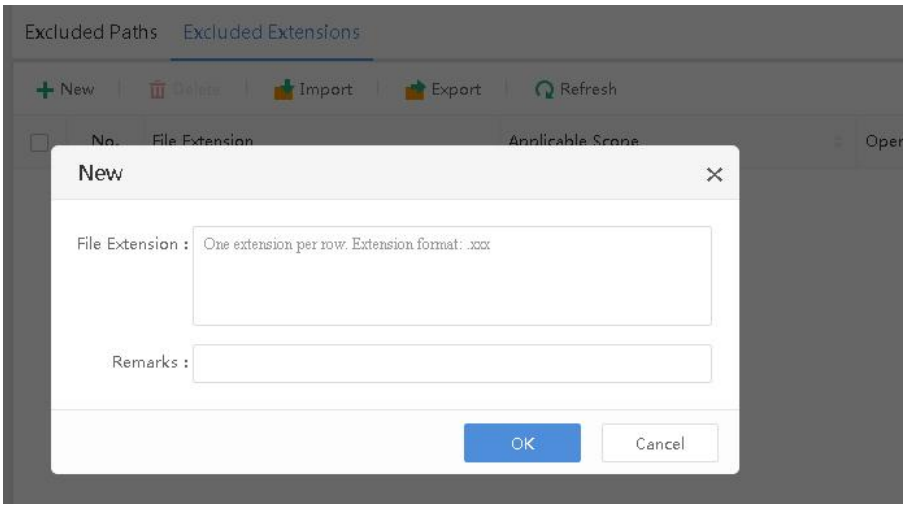
Go to **Response > Exclusion**, as shown in the figure below. When a false positive is found, it can be excluded based on files, file directories, and suffixes. Viruses, real-time monitoring, and webshell detection checking will not be performed on the excluded files.




Exclude files: No "/" at the end indicates files, such as D:\2022\10tools\test

Exclude directories: "/" at the end indicates a directory, such as D:\2022\10tools\test\

Exclude suffix according to the suffix format .xxx, as shown below.



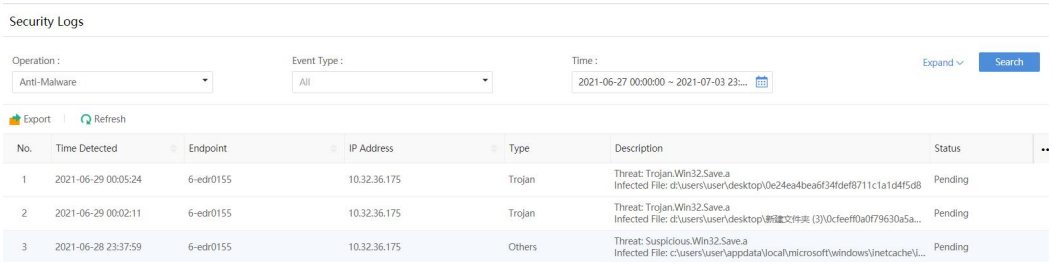

# 3.7 Logs

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

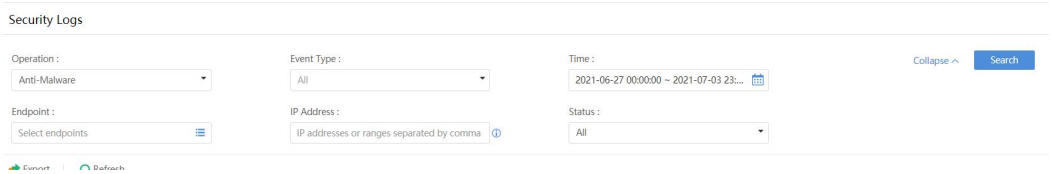
## 3.7.1 Security Logs

The **Security Logs** page displays security logs about different security policies, such as malware, intrusion detection, vulnerability scan, security compliance check, micro-segmentation, server protection, unauthorized outbound access, RDP secondary authentication, USB control, and hot patching. The following figure shows the **Security**

**Logs** page.

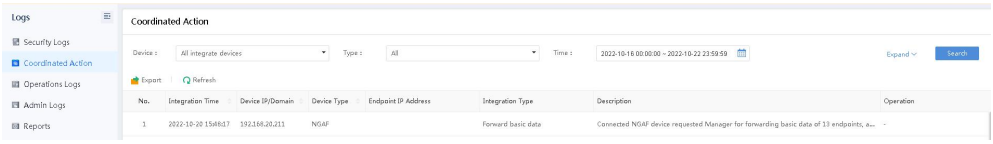



You can filter security logs by log type, statistical period, and time and click **Expand** to further search for security logs by endpoint name and IP address. You can click **Export** to export the search result.




## 3.7.2 Coordinated Action

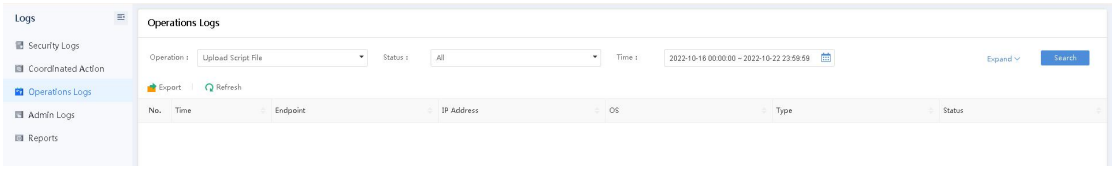
The **Coordinated Action** page displays information about integration between NovaGuard and other products, including NGAF, Cyber Command, IAG, Platform-X, and Neutral-X. The information includes the overall integration status, integration time, IP addresses and types of integrated devices, integration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

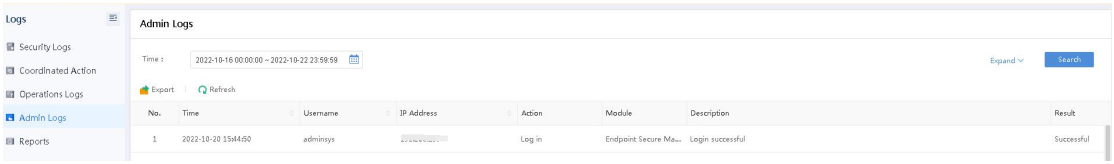
The **Operation Logs** page displays operation logs about remote access, including the operation time, endpoint name, IP address, OS, type, and execution status. The following figure shows the **Operation Logs** page.




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 NovaGuard Manager, including the operation time, username, IP address, operation type, object, description, and result. The following figure shows the **Admin Logs** page.

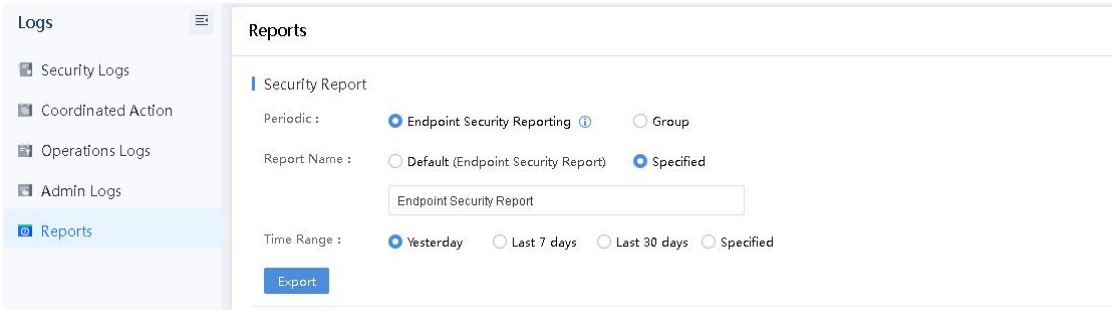



You can filter admin logs by statistical period and time and click **Expand** to further search for admin logs by username, IP address, and execution status. You can click **Export** to export the search result.

# 3.7.5 Reports

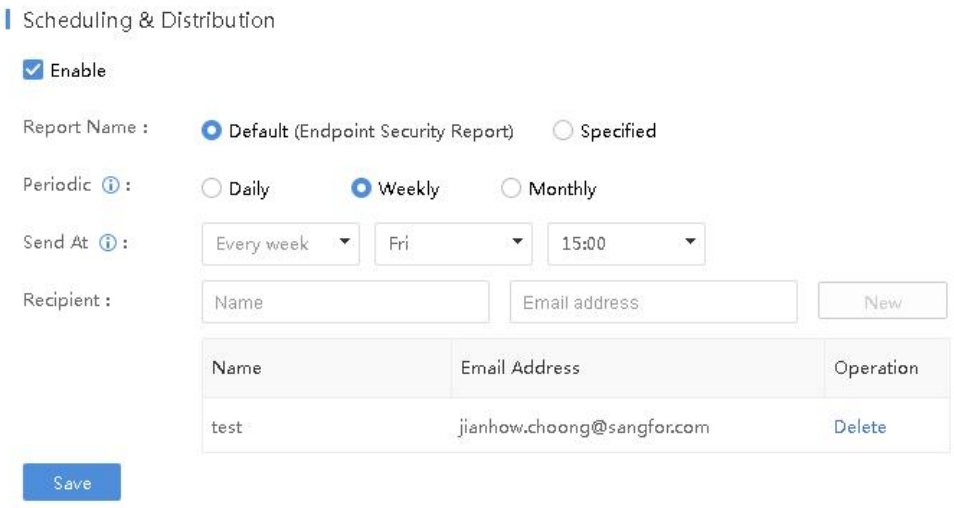
## 3.7.5.1 Export

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.




## 3.7.5.2 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.

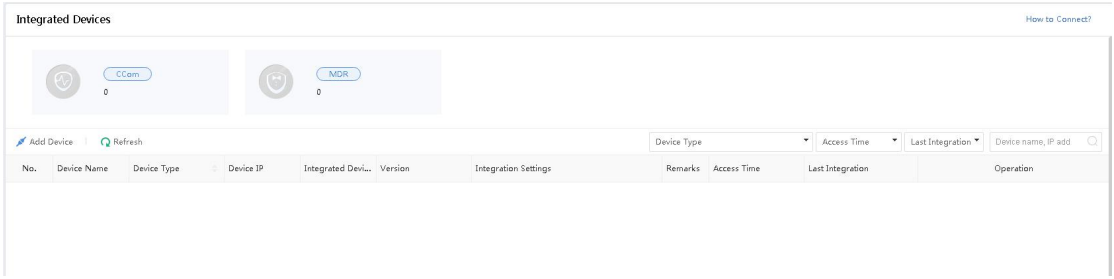
NOTE

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

## 3.8.1 Integrated Devices

The **Integrated Devices** page manages integration between NovaGuard and Cyber Command and MDR. 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 NovaGuard 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 NovaGuard and other products.

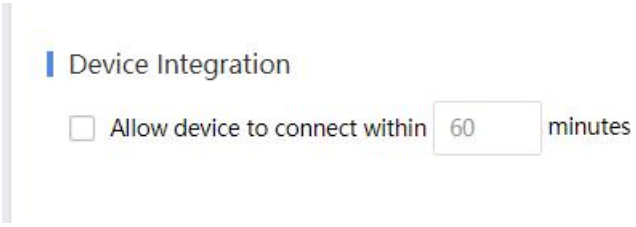
| Integrated Product | Agent Deployment Redirection | Correlated Block | Log Reporting | Access Control | Correlated Scan | Correlated Malicious File Fixing | Process Forensics | Anti-Proxy |
|---|---|---|---|---|---|---|---|---|
| MDR | - | - | - | - | - | - | - | - |
| Cyber Command | No | Yes | Yes | Yes | Yes | Yes | Yes | No |

Table 8: Functions supported for integration between NovaGuard and other products

NOTE

Since the MDR service is not available yet, it will not be further described here for MDR integration.

To integrate NovaGuard with any product required to enable the **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 ForeNova products are first time connected.

### 3.8.1.1 Integration with Cyber Command

Integration between NovaGuard 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 NovaGuard can be reported to Cyber Command for centralized operations and analysis. To integrate NovaGuard with Cyber Command, ensure that the following conditions are met:

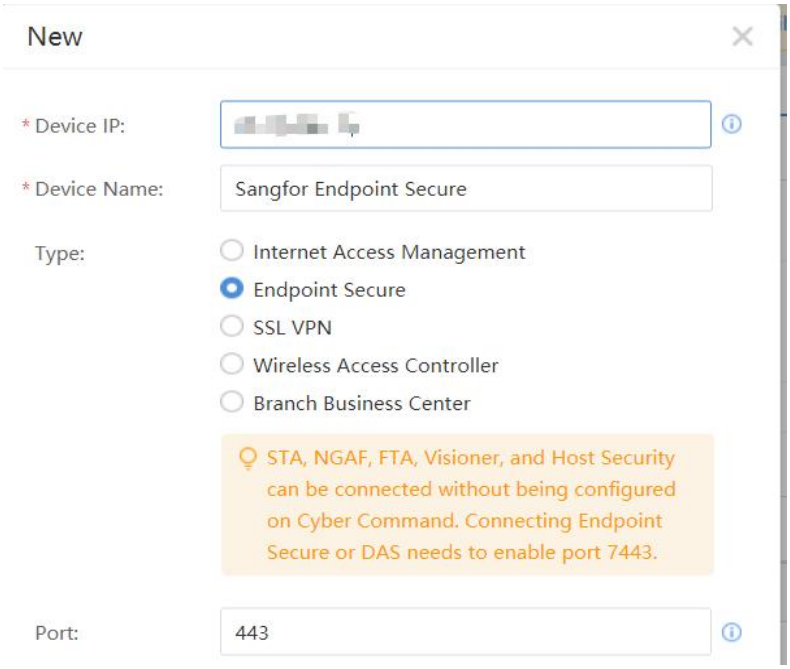
**Network connectivity:** Cyber Command can communicate with **TCP port 443** of NovaGuard, and the NovaGuard Manager can communicate with **TCP port 7443** of Cyber Command.

**Version:** The Cyber Command version is 3.0.49 or later.

To integrate NovaGuard with Cyber Command, you only need to configure the NovaGuard 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 NovaGuard Manager.

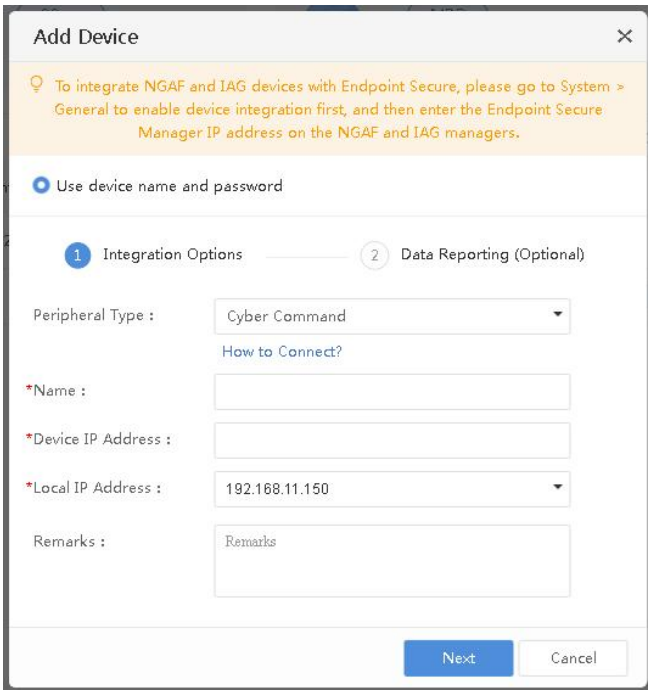
**Device Name**: Customize a device name that is easy to identify.

**Type**: Select **NovaGuard**.

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

**Integration Procedure on the NovaGuard Manager**

1. Log in to the NovaGuard 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:

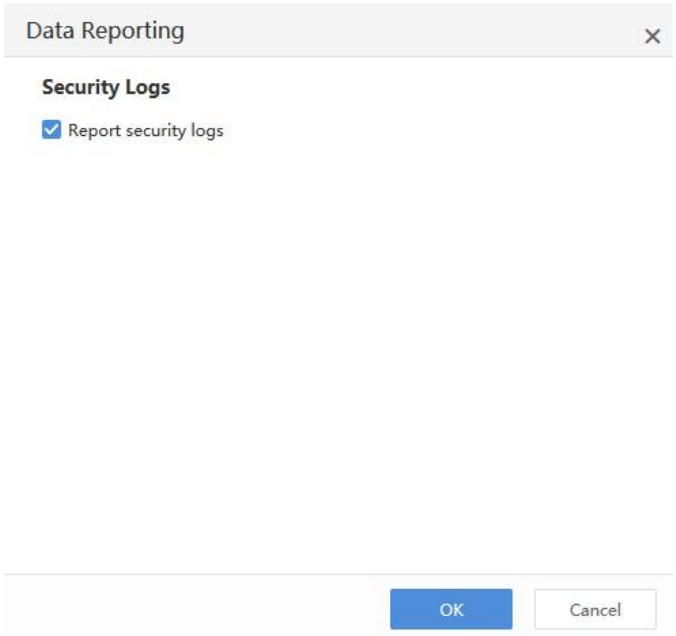
**Device Type**: Select **Cyber Command**.

**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 NovaGuard Manager that can communicate with Cyber Command.

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

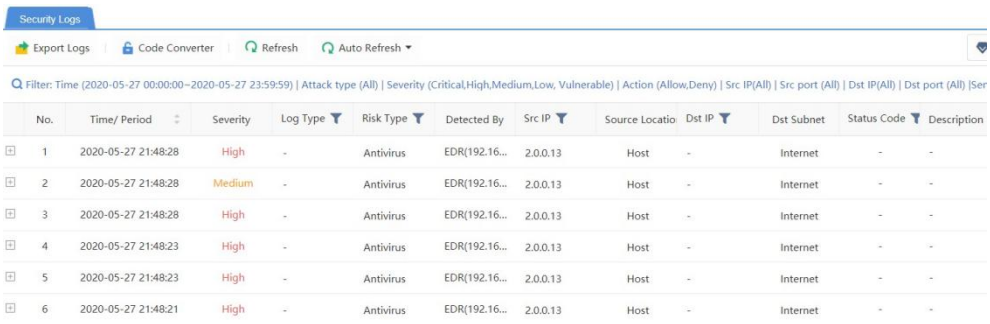



**Security Logs**: After selecting it, NovaGuard will report selected information to the Cyber Command Manager for centralized analysis.

**Integration Effect**

1. NovaGuard security log reporting

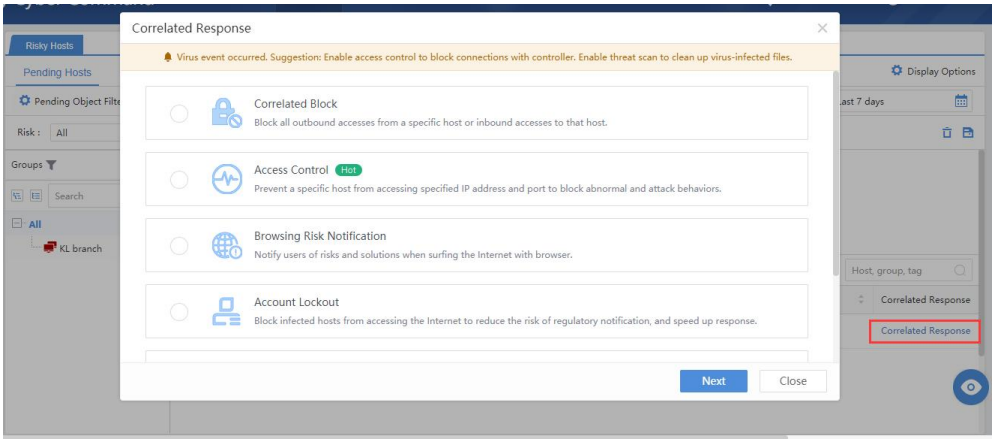
Security logs generated by NovaGuard can be automatically reported to the Cyber Command Manager for centralized analysis and operations. On the Cyber Command Manager, you can choose **Analytics > Security Logs** and select NovaGuard as the data source to query and analyze security logs reported by NovaGuard,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




2. Correlated virus scan

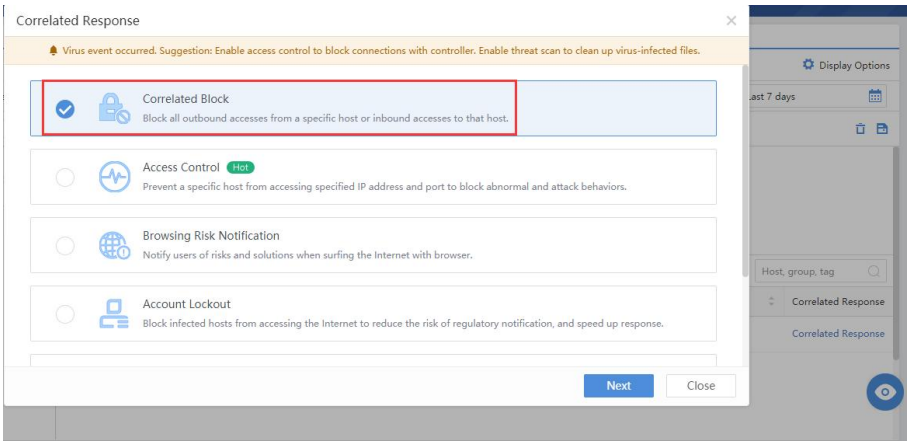
Cyber Command can correlate with NovaGuard for virus scans when identifying risky endpoints. Under **Response** > **Risky Hosts** of the Cyber Command Manager, you can correlate Cyber Command with NovaGuard to perform virus scans for identified risky endpoints and isolate, trust, or ignore identified malicious files. The following figure shows

the integration page.



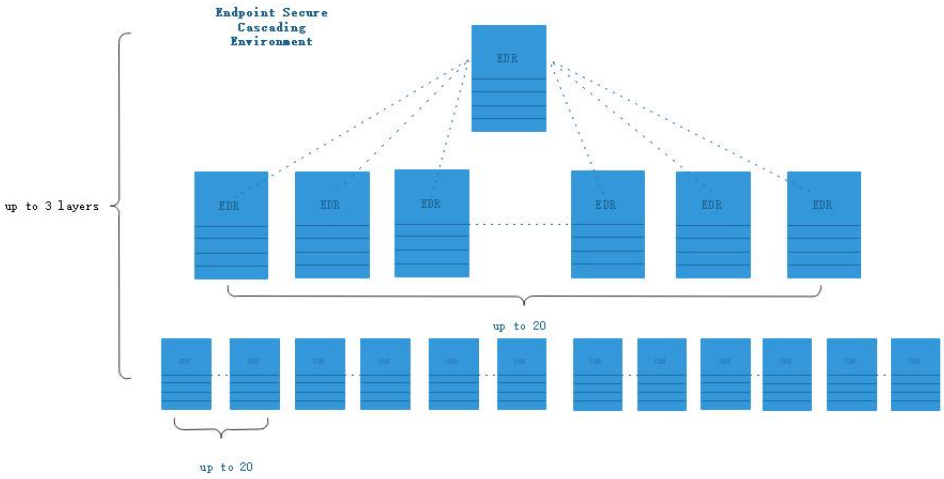

3. Risky endpoint isolation

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




## 3.8.2 Branches

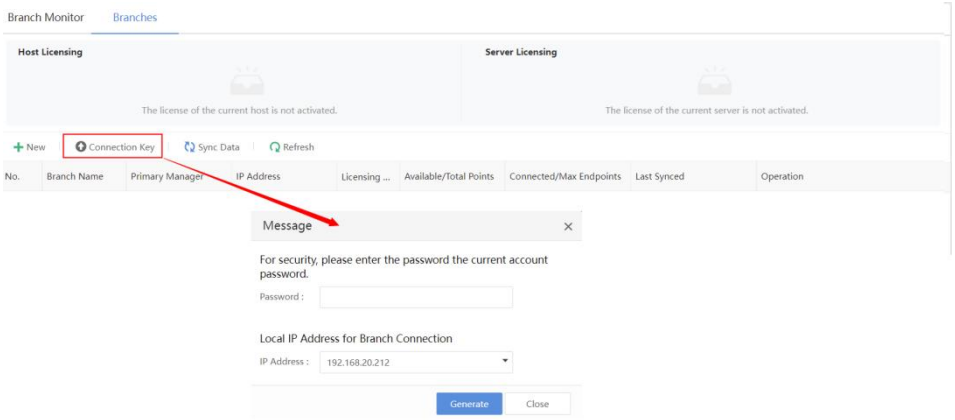
The **Branches** page consists of the **Branch Monitor** and **Branches** tab pages for cascading NovaGuard management. Up to three cascading layers are supported, and each NovaGuard can be cascaded with up to 20 NovaGuard Managers. The following figure shows the NovaGuard cascading environment.



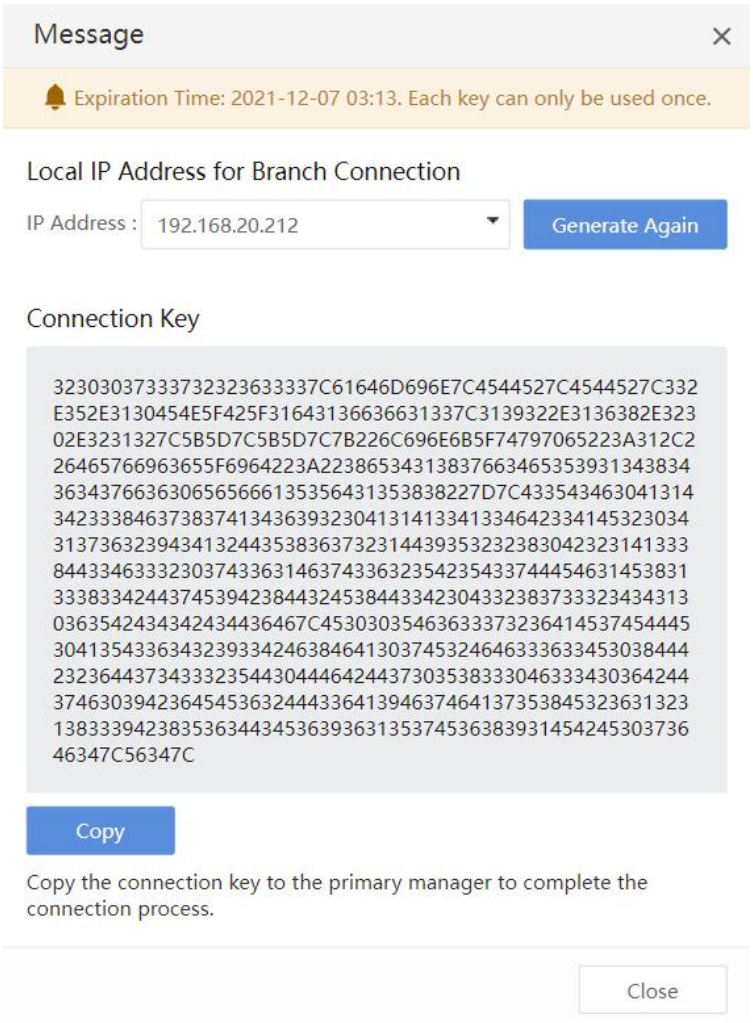

## 3.8.2.1 Branches Setting

1. The lower-level NovaGuard Manager generates the connection code.

   Log in to the lower-level NovaGuard Manager, go to **System > Branches > Branches**, and click **Connection Key**, as shown below.



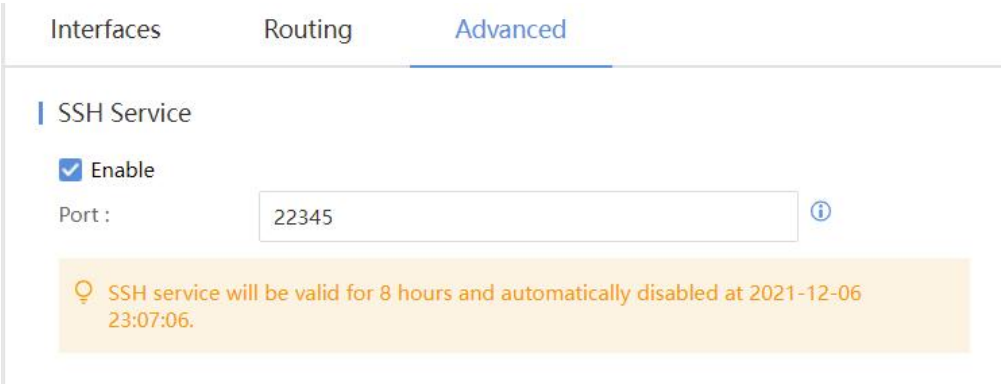

   Enter the admin account password and click **Generate** to generate the connection key, as shown in the figure below.




Click **Copy** to copy the connection key to the superior NovaGuard platform to complete the branches' docking.

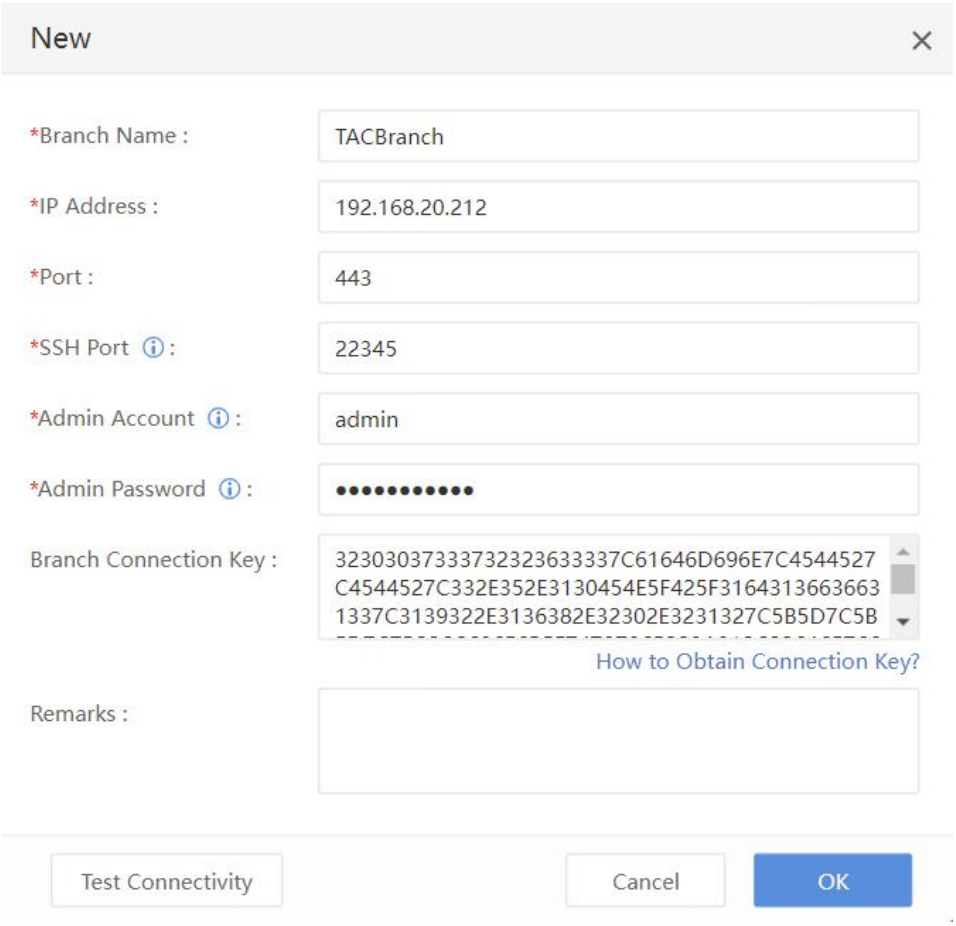
2. Enable the SSH service on the lower-level NovaGuard Manager platform.

   Log in to the lower-level NovaGuard Manager, go to **System > General > Network > Advance**, and enable the SSH server Service settings, as shown in the figure below.




3. The superior NovaGuard Manager completes the branches' docking.

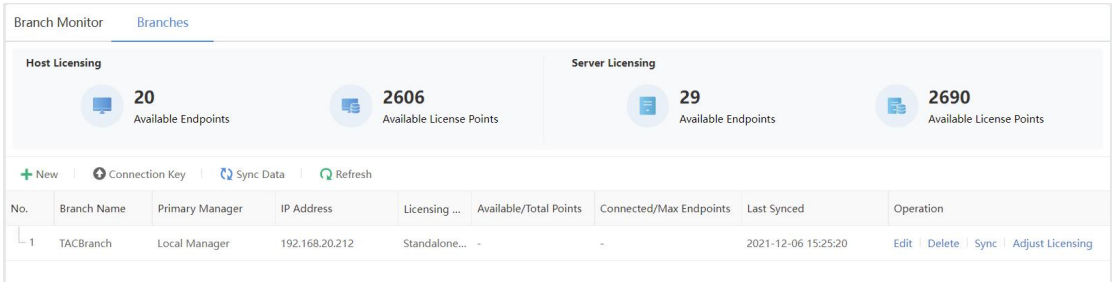
   Log in to the superior NovaGuard Manager, then go to **System > Branches > Branches**, and click **New**, as shown below.




Fill in the **Branch/Name, Branch NovaGuard platform IP, Branch NovaGuard console login port, Branch SSH port, branch admin account** and **admin password**, and the

**connection key**.

Enter the login password of the current management platform, click, and the cascade is successful, as shown in the figure below.




**Host Licensing**: Display the available host access and available host license points at this level.

**Server Licensing**: Display the available number of server access and available server license points at this level.

The branch's success page displays the name of the lower-level platform, IP address, licensing mode, available license points, and connected endpoints.

, last synced and related operations.

**Licensing mode**: In the branch's deployment scenario, the lower-level management platform has two modes: **Standalone licensing** and **Cascade licensing** that can be adjusted.

**Standalone licensing**: The lower-level management platform opens the licensing by itself, and the upper-level management platform cannot dynamically adjust the lower-level management platform.

**Cascade licensing**: Branches licensing-- the upper-level management platform allocates the licensing of the lower-level management platform, and the upper-level management platform can dynamically adjust the licensing of the lower-level management platform according to the actual situation.

**Remaining/total authorized resources**: The number of remaining authorized resources and total authorized resources of the lower-level management platform

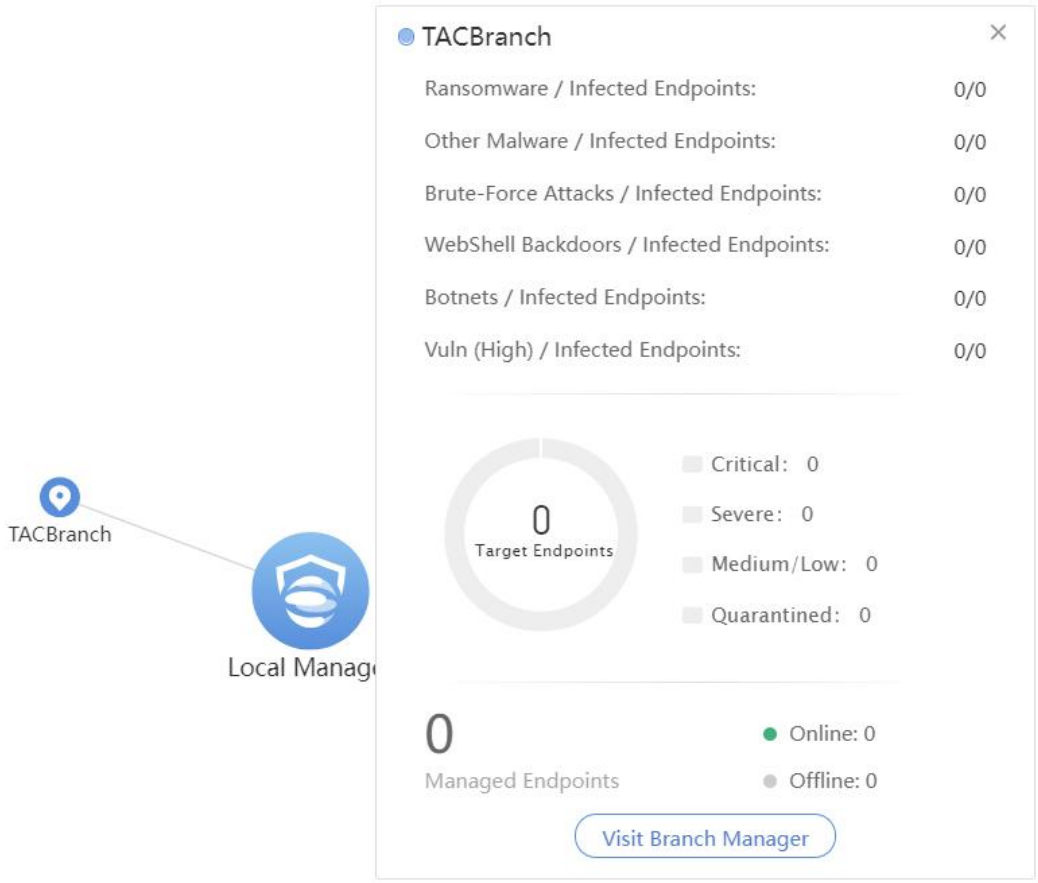
**Connected/maximum accessible terminals**: The number of terminals that the lower-level management platform Connected and the number of terminals that support the maximum access.

### 3.8.2.2 Branches Effect

1. View the **Not Compromised** status of the lower-level management platform

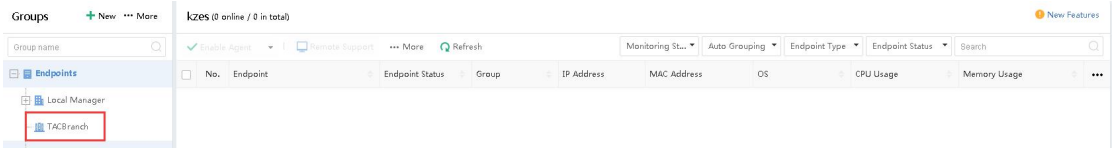
Open **System > Branches > Branch Monitor**, move the mouse to the lower-level management platform, and display the lower-level management platform.

Not Compromised status, click **Visit Branch Manager** to jump to the login page of the lower-level management platform console, as shown in the figure below.




2. View the access terminal of the lower-level management Endpoints

Open **Endpoints > Groups.** You can view the Administrator of the lower-level management platform, as shown in the figure below.



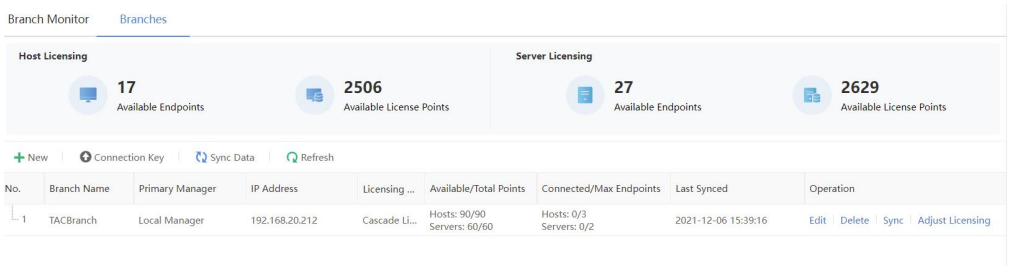

3. Branches Licensing

When the total number of licensings is fixed, and the number of licensings in each Branch

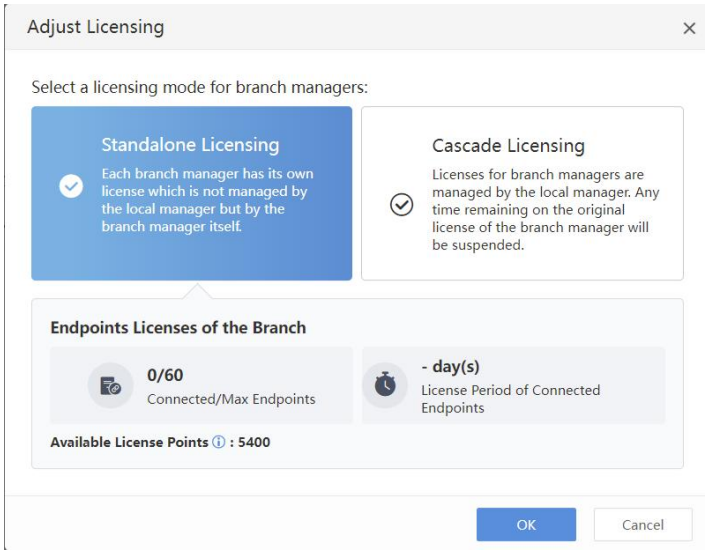
needs to be dynamically adjusted, you can use the cascaded licensing.

The upper-level management platform opens the total authorized resources, and the lower-level management platform does not need to open the licensing. The upper-level and lower-level management platforms form a branch deployment, and the authorized resources can be dynamically adjusted to the lower-level management platform.

Open **System > Branches> Branches**. The branch effect is shown in the figure below.




Click **Adjust Licensing** to enter the licensing adjustment page, as shown in the figure below.

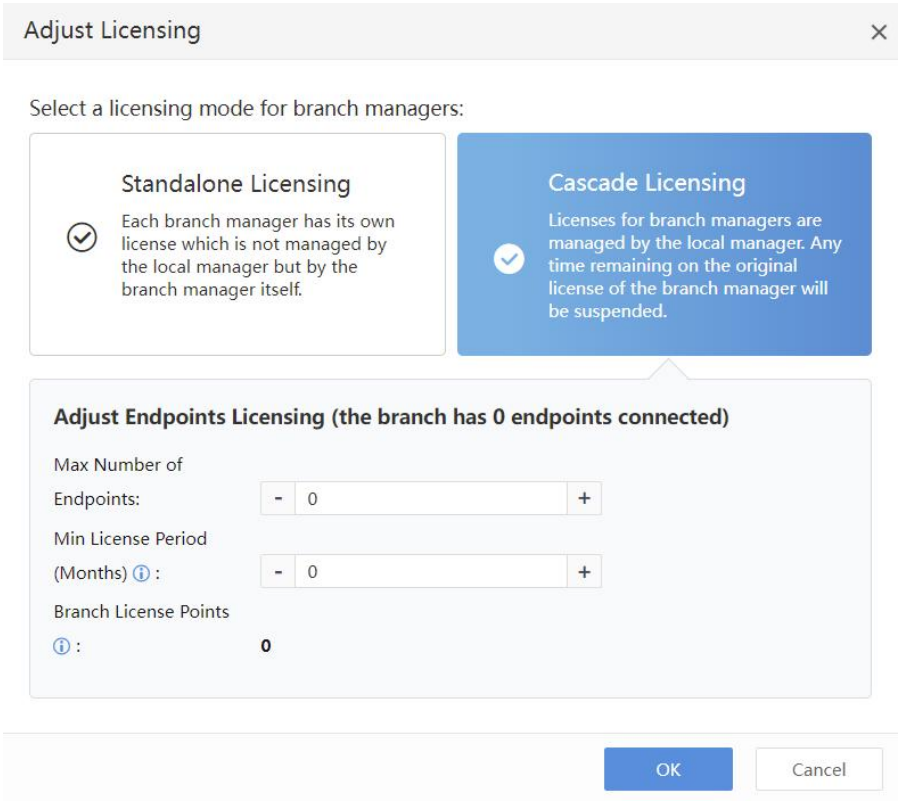



The licensing mode of the lower-level platform can be set to **Standalone Licensing** or **Cascade Licensing.** Standalone licensing is the lower-level management platform.

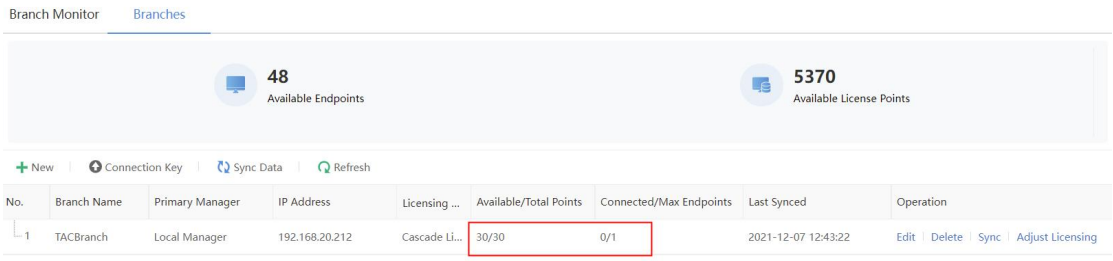
You need to open the licensing yourself, and the upper-level management platform cannot dynamically adjust the licensing to the lower-level management platform.

As shown in the figure below, Cascade licensing allocates the access number and usage

time of the lower-level platform PC and server according to the Duration.




After the cascade licensing adjustment is successful, as shown below




**NOTICE**

1. If the adjusted lower-level platform can authorize the number of PC Endpoints and servers lower than the number Connected to the lower-level platform, reclaim the excess Endpoints licensing in the following order: **Disabled Endpoints> offline Endpoints> online Endpoints**.

2. The authorized number is not occupied in the Endpoints group management if the Endpoints status is Agent uninstalled or Not Licensed.

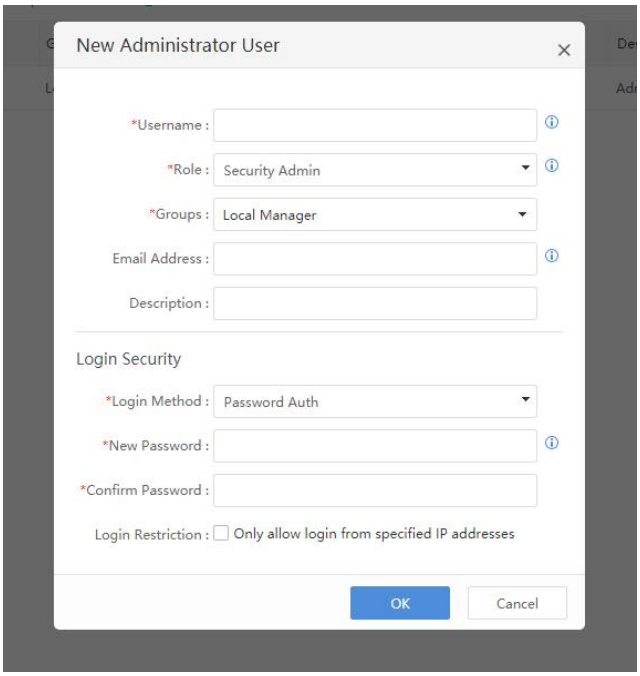
3. Using the branch's licensing scenario. The lower-level administrator does not need to activate the licensing. The lower-level administrator does not need to activate the licensing. The upper-level and

lower-level management platforms form a branch deployment, and the authorized resources can be dynamically adjusted to the lower-level management platform.

## 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 NovaGuard 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 permission to view the home page and configure system settings.

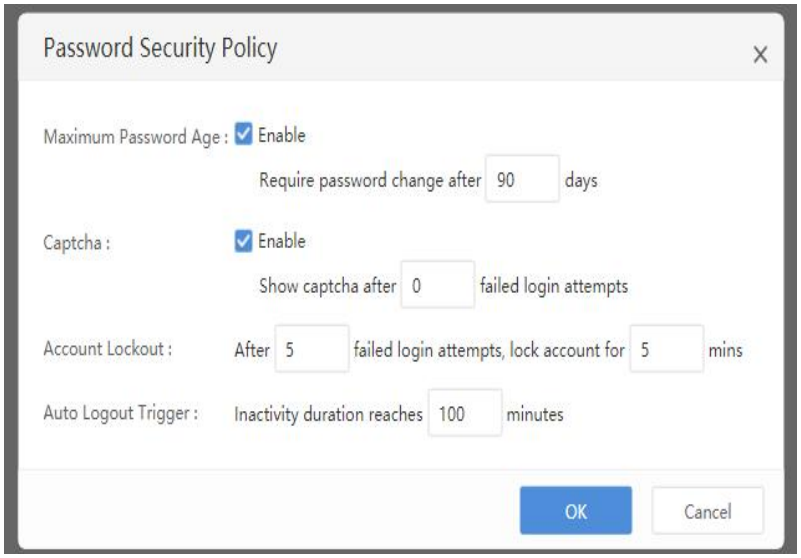
**Security Admin**: has all permissions except those required to perform operations on the **Micro-Segmentation**, **Integrated Devices**, **Reports**, **Administrators**, **System Updates**, **Licensing**, **Branches**, and **System** modules.

**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 NovaGuard Manager accounts.

### 3.8.3.2 Password Security Policy

You can configure a password security policy for managing the login to the NovaGuard Manager based on your installation requirements. To configure a password security policy, perform the following steps: Log in to the NovaGuard 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:

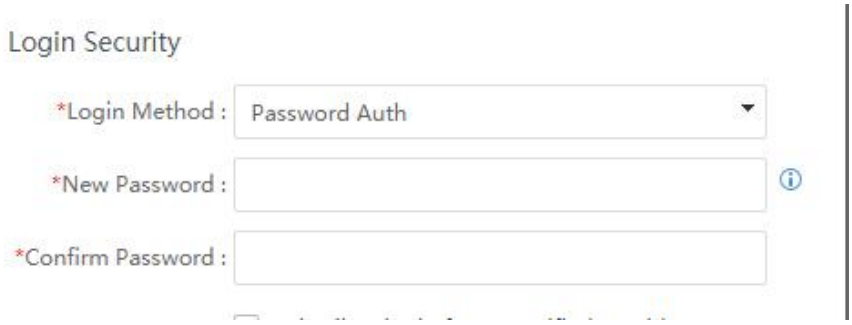
- **Maximum Password Age**: If you select **Enable** to enable the password validity period, which is disabled by default, you will be forced to change the password during login after the specified period expires (90 days by default, value range: 1-365). If you do not change the password, you will be 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 NovaGuard Manager provides the **Password Auth and Password + TOTP** method for authenticating login accounts.

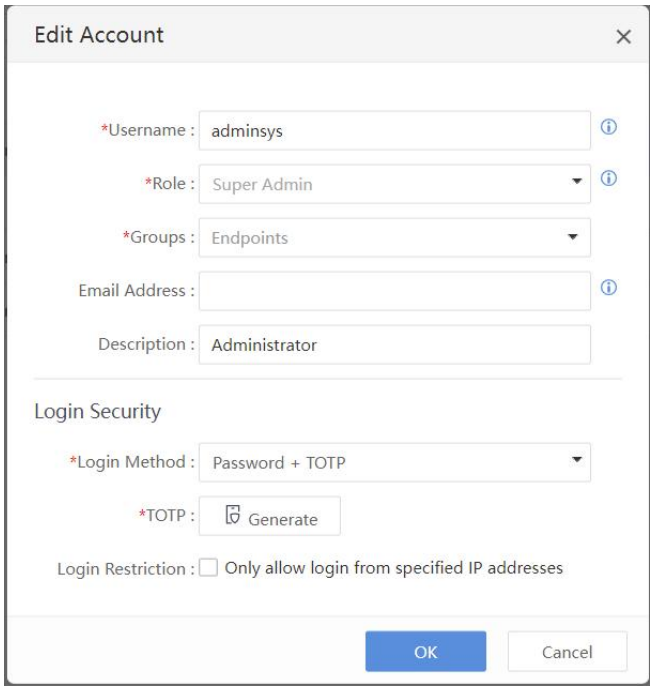
### 3.8.3.3.1 Password Auth

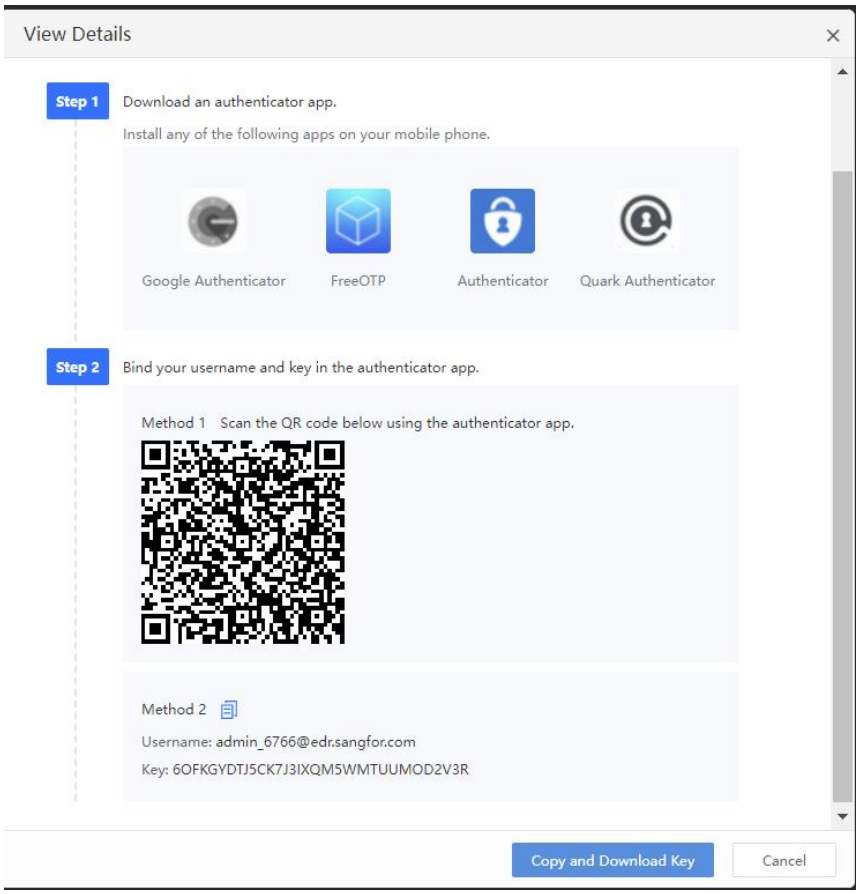
If the account selects **Password Auth**, the user needs to insert a password for authentication during login.




### 3.8.3.3.2 Password + TOTP

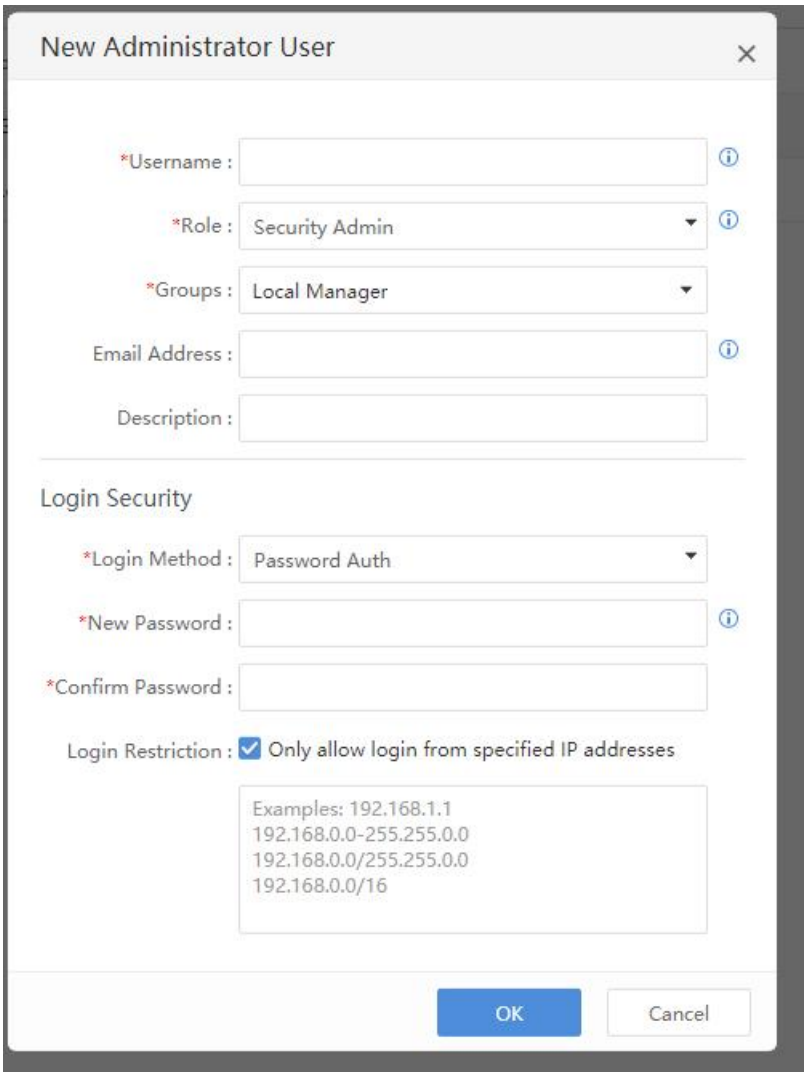
If the account selects **Password + TOTP**, the user needs to insert a password for authentication during login. After passing the password authentication, the user needs to insert the OTP code, which binds with the account.






## 3.8.3.4 Login IP Address Restriction

NovaGuard Manager accounts can be used to log in to the NovaGuard Manager only from authorized IP addresses. To set the IP addresses from which an account can log in to the NovaGuard 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

NovaGuard license has a standard version or ultimate version. Different types of licenses have different functional modules and security protection capabilities, as shown below.

| Feature/Module | | Standard Edition | Ultimate Edition |
|---|---|---|---|
| Prevention | Vulnerability Scan | ✓ | ✓ |
| | Remediation | ✓ | ✓ |
| | Security Compliance Check | ✓ | ✓ |
| | Asset Inventory | ✓ | ✓ |
| | Asset Discovery | ✓ | ✓ |
| | Micro-Segmentation | | ✓ |
| | Hot Patching | | ✓ |
| Protection | Realtime File Monitoring | ✓ | ✓ |
| | Ransomware Honeypot | ✓ | ✓ |
| | Ransomware Protection | ✓ | ✓ |
| | Ransomware Defense | ✓ | ✓ |
| | Fileless Attack Protection | | ✓ |
| | End-of-Support Windows System Protection | ✓ | ✓ |
| | RDP Secondary Authentication (Anti-Ransomware) | | ✓ |
| | Trusted Processes (Anti-Ransomware) | | ✓ |
| | Key Directory Protection (Anti-Ransomware) | | ✓ |
| Detection | Malicious File Detection | ✓ | ✓ |
| | APT Detection | ✓ | ✓ |
| | Brute-Force Attack Protection | ✓ | ✓ |
| | Coordinated Malware Response with XDR | | ✓ |
| | WebShell Detection | | ✓ |
| Response | File Quarantine | ✓ | ✓ |
| | Endpoint Isolation | ✓ | ✓ |
| | File Remediation | ✓ | ✓ |
| | Virus Mitigation | ✓ | ✓ |
| | Extended Detection, Defense and Response (XDR) | | ✓ |
| | Threat Investigation | | ✓ |
| Maintenance | USB Control | ✓ | ✓ |
| | Unauthorized Outbound Access Detection | ✓ | ✓ |
| | Remote Support | ✓ | ✓ |

ted using points; each license point consumes 1 point for one day of usage.

### 3.8.4.1 Examples of License Calculation

If a customer purchases 200 license points, with a total duration of 1 year, and 100 points have been installed and used for 6 months, the points are calculated as follows.

**Total license points**: 200*365=73000 points

**Used license points**: 100*180=18000 points

**Remaining available license points:** 73000-18000=55000.

If you use all 200 licenses = 275 available days.

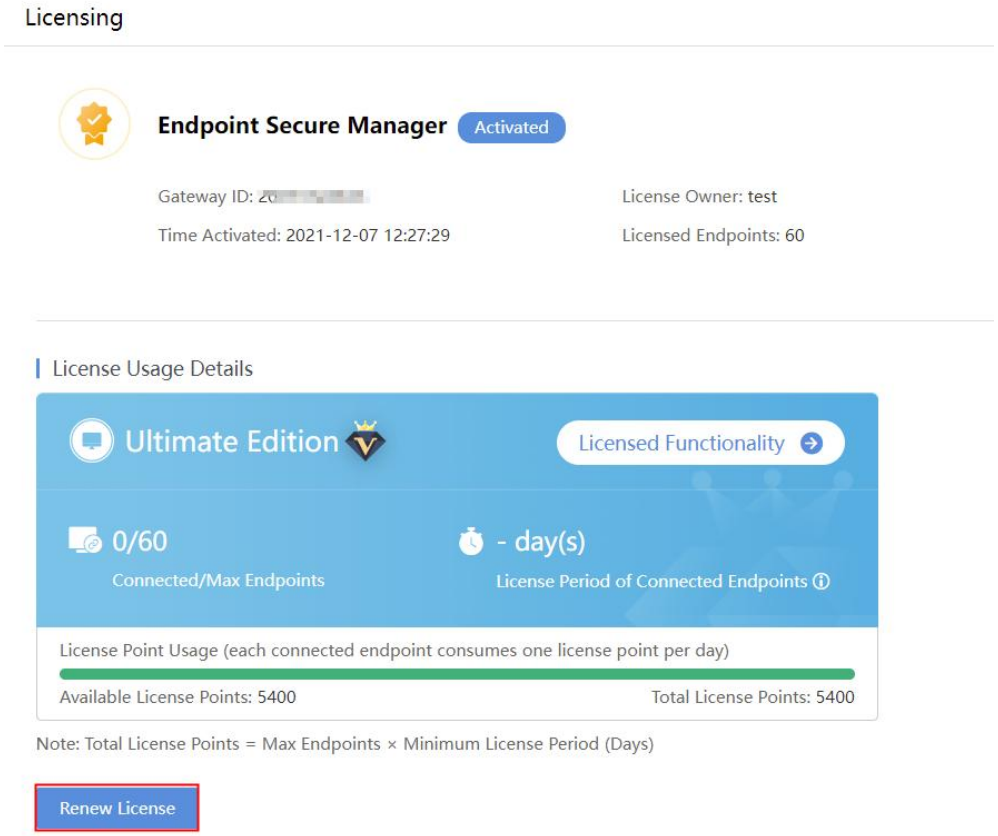
If you use only 1 license = 55000 available days.

**Old version upgrade scenario:**

Unlike the previous version, the current licensing version uses a points calculation method. Therefore, licensing will be smoothly converted when upgrading the previous version to the newest version.

**Add point renewal scenario:**

In the scenario of licensing expiration renewal or point addition, a new licensing ID or new licensing file will be generated. Open **System > Licensing**, click **Renew License**, and import the licensing file to activate or renew the licensing, as shown below.



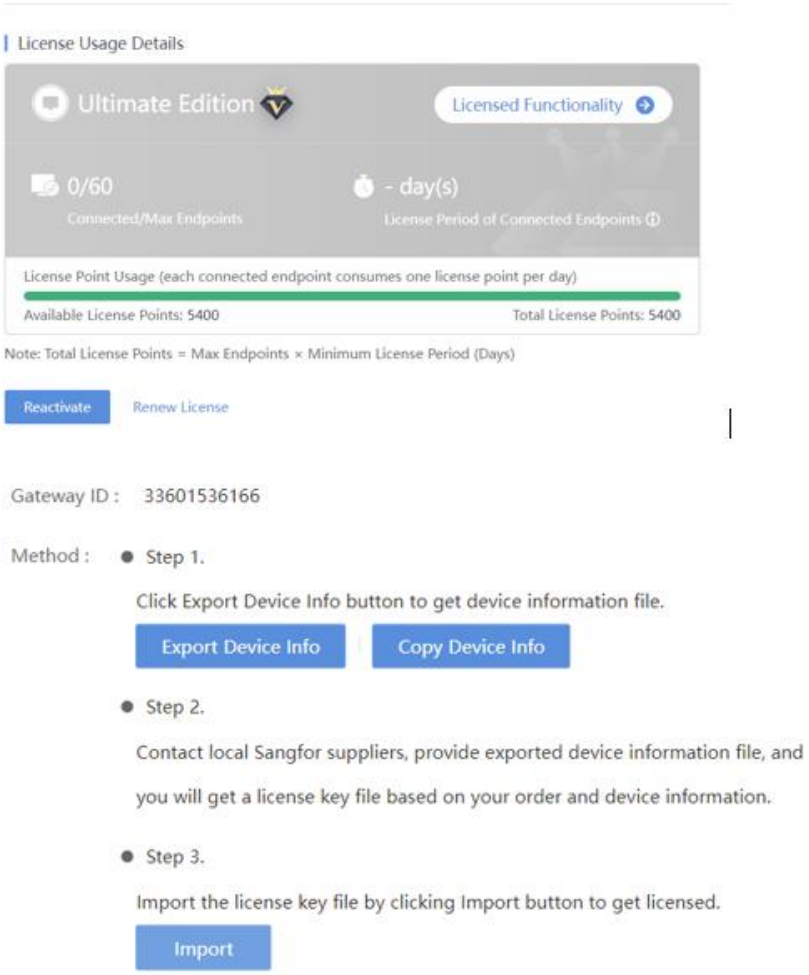

**Relicensing scenario:**

The licensing allows two activations, i.e., the first activation and the activation after the license has expired. The licensing information is related to the hardware of the management platform. If the hardware information changes, the original licensing will be invalid. There are two scenarios of re-licensing as follows.

**The original management platform hardware information has changed and needs to**

**be re-authorized:**

4. Open **System > Licensing** and click **Reactivate**, as shown below.




**The original management platform failed, migrated to a new server installation, and needs to be re-authorize:**

Open **System > Licensing**, export the device info and find a ForeNova representative to get new licensing.

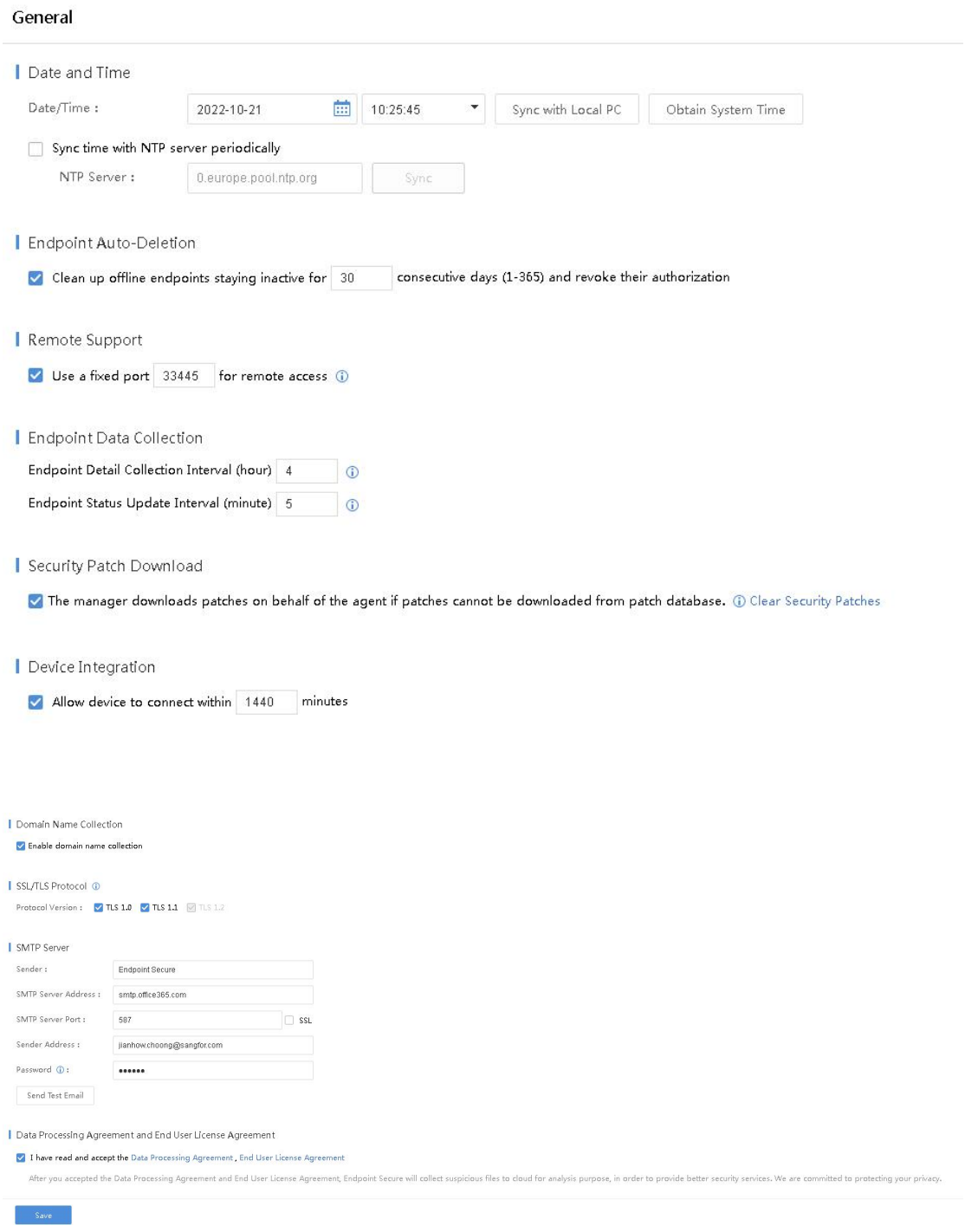
## 3.8.5 System

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 NovaGuard Manager. The following figure shows the configuration page.




The parameters are as follows:

1. **Date and Time**: Set the date and time of the NovaGuard Manager. If you click **Sync**

**with Local PC**, the NovaGuard Manager synchronizes the time with the login PC. If you click **Obtain System Time**, it will obtain the motherboard time of the NovaGuard Manager server. If the NovaGuard Manager is accessible to the Internet, you can check the **Sync time with NTP server periodically** checkbox. In this case, the NovaGuard Manager synchronizes the time with the NTP server.

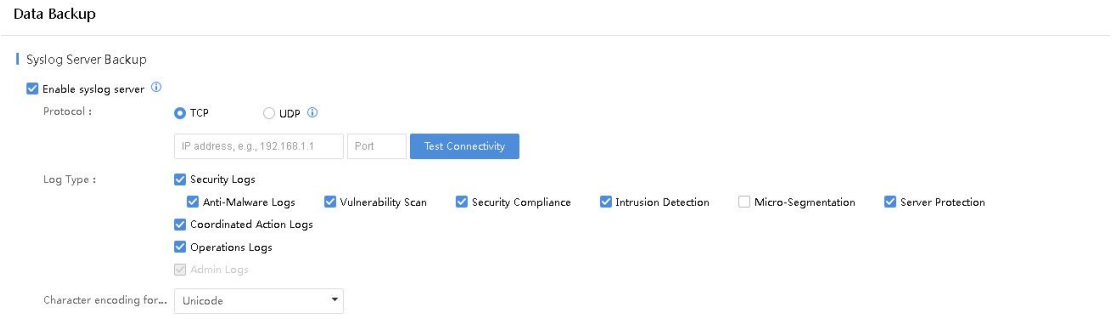
2. **Endpoint Auto-Deletion**: Enable automatic deletion of endpoints on the NovaGuard Manager that are inactive for a long time to release idle licenses automatically.
3. **Remote Support**: Set the fixed port for the NovaGuard remote support function. The computer can remotely control it through the set fixed port.
4. **Endpoint Data Collection**: Set the interval for collecting endpoint data for endpoint checkup in hours. Enter an integer that ranges from 4 to 168.
5. **Security Patch Download**: If the Agent cannot download security patches due to lack of access to the Internet, the NovaGuard Manager can download the security patches on behalf of the Agent. Then, the Agent downloads the security patches from the NovaGuard Manager.
6. **Device Integration**: Set the maximum period within which devices integrated with NovaGuard are allowed to access the NovaGuard Manager. To ensure the access security of integrated devices, such as IAG, NGAF, and Cyber Command, the integrated devices can access the NovaGuard Manager only within the specified period when this check box is selected.
7. **Domain Name Collection**: If **Enable domain name collection** is selected, NovaGuard can record processes that access malicious domain names. This function is used together with correlated botnet forensics and malicious domain name investigation.
8. **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 NovaGuard with other devices, you must select TLS1.0 and TLS1.1.
9. **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.
10. **Data Processing Agreement and End User License Agreement**: If **I have read and accept the Terms of Use and Privacy Policy** is selected, NovaGuard will collect suspicious files to the cloud for analysis to provide better security services. Make sure that the NovaGuard Manager is accessible at https://clt.forenova.com.

## 3.8.5.2 Data Backup

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

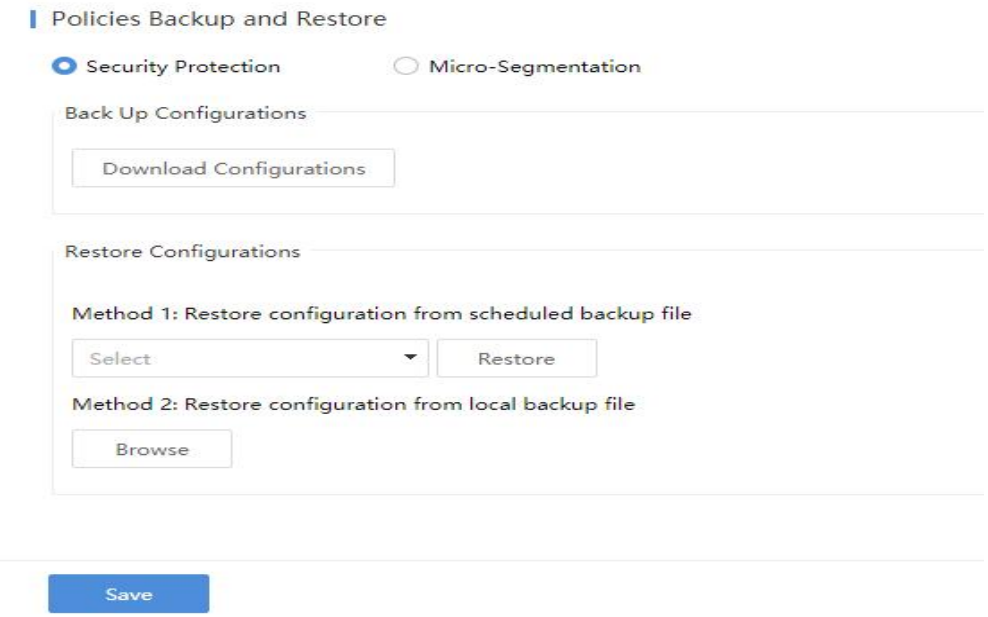
### 3.8.5.2.1 Syslog Server Backup

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




### 3.8.5.2.2 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.

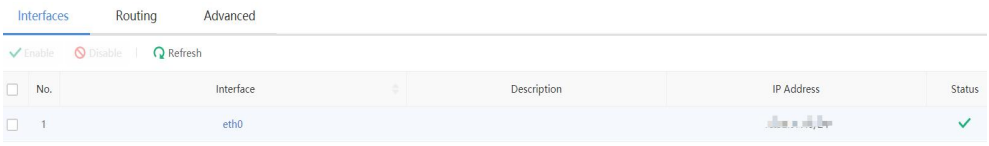
- To restore configurations from a scheduled backup file, select the scheduled backup file, click **Restore**, and then wait until restoration is complete.
- To restore configurations from a local backup file, click **Browse**, select the local backup file, and wait until restoration is complete.

### 3.8.5.3 Network

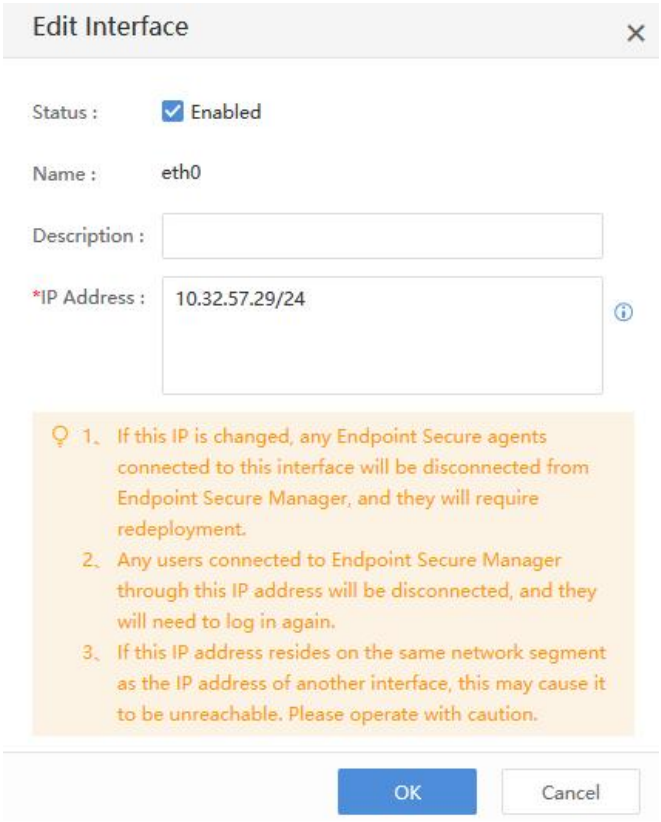
The **Network** page consists of the **Interfaces**, **Routing**, and **Advanced** tabs.

1. **Interfaces**

On the **Interfaces** tab, you can configure IP addresses for network interfaces used for communication between the NovaGuard Manager and internal endpoints. Endpoints can also use the IP addresses to access the NovaGuard 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.



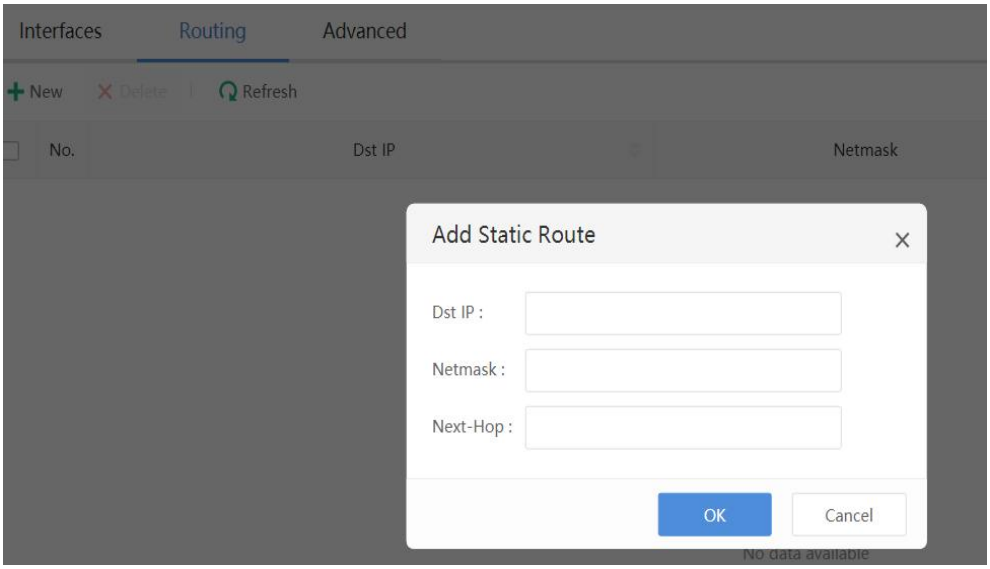

**WARNING**

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

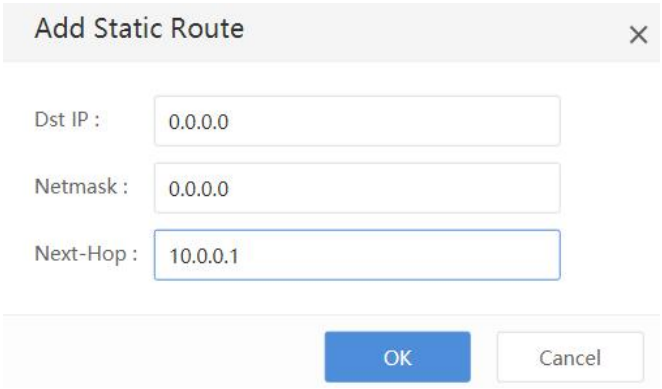
The **Routing** and **Advanced** tabs are displayed if the NovaGuard Manager is installed in ISO or OVA image mode. They are not displayed if the NovaGuard Manager is installed in script mode.

## 2. Routing

The NovaGuard 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.

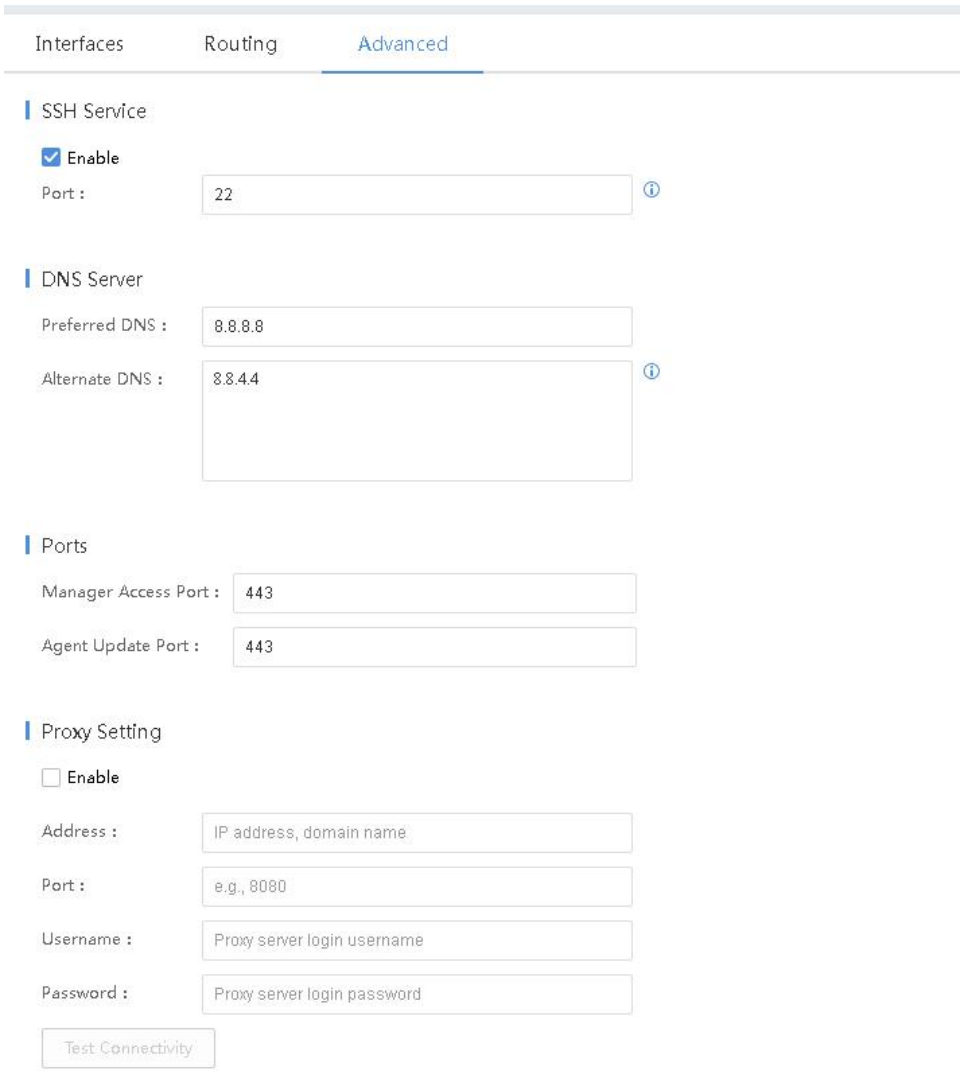


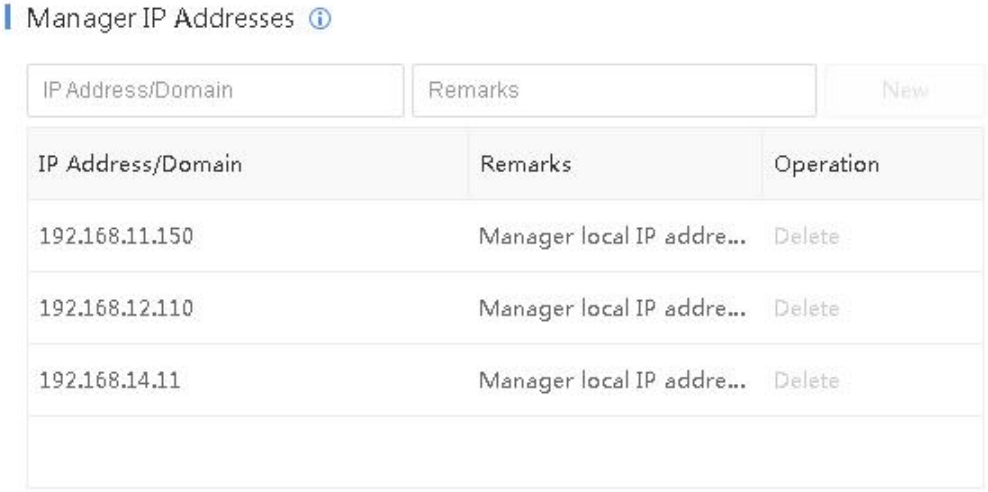

Click **New** and specify the route information.




### 3. Advanced

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


Interfaces
Routing
Advanced
SSH Service
Enable
Port :
22
DNS Server
Preferred DNS :
8.8.8.8
Alternate DNS :
8.8.4.4
Ports
Manager Access Port :
443
Agent Update Port :
443
Proxy Setting
Enable
Address :
IP address, domain name
Port :
e.g., 8080
Username :
Proxy server login username
Password :
Proxy server login password
Test Connectivity


Manager IP Addresses
IP Address/Domain
Remarks
New
IP Address/Domain
Remarks
Operation
192.168.11.150
Manager local IP addre...
Delete
192.168.12.110
Manager local IP addre...
Delete
192.168.14.11
Manager local IP addre...
Delete

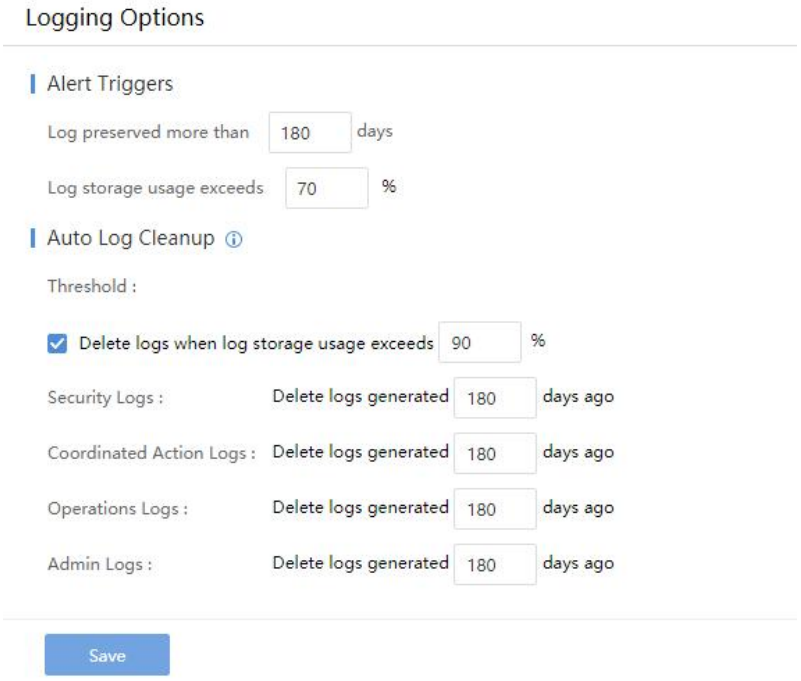
The parameters are as follows:

- **SSH Service**: In this area, you can enable or disable the SSH port and change the SSH port of the NovaGuard Manager backend. The default port is 22345.
- **DNS Server**: In this area, you can set the DNS server addresses of the NovaGuard Manager for domain name resolution when the NovaGuard Manager connects to the Internet to update the antivirus database.
- **Ports**: In this area, you can configure the port to access the NovaGuard Manager and the port used for Agent updates.
- **Proxy Setting**: When the NovaGuard manager cannot directly connect to the Internet, and there is a proxy server in the intranet, you can configure it to update the database through the proxy server and use cloud search. Support for HTTP or HTTPS proxy.
- **Manager IP Addresses**: In this area, you configure multiple IP addresses or domain names to enable NovaGuard Manager to communicate with the agent, whether the agent is connected to the intranet or the internet.

### 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**:

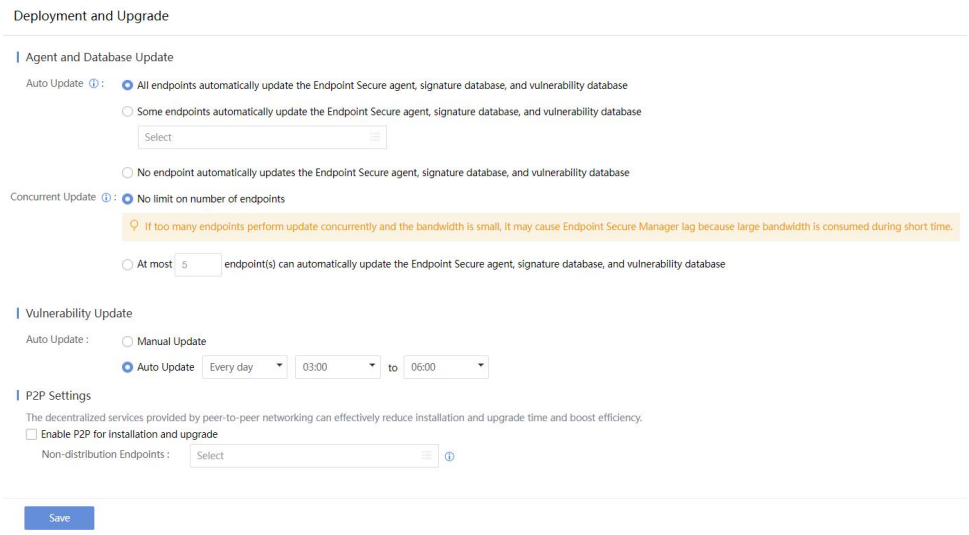
1. When the log storage usage exceeds 70%, a banner notification will be displayed.
2. When the log storage usage exceeds the threshold for deleting logs, logs are automatically deleted. Security logs include Anti-Malware, Vulnerability Scan, Integrity Check, Intrusion Detection (WebShell Detection,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

## 3.8.5.5 Update Options

The NovaGuard Manager supports canary updates and staggered updates of the NovaGuard 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 concurrently updated endpoints to reduce the update's impact on the network bandwidth.

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

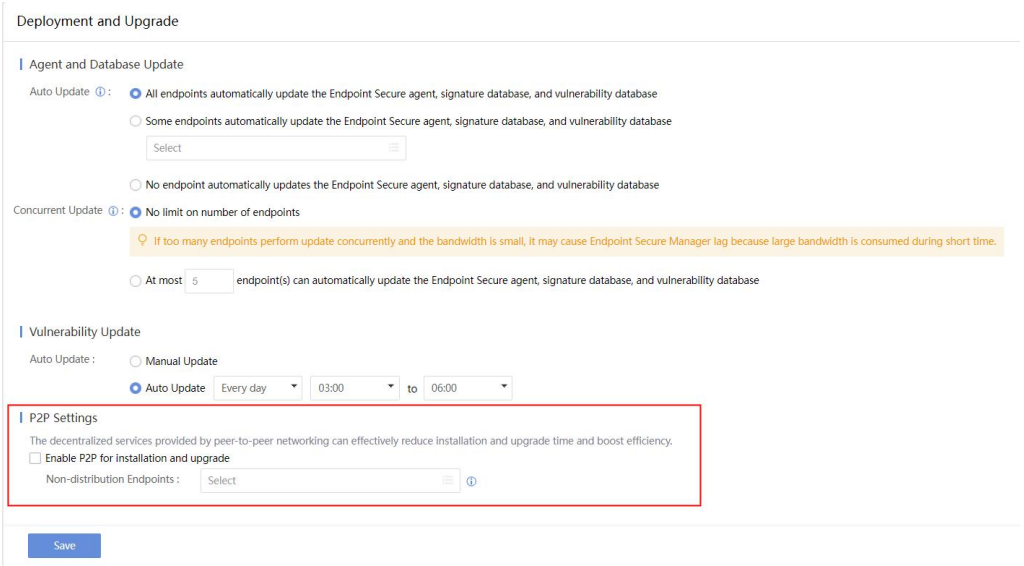



**Agent and Database Update**: Set the endpoint update method and the maximum number of concurrently updated endpoints.

- **Auto Update**: that is, canary update. Select endpoints to be updated.
- **Concurrent Update**: that is, staggered update. Set the maximum number of concurrently updated endpoints 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 NovaGuard Manager automatically updates the vulnerability database at the specified time.

Enable P2P for installation and upgrade in **P2P Settings**, and each endpoint that has completed deployment or upgraded can assist the management platform in distributing resources to other endpoints in the subnet.



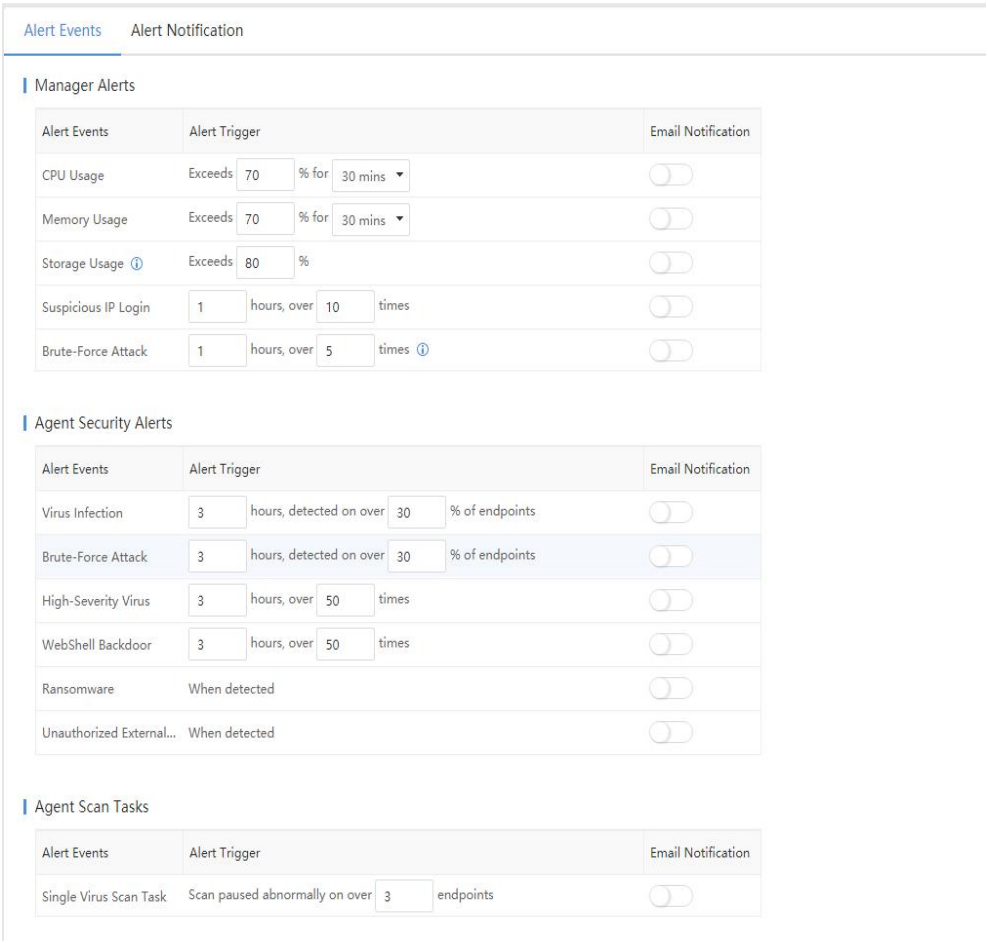
NOTE

Only support intranet environment. NAT and public network scenarios are not recommended to open this function. The upgrade speed will be reduced after enabled.

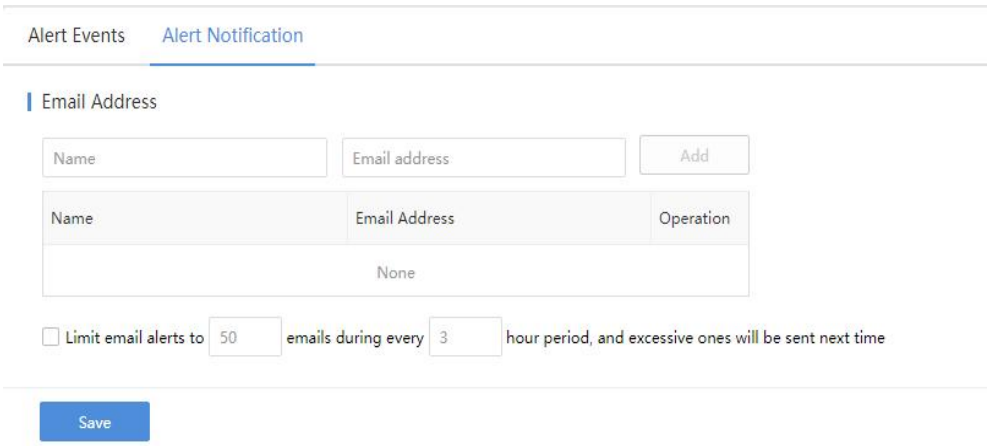
## 3.8.5.6 Alert Options

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

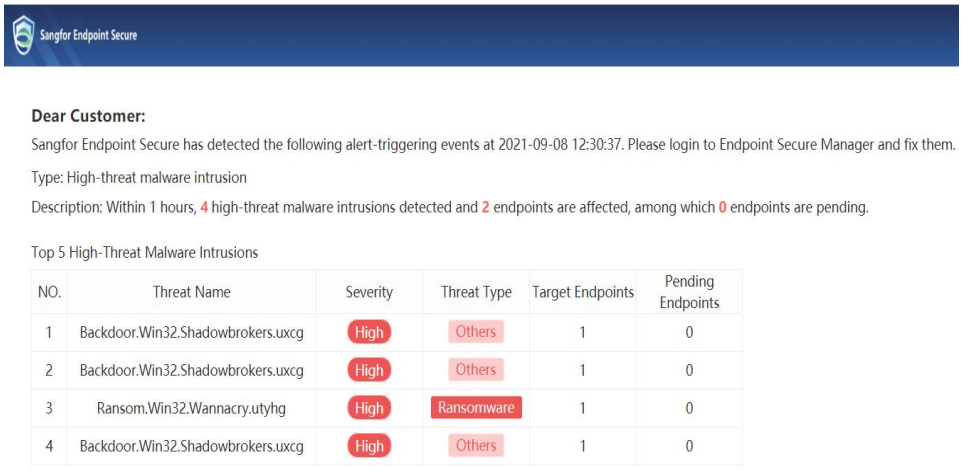
The **Alert Options** page consists of the **Alert Events** and **Alert Notification** tabs. The following figure shows the **Alert Events** tab.




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




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




**NOTE**

You must first configure the SMTP server on the **General** page to send alert emails.

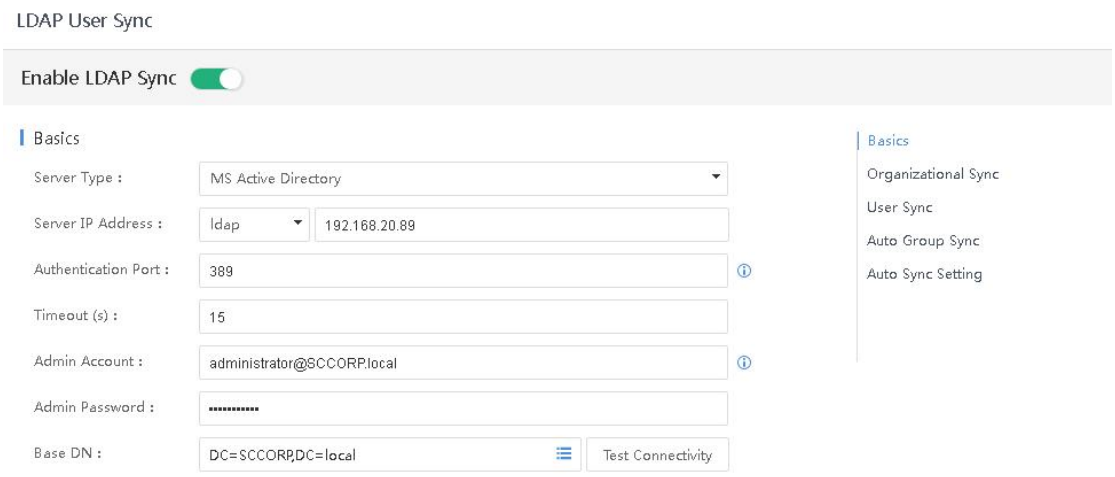
## 3.8.5.7 LDAP Sync

The customer's intranet already has an AD domain controller server, and intranet assets are managed uniformly on the AD domain controller server. The administrator needs a way to automatically synchronize the OUs and users specified by the AD domain server to the NovaGuard to achieve unified user information management.

**LDAP Sync Configuration**

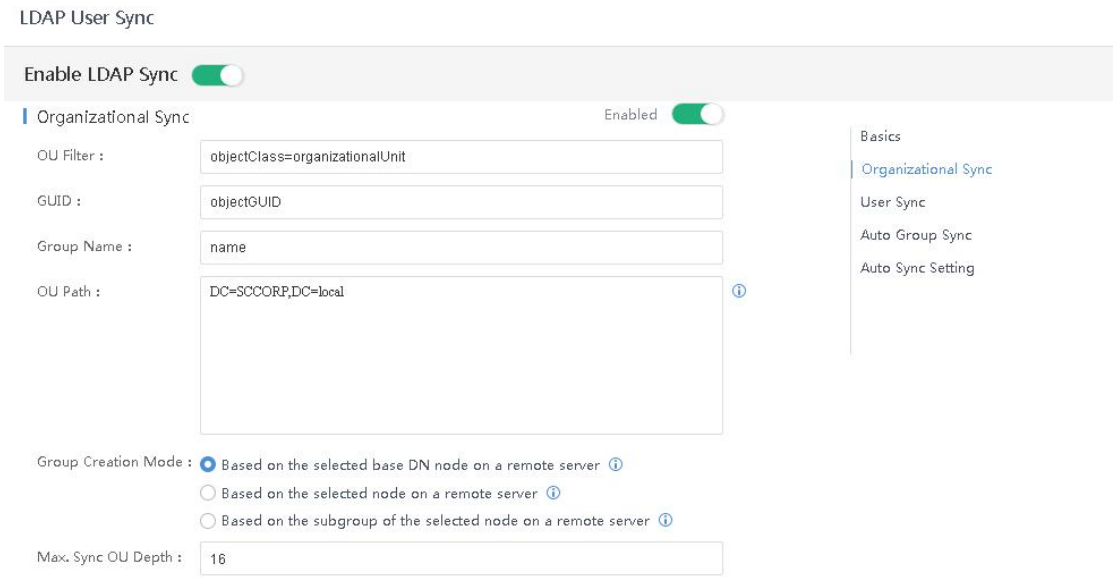
Go to **System > System > LDAP User Sync.**

1. Basic Configuration



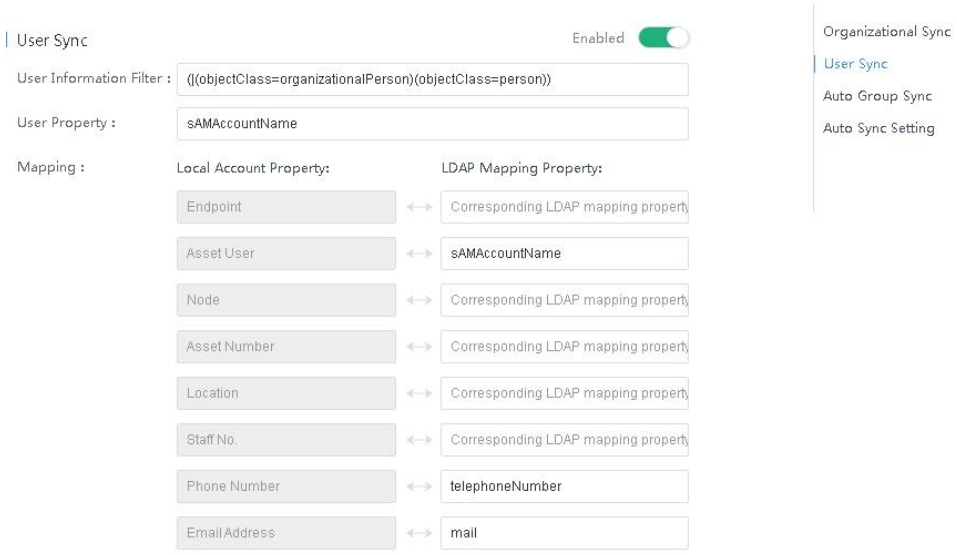

**Basic configuration**: Configure the AD domain controller server IP address, Authentication Port, Admin Account, Admin Password, and Base DN. The administrator account needs to be in the following format, such as administrator@domain.com.

2. **Organizational Sync**



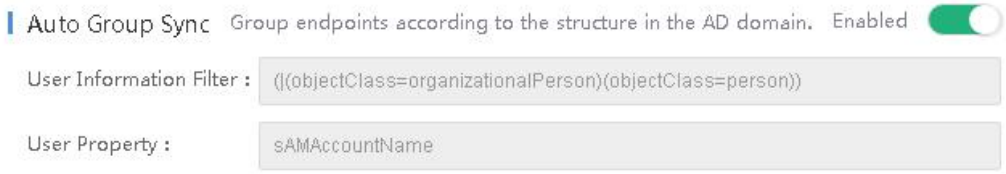

Configure the **OU Path** and the **Group Creation Mode**, and keep the other settings as defaults.

3. **User Sync**




**User synchronization**: Map domain user attributes to NovaGuard management information. The rest keep the default configuration.

4. **Auto Grouping**



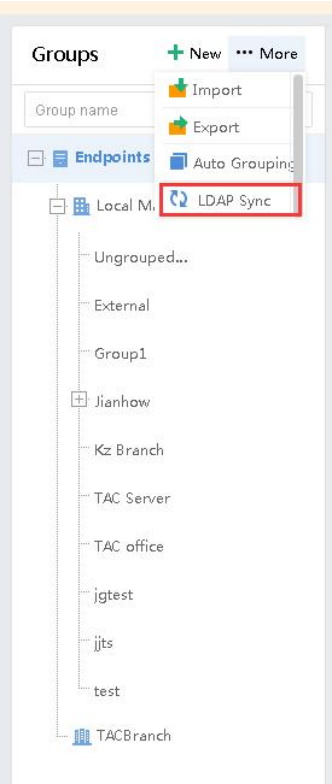

**Auto Group Sync**: Achieve automatic grouping on the NovaGuard management according to the OU where the endpoint account name is located. The endpoint has been logged in with a domain account, and the automatic grouping can be triggered only when the LDAP synchronization is triggered.

**Trigger LDAP Sync**

LDAP synchronization can be triggered by manual synchronization or auto synchronization.

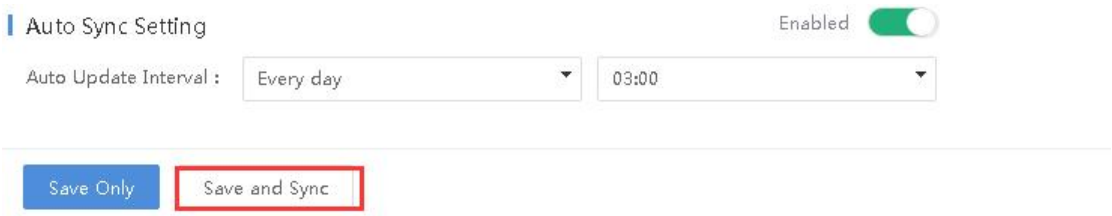
**5. Manual Trigger**

Go to **Endpoints > Groups > More, and c**lick **LDAP Sync** to trigger an immediate sync manually, as shown below.



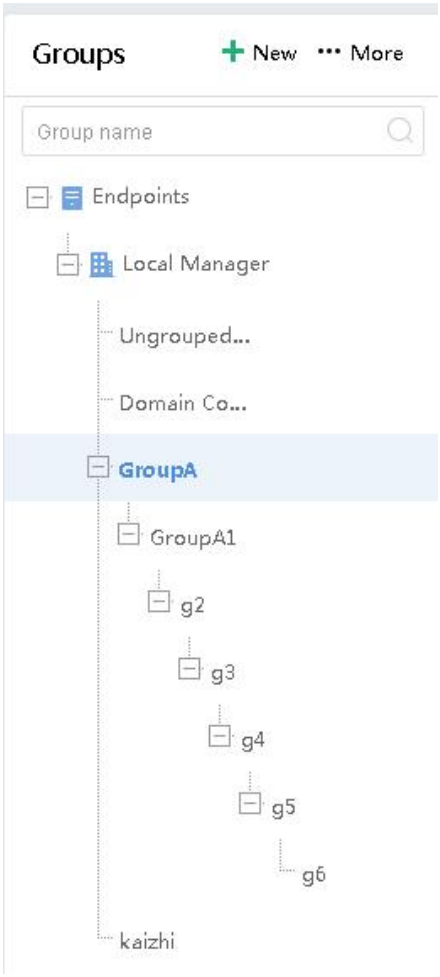

### 6. Auto Sync

Enable **Auto Sync setting**. Real-time synchronization will start when you click **Save and Sync**.

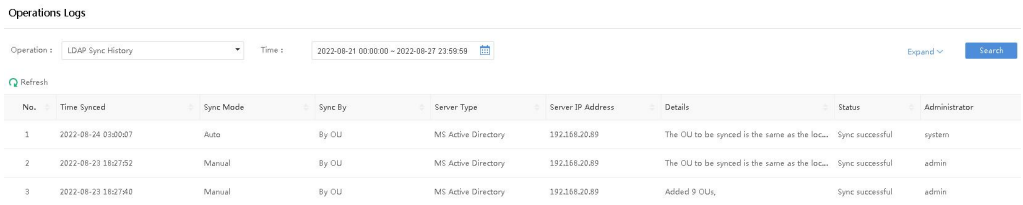



**LDAP Sync Result**

The domain OU is synchronized to the endpoint group page, as shown in the figure below. When the agent is installed on an endpoint and logged in with a domain account, it will automatically go online to the group where the domain controller OU is located.

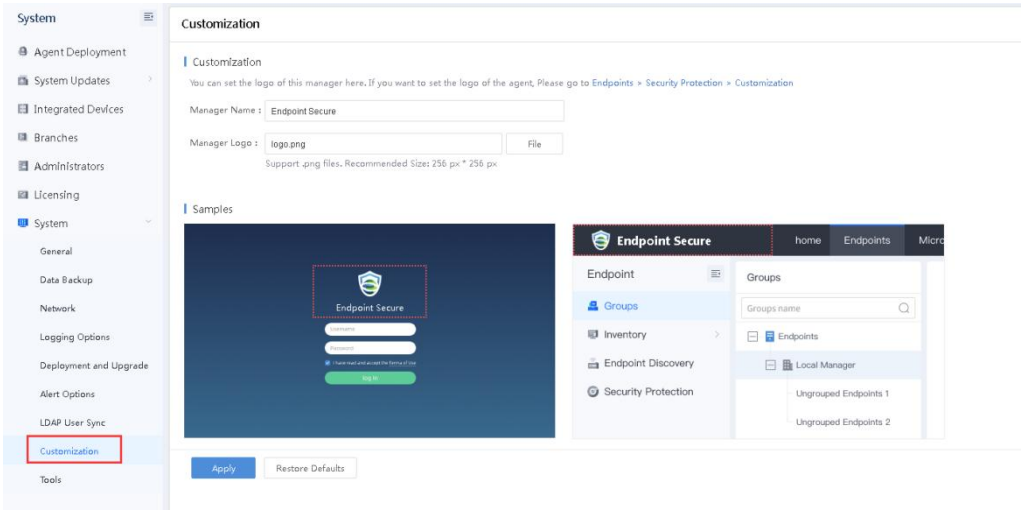



View **Logs > Operation Logs** to view the details of LDAP synchronization history, as shown in the following figure.




## 3.8.5.8 Customization

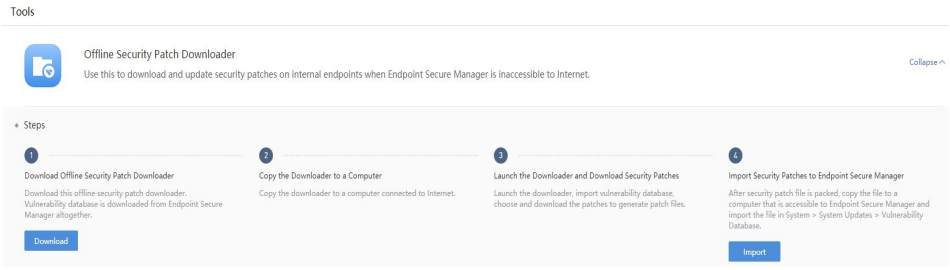
You can personalize the platform's icon and logo in the management platform's system settings.




## 3.8.5.9 Tools

The **Tools** page provides the Offline Security Patch Downloader, which is used with the NovaGuard Manager's vulnerability scan and patching function. Suppose the NovaGuard 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 NovaGuard Manager to patch endpoint vulnerabilities.

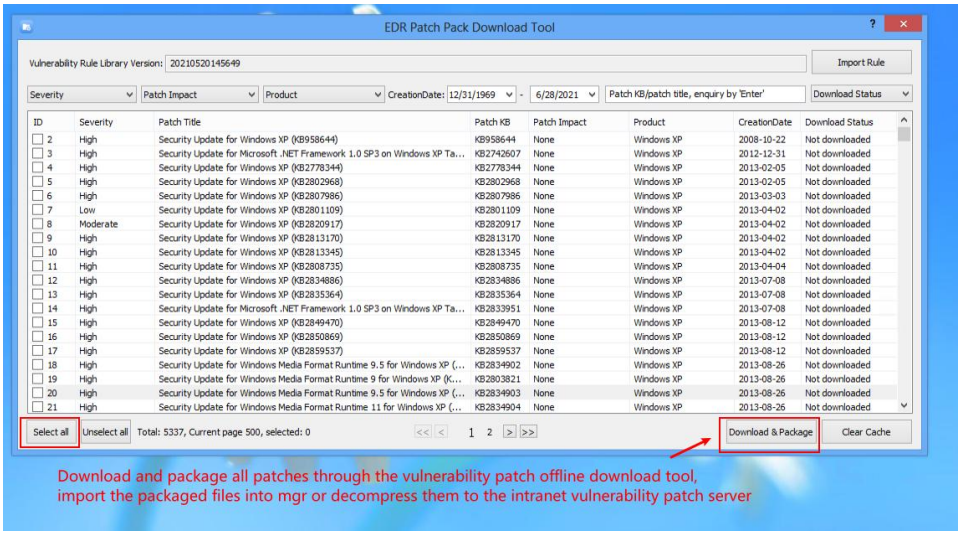
The following figure shows the **Tools** page.



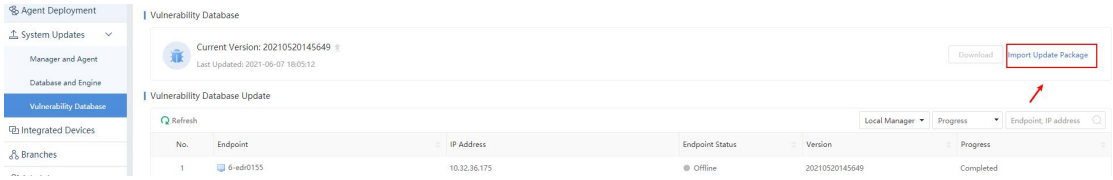

### 3.8.5.9.1 Tools

**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 NovaGuard Manager, as shown in the following figure.




**Step 4.** Scan and patch endpoint vulnerabilities.

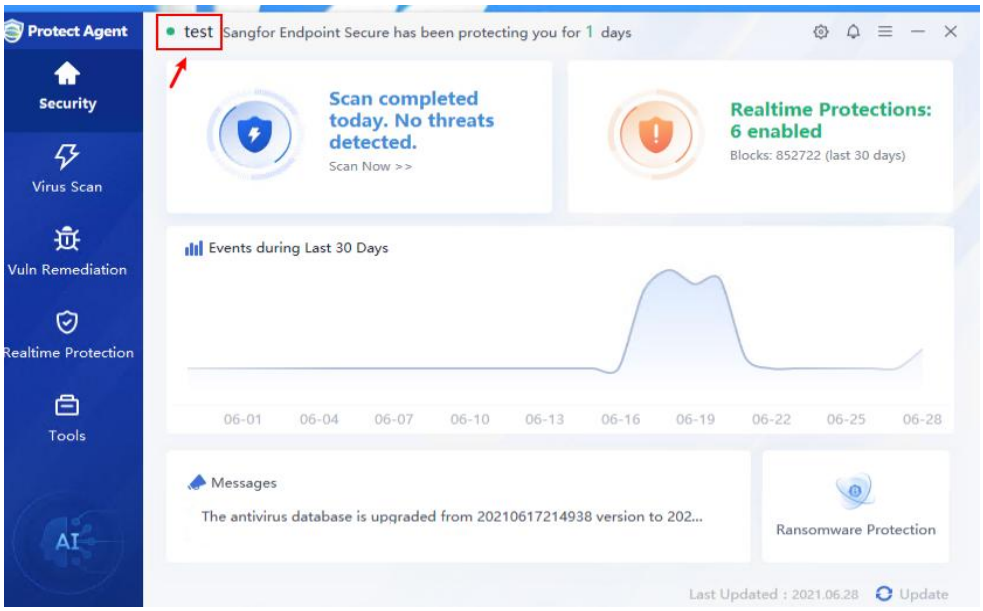
# 4 Agent

## 4.1 Windows 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.

### 4.1.1 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.



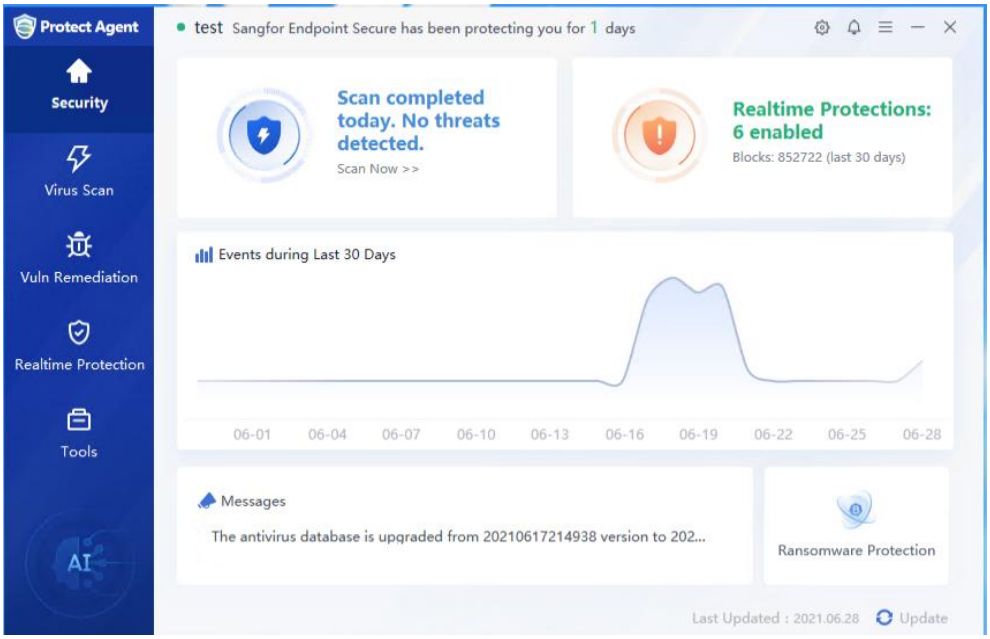

### 4.1.2 Security

On the **Security** page, the endpoint protection duration and the connection status between the Agent and the NovaGuard Manager are at the top.

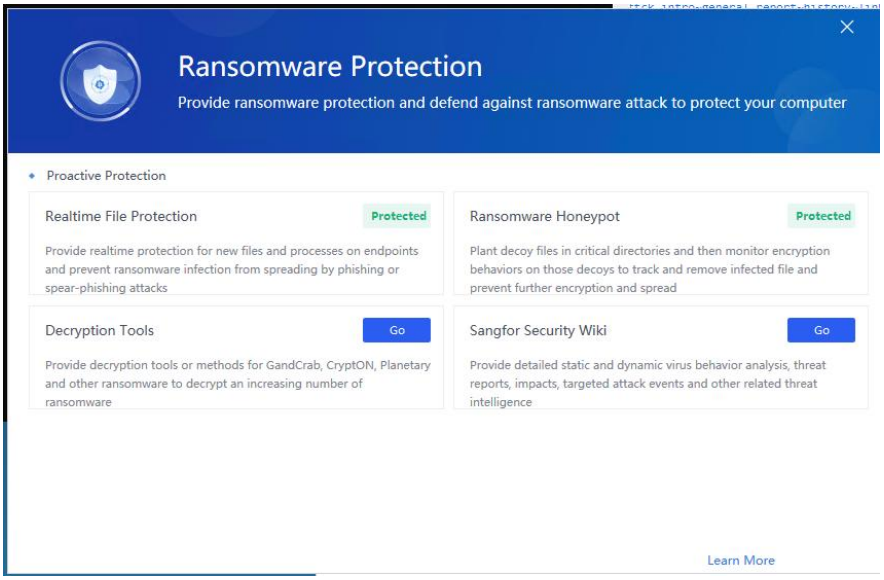
- If  at the upper left corner is green, the Agent is connected to the NovaGuard Manager.
- If the icon is gray, the connection between the Agent and the NovaGuard Manager is abnormal.

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 updates, software version updates, and notifications sent by the administrator.

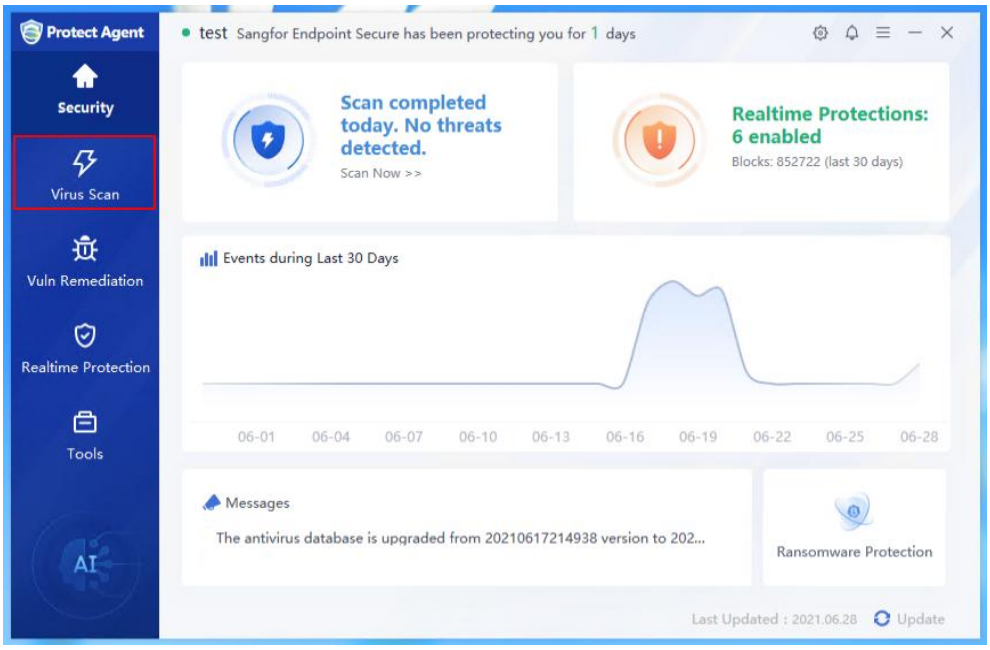



The lower right corner displays the ransomware protection mechanisms in the prevention, protection, detection, and response phases, as shown in the following figure.




## 4.1.3 Virus Scan

On the **Virus Scan** 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 their subdirectories.

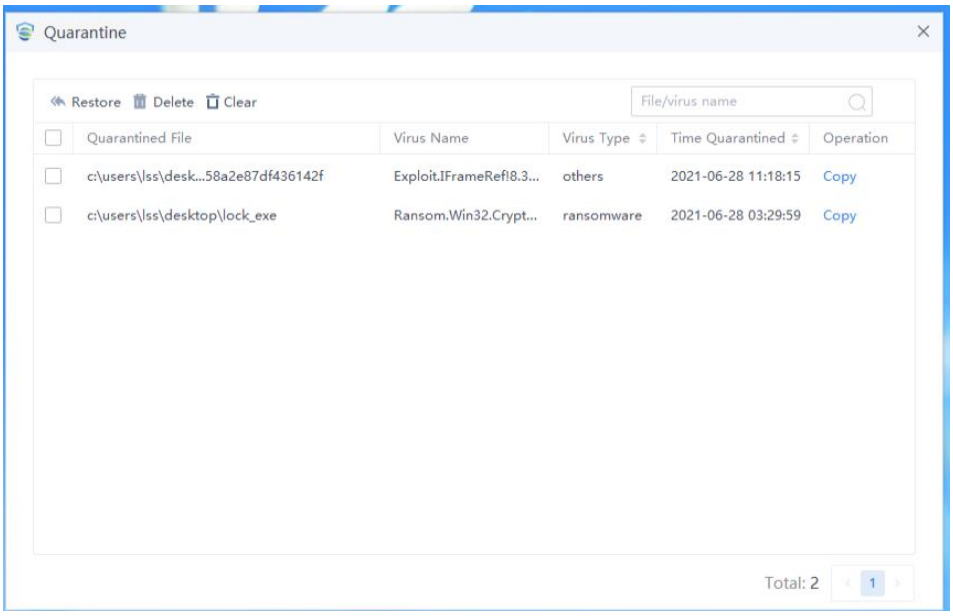
**Full Scan**: Scan all Windows system directories.

**Custom Scan**: Scan specified files or directories.

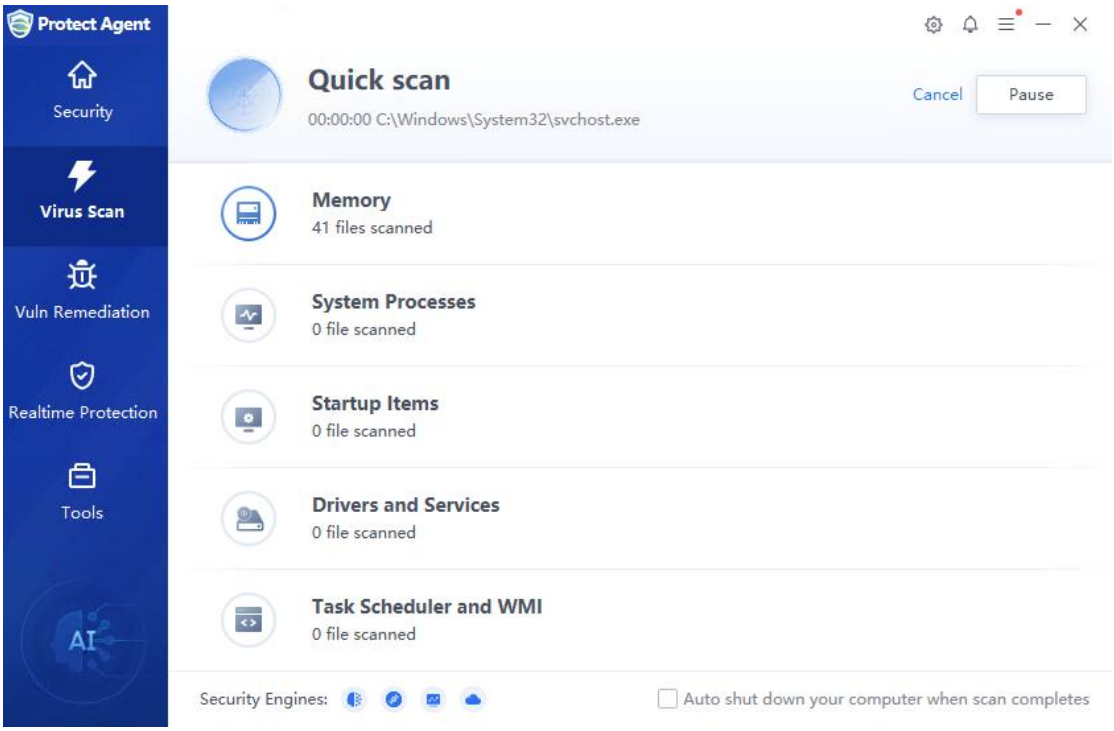
In the lower-left corner of the **Virus Scan** page, you can view the scan engines. A blue icon indicates that an engine is enabled, and a gray icon indicates that an engine is disabled. You can move the cursor to the engine icon to view detailed engine information.

| Icon | Engine | Description |
|---|---|---|
| | Engine Zero | It is a ForeNova-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**, restore, delete, or clear quarantined files with one click, as shown in the following figure.



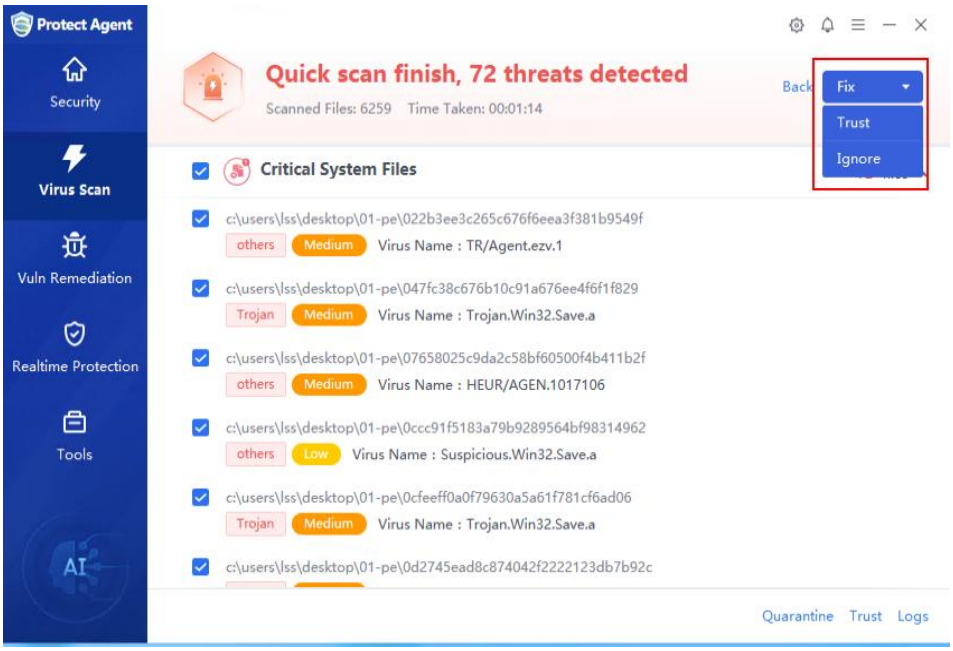

For example, click **Quick Scan** to trigger the scanning of critical system directories, as shown in the following figure.




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.

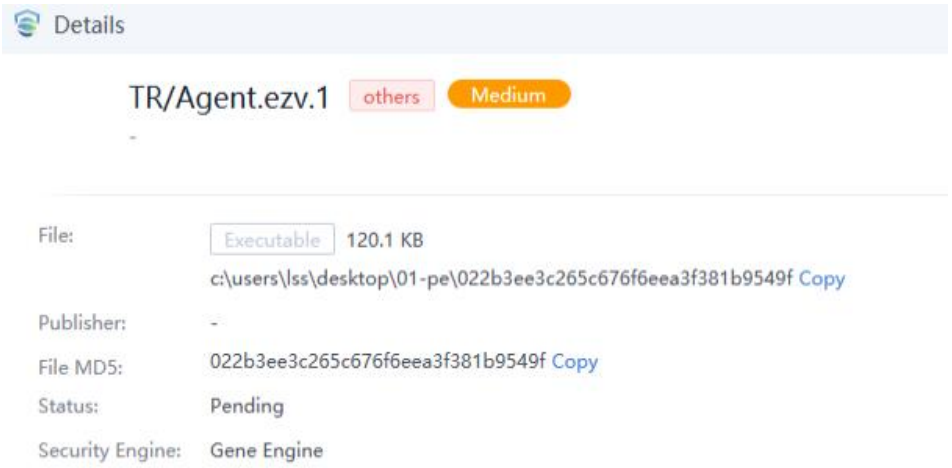



**Fix**: Quarantine found malicious files. For a macro virus or infectious malicious files, the NovaGuard agent will try to fix them first. Quarantined files can be viewed in the **Quarantine** area.

**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.

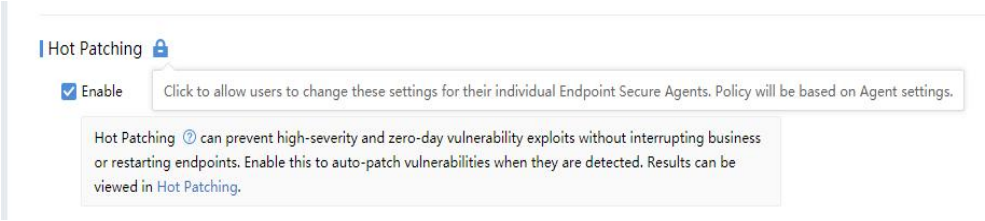
**Details**: View detailed information about a malicious file, as shown in the following figure.



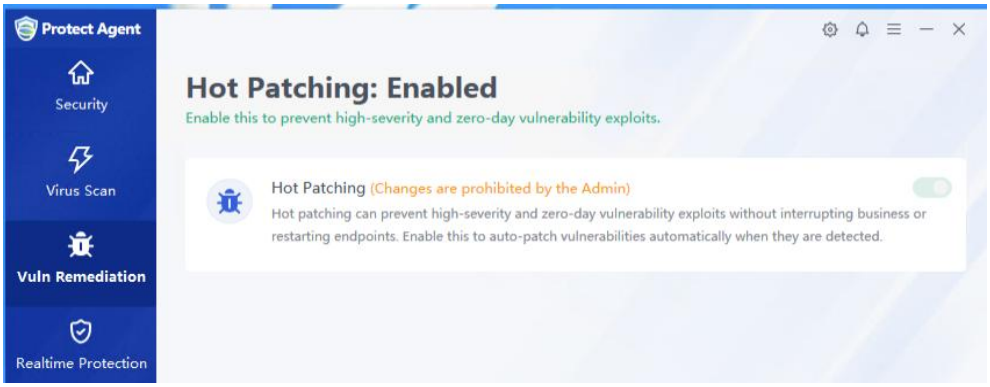

## 4.1.4 Vulnerability Scan

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

Display on the NovaGuard Manager.

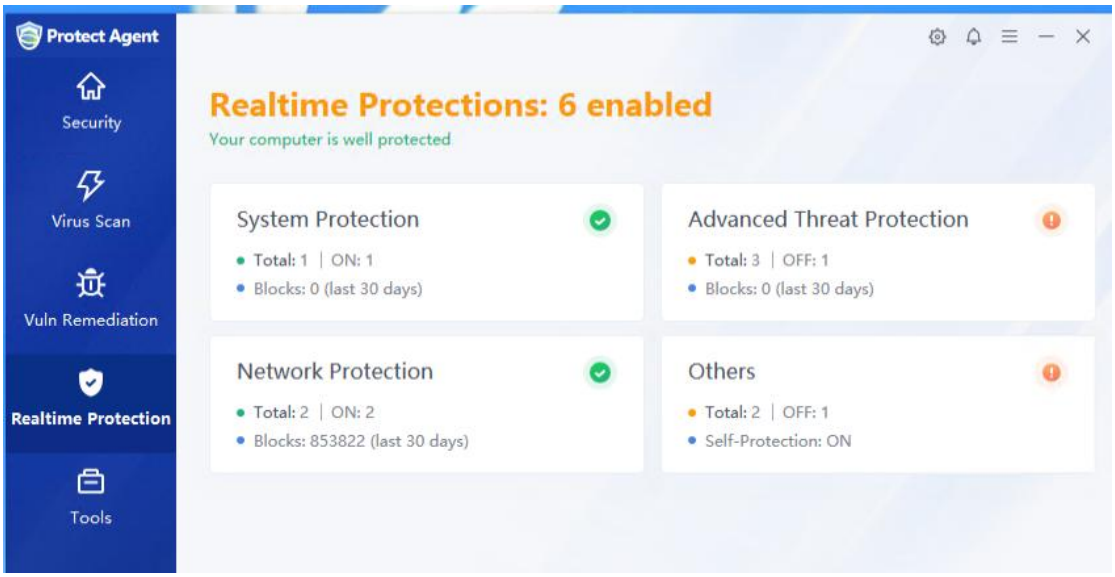



Display on the NovaGuard Agent.

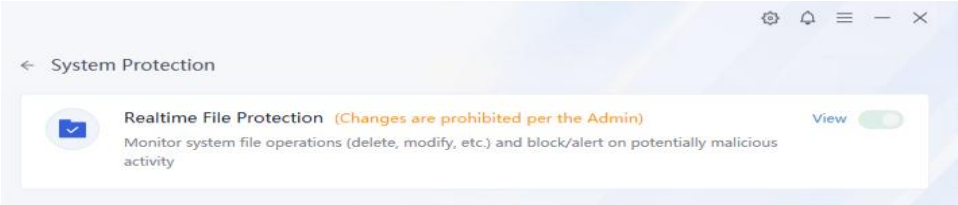



## 4.1.5 Realtime Protection

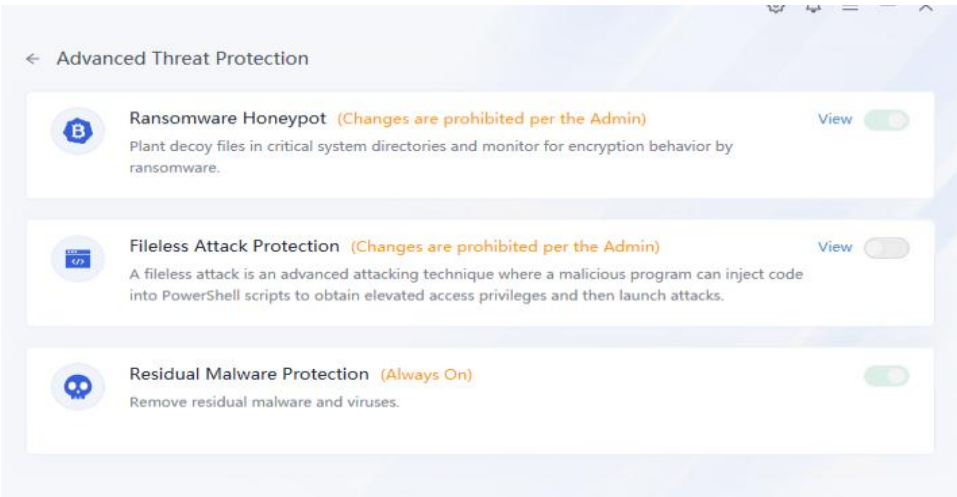
Realtime protection provides the following types of protection: **System Protection, Advanced Threat Protection, Network Protection**, and **Others**. The **Realtime Protection** page displays the statuses of different protection types, as shown in the following figure.



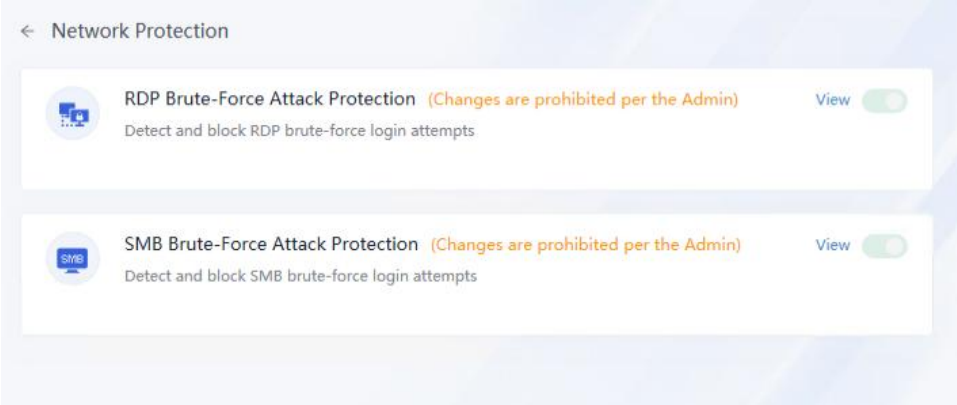

Click **System Protection** to go to the **System Protection** page, where **Realtime File Protection** is provided. The administrator can revoke the configuration permissions from endpoint users. Suppose the administrator does not allow endpoint users to modify the configurations. In that case, the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



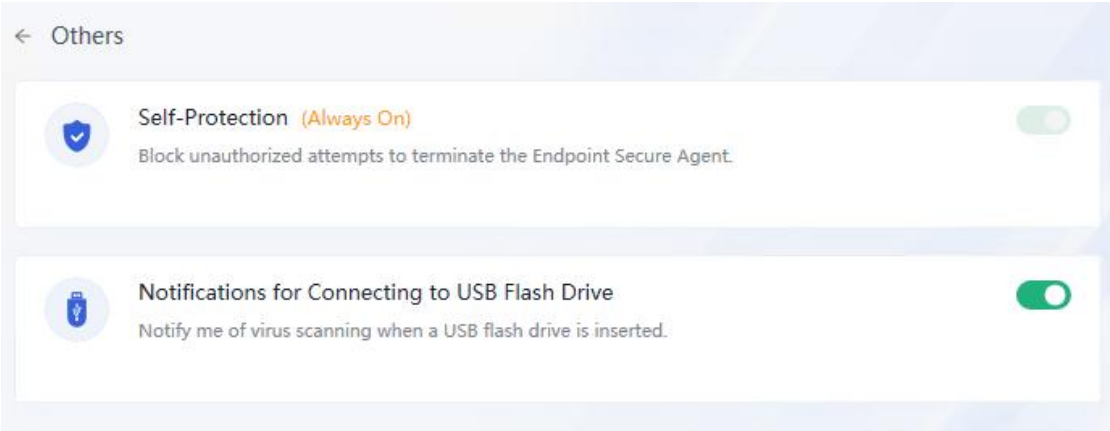

Click **Advanced Threat Protection** to go to the **Advanced Threat Protection** page, where **Ransomware Honeypot**, **Fileless Attack Protection**, and **Residual Malware Protection** are provided, as shown in the following figure.




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 **Notifications for Connecting to USB Flash Drive** are provided, as shown in the following figure.




**Notifications for Connecting to USB Flash Drive** is enabled by default. A shortcut menu is displayed in the lower right corner when a USB flash drive is inserted into the endpoint.

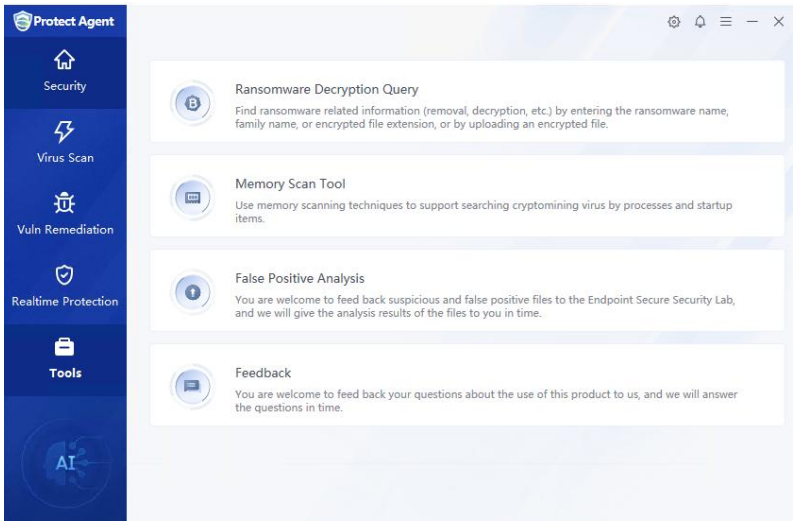
You can open, remove, or perform a virus scan for the USB flash drive, as shown in the following figure.




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

## 4.1.6 Tools

The **Tools** page consists of the **Ransomware Decryption Query**, **Memory Scan Tool, False Positive Analysis**, and **Feedback**.

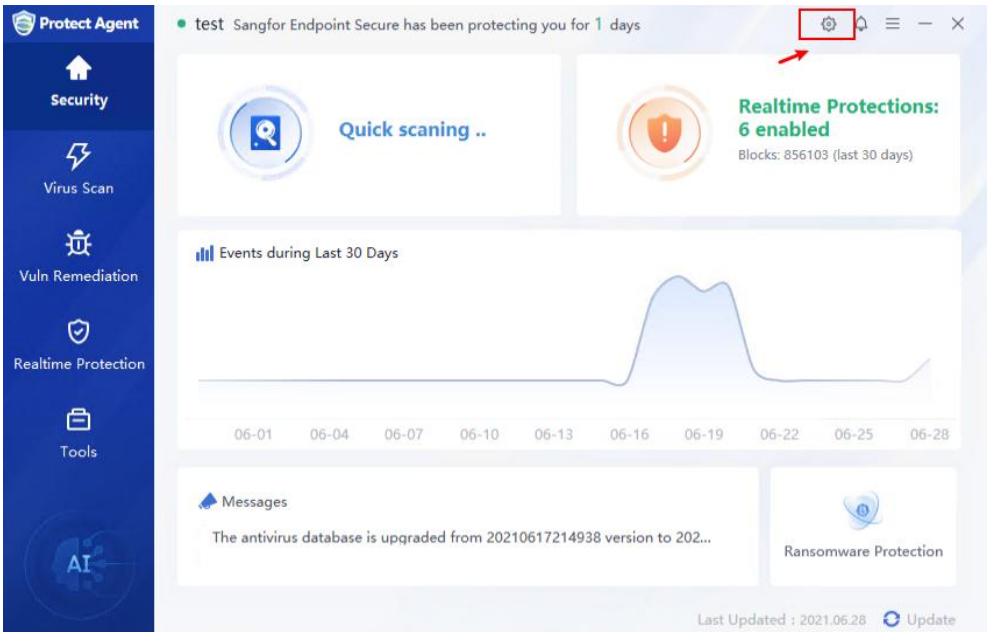



**Ransomware Decryption Query**: When the server is attacked by ransomware, you can query ransomware information and whether decryption is available using the ransomware decryption tool based on ransomware features, such as the encrypted file extension and ransom information.

## 4.1.7 NovaGuard Agent-Settings

Click  in the upper right corner of the Agent to go to the **NovaGuard Agent > Settings**

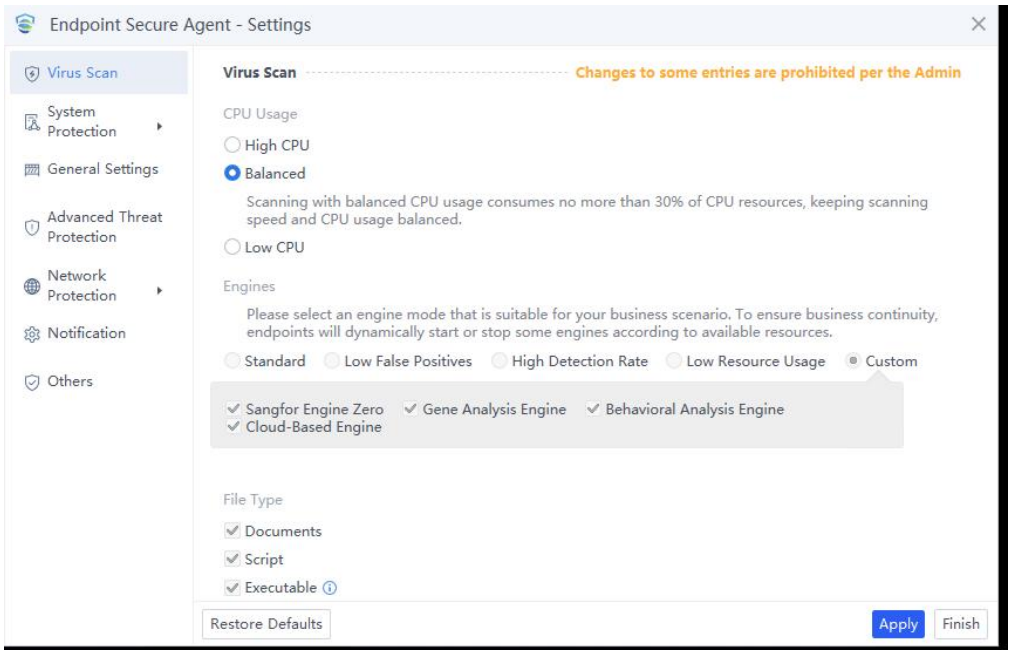
page, as shown in the following figure.




The **NovaGuard 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 NovaGuard Manager. The administrator can revoke the configuration permissions from endpoint users.

In the **Security Protection** module of the NovaGuard 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 to some entries are prohibited per 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 actions.

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 between scan speed and CPU usage is reached, 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 the maximum number of compression layers of a file to scan. The scan software can scan compressed files up to 10 layers deep.

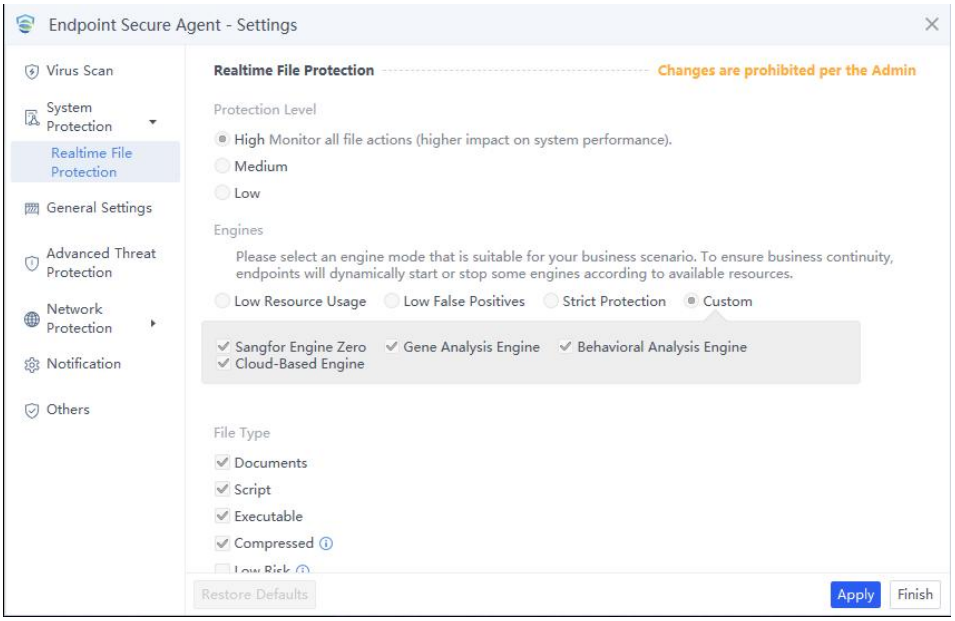
**Action**: When malicious files are found, the actions that can be performed include **Standard**, **Enhanced**, and **No Action - Report Only**.

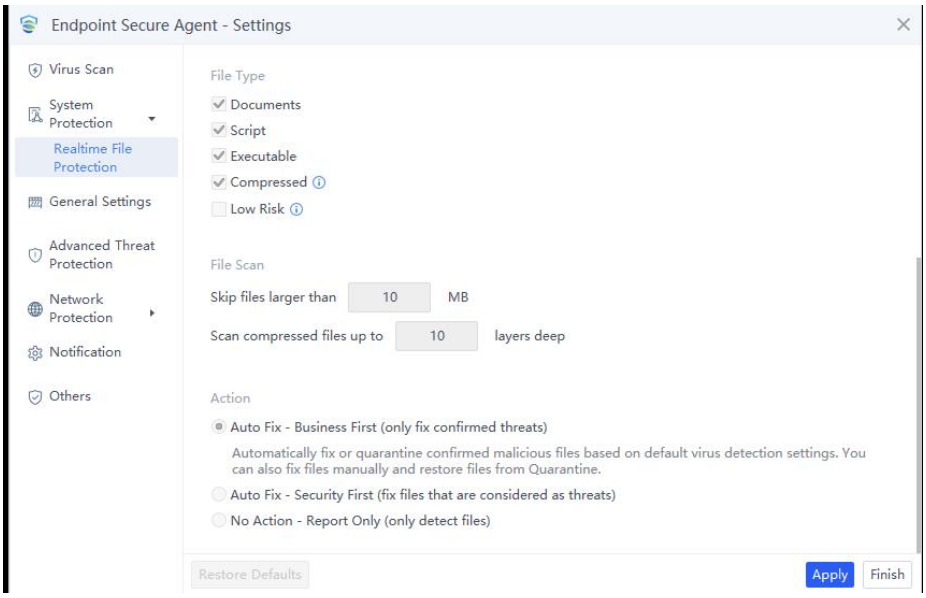
- **Auto Fix – Business Continuity First**: Quarantine malicious files on the blacklist and report detection logs for threat files not on the blacklist. **Standard** is selected by default.
- **Auto Fix-Security First**: Quarantine all detected threat files. This option is suitable for strict protection scenarios.

- **No Action-Report Only**: Report security logs for all threat files without quarantining the files. This option is suitable for scenarios where an on-duty security professional is responsible for fixing threats.

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

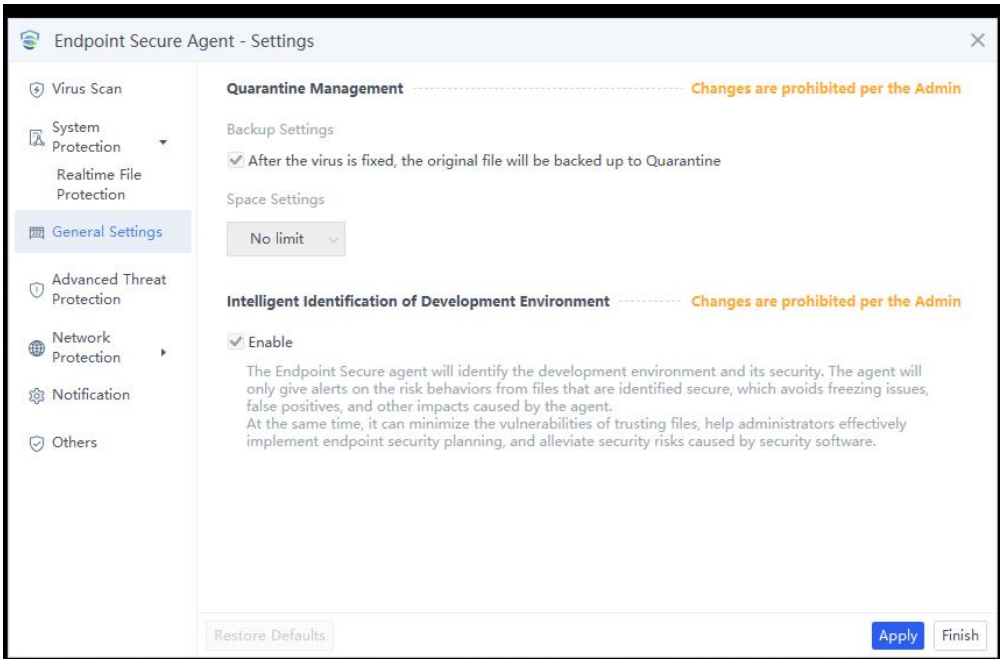
Click **Save & Exit** to save the page configurations and close the **NovaGuard Agent > Settings** page.



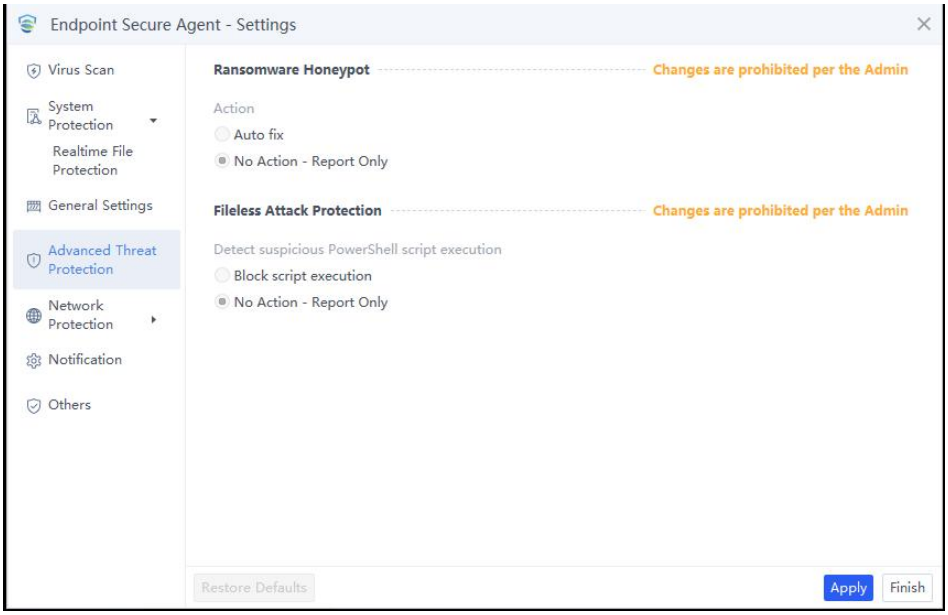




**System Protection**: On the **System Protection** page, you can set the protection level, scan engine, file type, scan options, and action for real-time file protection. The parameter settings are the same as those in the **Realtime File Protection** area on the **Realtime Protection** tab under **Endpoints**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

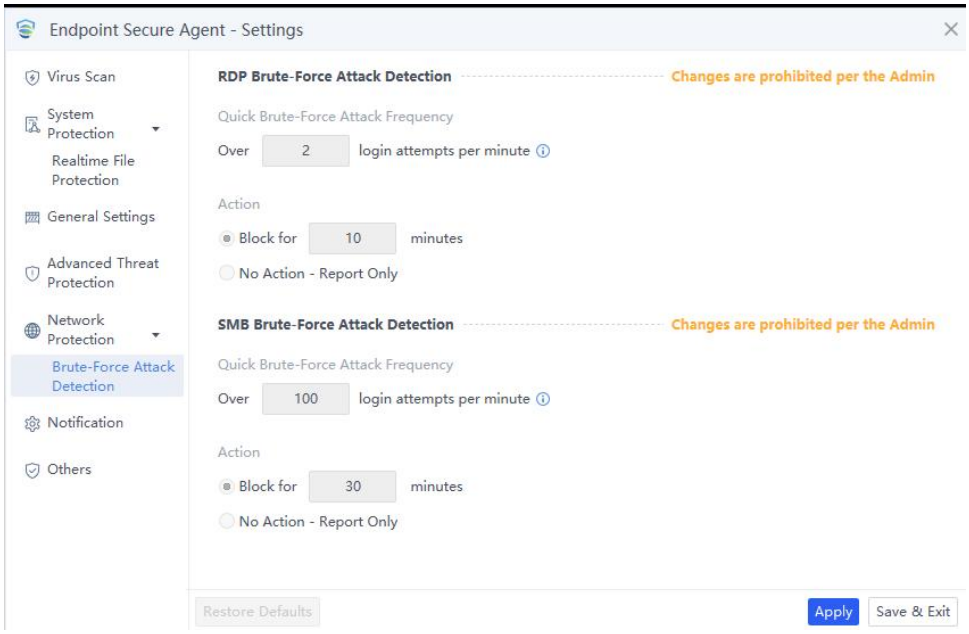
details, see Realtime Protection.



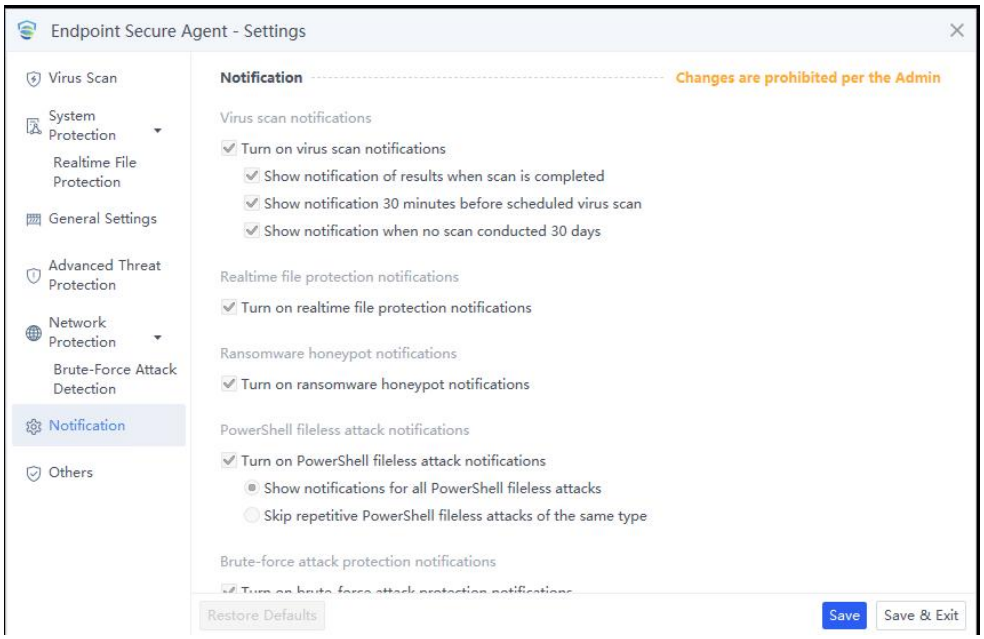

**General Settings:** It supports setting the backup policy and quarantine area size of the Windows endpoint or Linux endpoint. The parameter settings are the same as those in the **General Settings** area under **Endpoints** > **Security Protection** on the **NovaGuard Manager**.




**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 under **Endpoints** > **Security Protection** on the NovaGuard Manager. For details, see Realtime Protection.



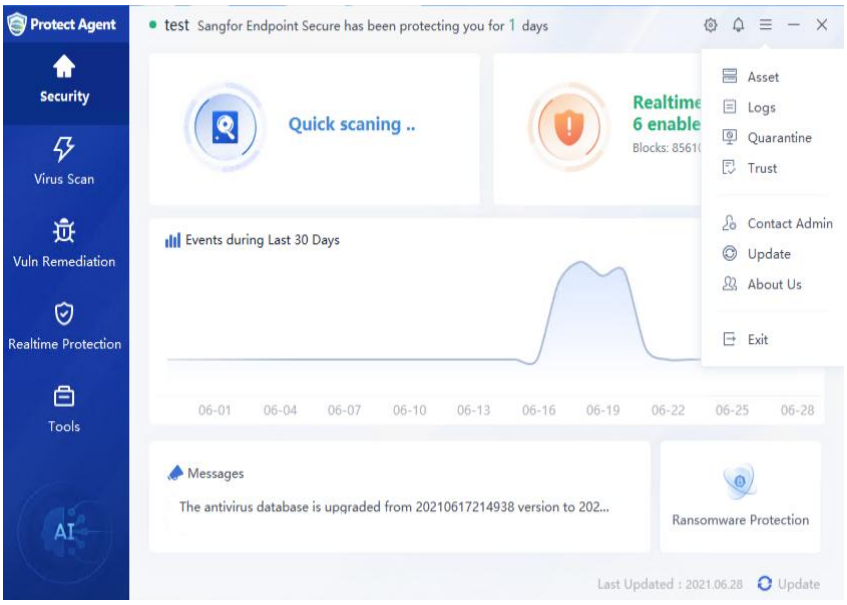

**Network Protection**: You can configure **RDP Brute-Force Attack Protection** and **SMB Brute-Force Attack Protection**. The parameter settings are the same as those in the **Brute-Force Attack Protection** area on the **Realtime Protection** tab under **Endpoints** > **Security Protection** on the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

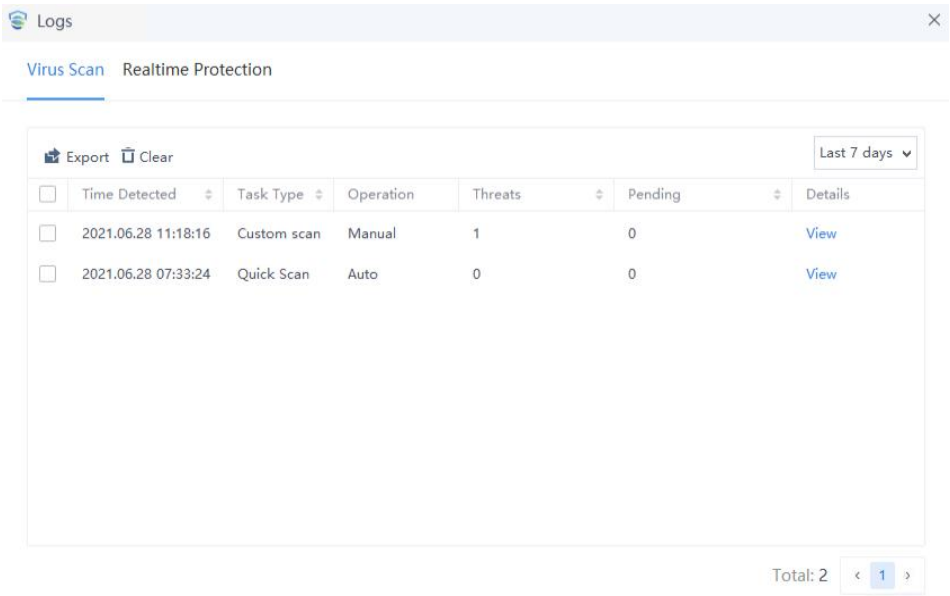



**Notification Settings**: You can configure the virus scan notification and alert notifications for real-time file protection, ransomware protection, and fileless attack protection. You can determine whether to enable a notification based on actual requirements. If the administrator has disabled notifications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

## 4.1.8 Security Logs

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

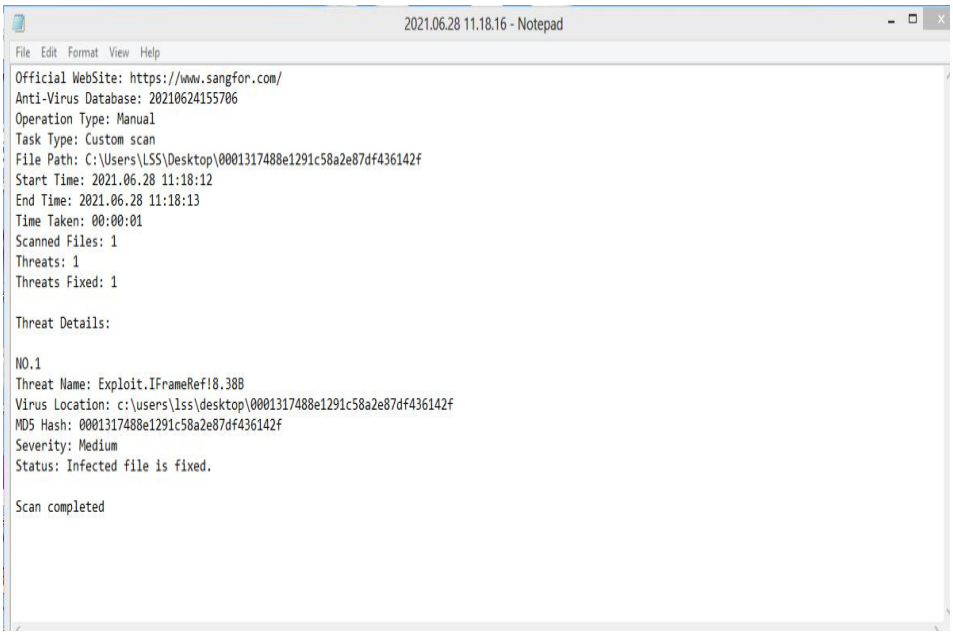



Security logs include **Realtime Protection** logs and **Virus Scan** logs.

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

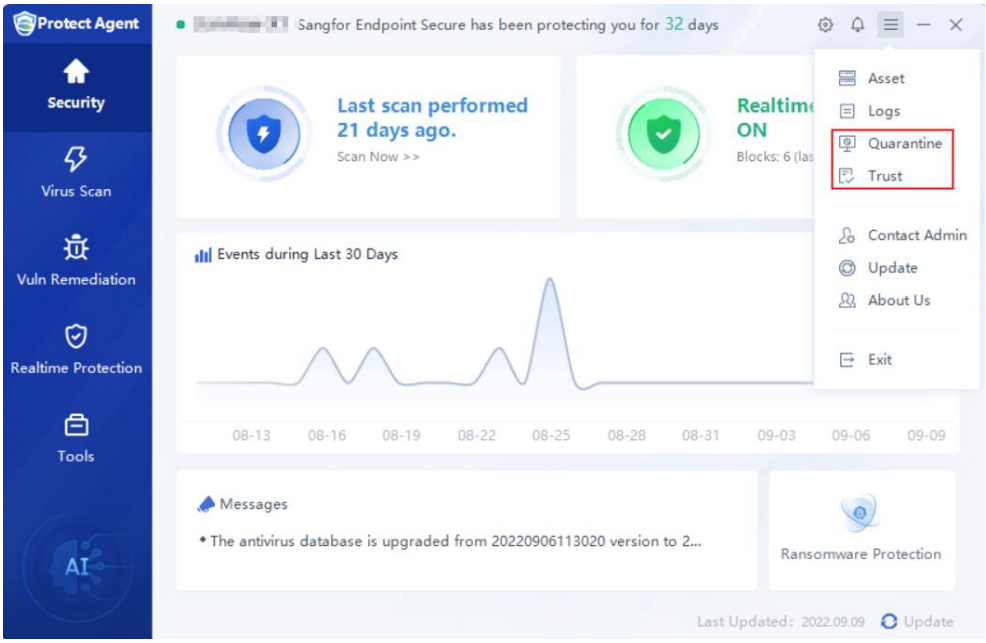
Virus Scan logs are operation logs about virus scans. You can click **Details** to view the virus scan details, as shown in the following figure.




## 4.1.9 Quarantine and Trust Zones

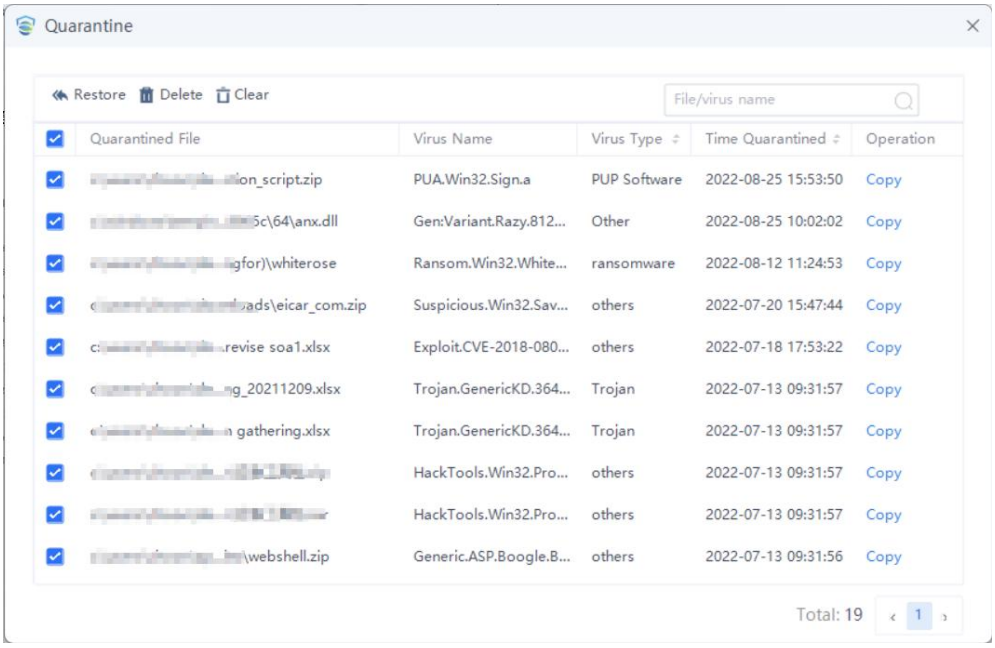
When NovaGuard detects malicious files for disposal, it will quarantine them and move them to the quarantine zone. While the files or processes are mistakenly reported, the user can add them to the trust zone, and the files in the trust zone will be automatically skipped by virus scanning or real-time file monitoring.

Click the icon at the top right corner of the agent page to open the **Quarantine** zone or **Trust** zone, as shown below.

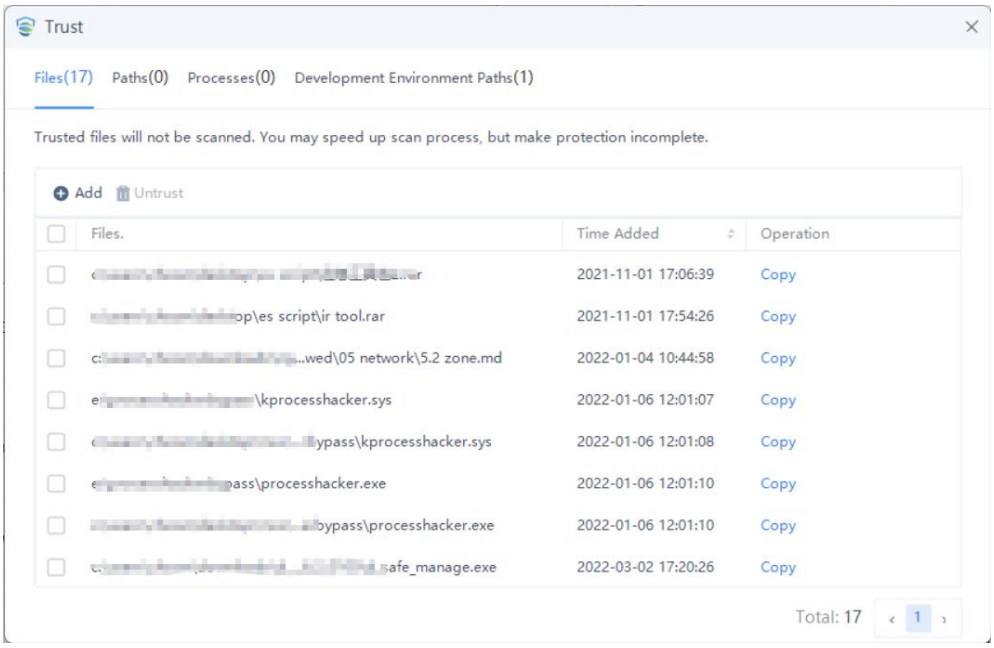



Click the **Quarantine**, and you can restore, delete or clear the files in the quarantine zone,

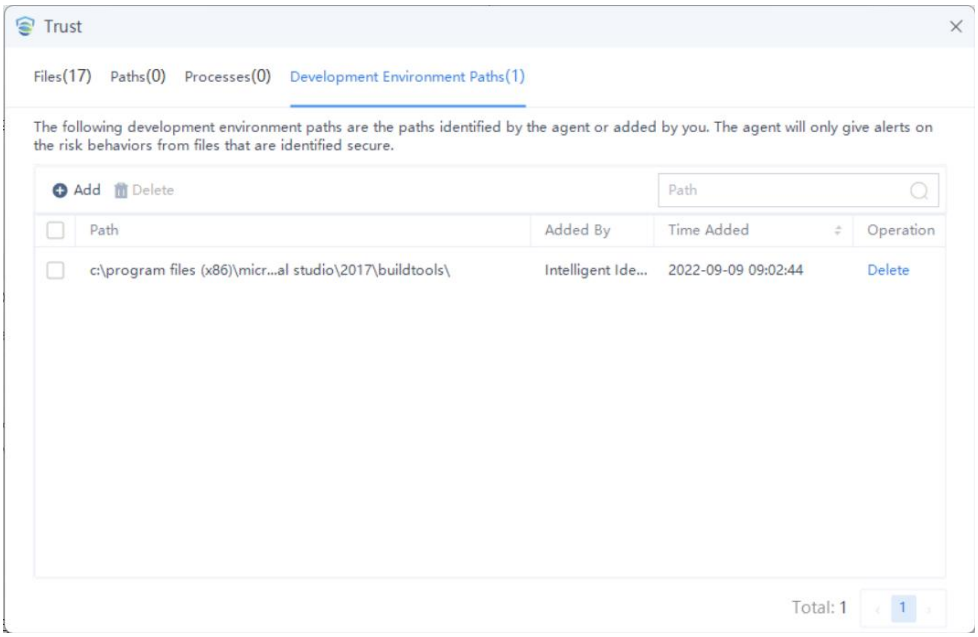
as shown below.



Click the **Trust**, and you can add **Files**, **Paths**, and **Processes** to the Trust zone, as shown below.

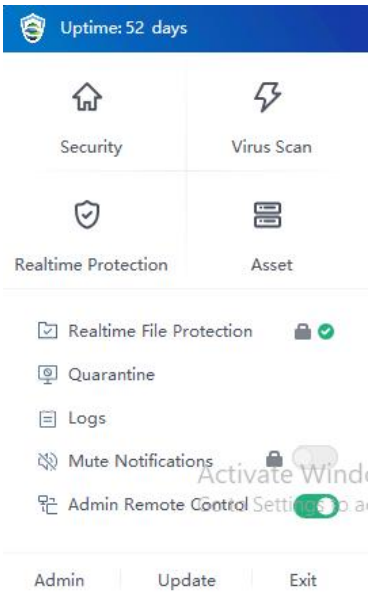



Enter the **Trust > Development Environment Paths**, and you can see the intelligently recognized development directories. In addition, you can also customize to add or delete development directories, as shown below.



## 4.1.10 System Tray

The NovaGuard 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.




**Uptime:X days**: shows how long NovaGuard has protected your computer.

**Shortcut: Security**, **Virus Scan**, **Realtime Protection**, **Asset**, **Realtime File Protection**, **Quarantine**, and **Logs.**

**Mute Notifications**: If it is enabled, NovaGuard will not alert when it detects malicious files. This function can be configured on the Agent or delivered by the administrator from the Manager.

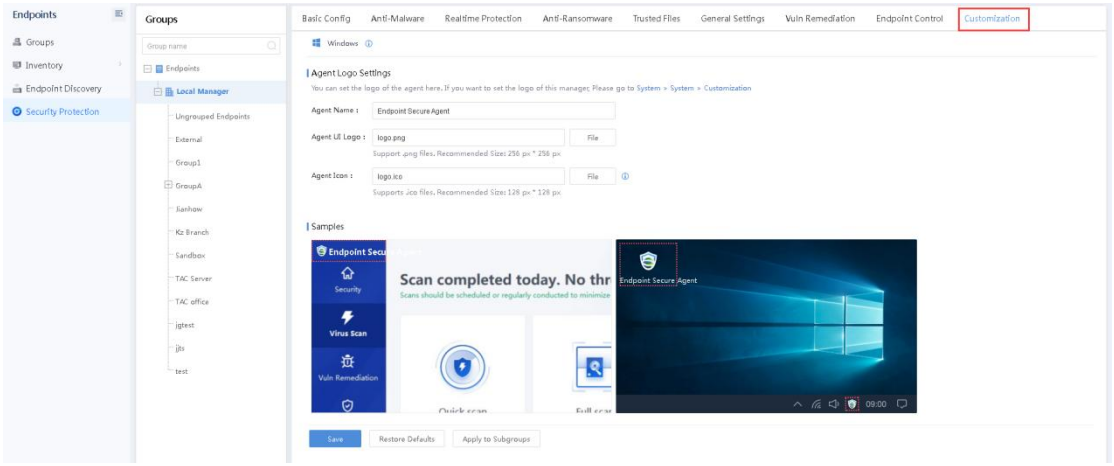
**Admin Remote Control**: This function is enabled by default, and Admin can remotely manage the terminal through the remote assistance function.

**Admin**: When you click **Admin**, the administrator information will be displayed, as shown below. You can contact the administrator if you encounter any issues using the NovaGuard Agent.



### 4.1.11 Customization

You can personalize the Agent logo and icon.

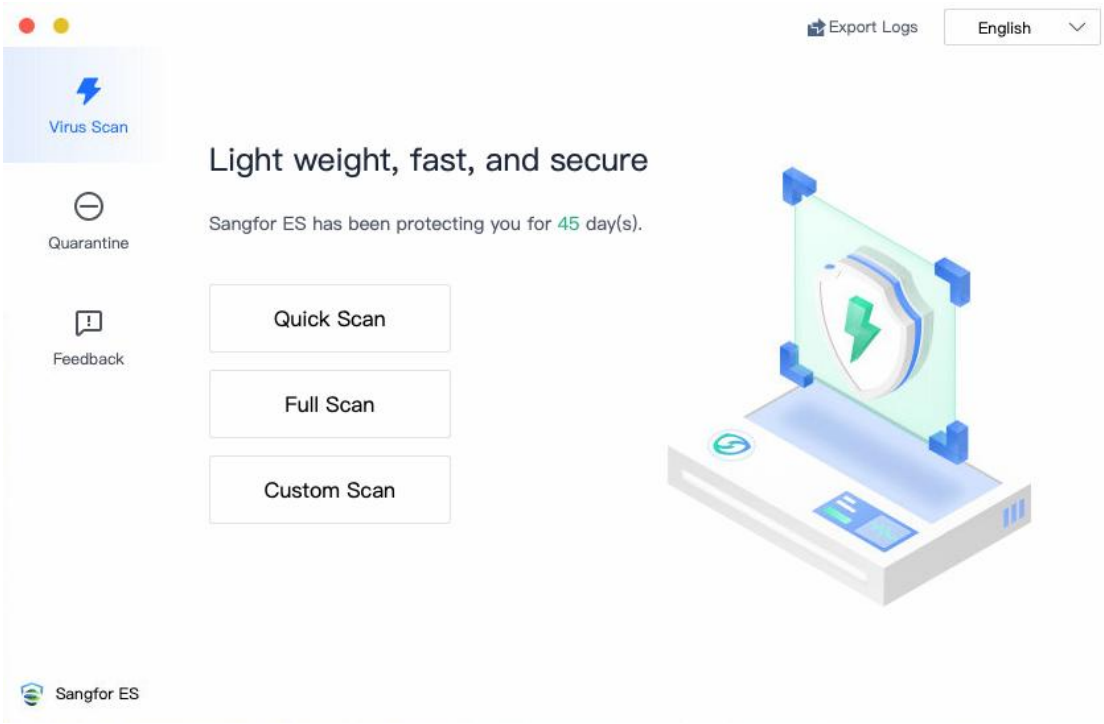



## 4.2 MAC Agent

Endpoint users can use the Agent to scan for viruses, export logs, and view the quarantined files.

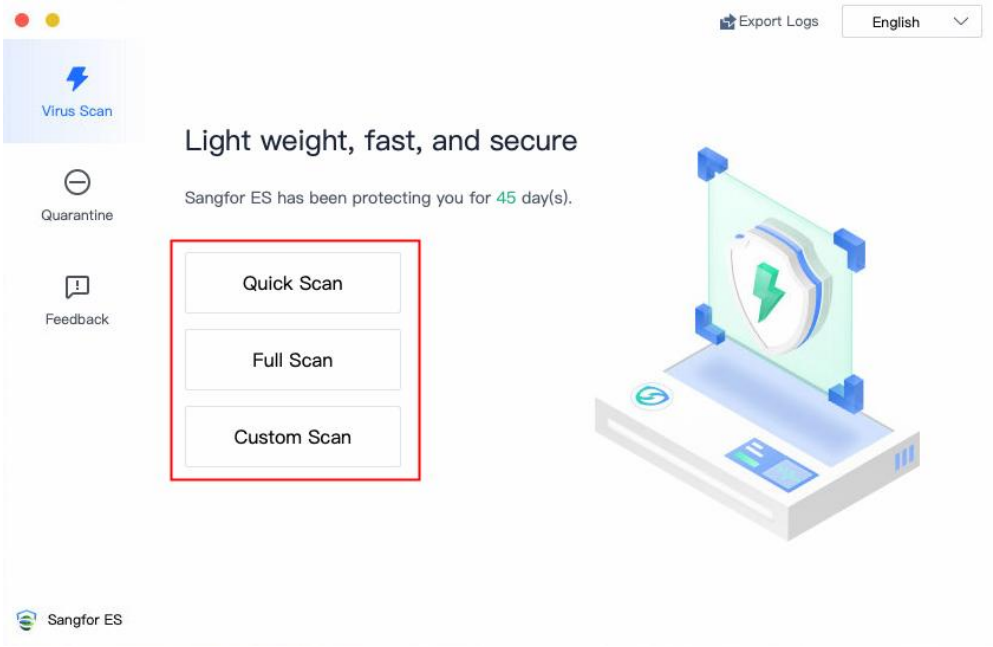
### 4.2.1 Main Page

After the Agent is deployed, you can view the endpoint protection durations and change the agent language shown in the following figure.




## 4.2.2 Virus Scan

On the **Virus Scan** page, you can perform a **Quick Scan, Full Scan**, or **Custom Scan** for the endpoint.




**Quick Scan**: Scan critical MAC system directories, for example, **/private/tmp , /tmp, /Users/Account used for login/Desktop, /Users/Account used for login/Documents** and

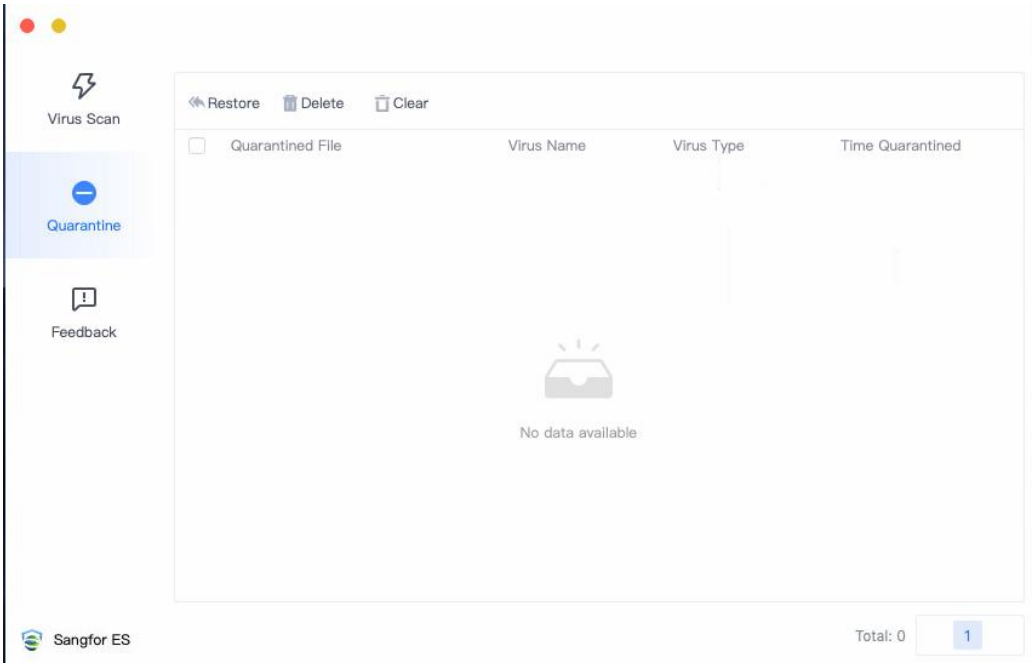
**/Users/Account used for login/Downloads**

**Full Scan**: Scan all MAC system directories.

**Custom Scan**: Scan specified files or directories.

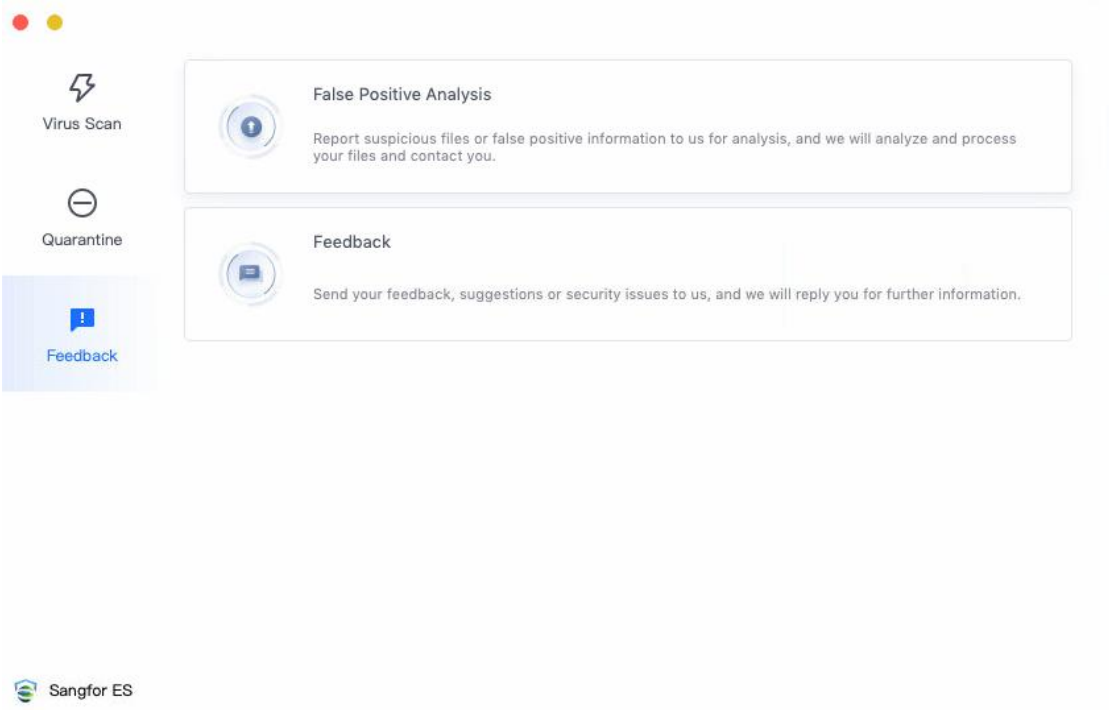
### 4.2.3 Quarantine

When NovaGuard isolates malicious files, the files are moved to the **Quarantine** area. You can **Restore**, **Delete**, and **Clear** isolated files on the **Quarantine** page with one click, as shown in the following figure.



## 4.2.4 Feedback

The **Feedback** page consists of the **False Positive Analysis** and **Feedback**.




**False Positive Analysis**: If you suspect that the NovaGuard agent detection results are false positive, you can report it through **False Positive Analysis** to the ForeNova security team for manual analysis.

**Feedback**: You may send feedback, suggestion, or security issues to the ForeNova team for product improvement.

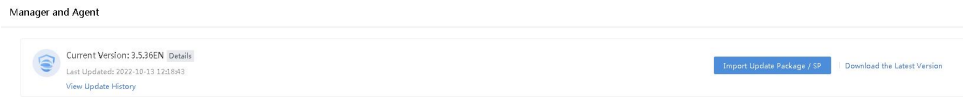
# 5 Product Update

NovaGuard 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.forenova.com/plugin.php?id=service:download, download the update package of the corresponding version, and verify the MD5 value.
2. Log in to the NovaGuard 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.

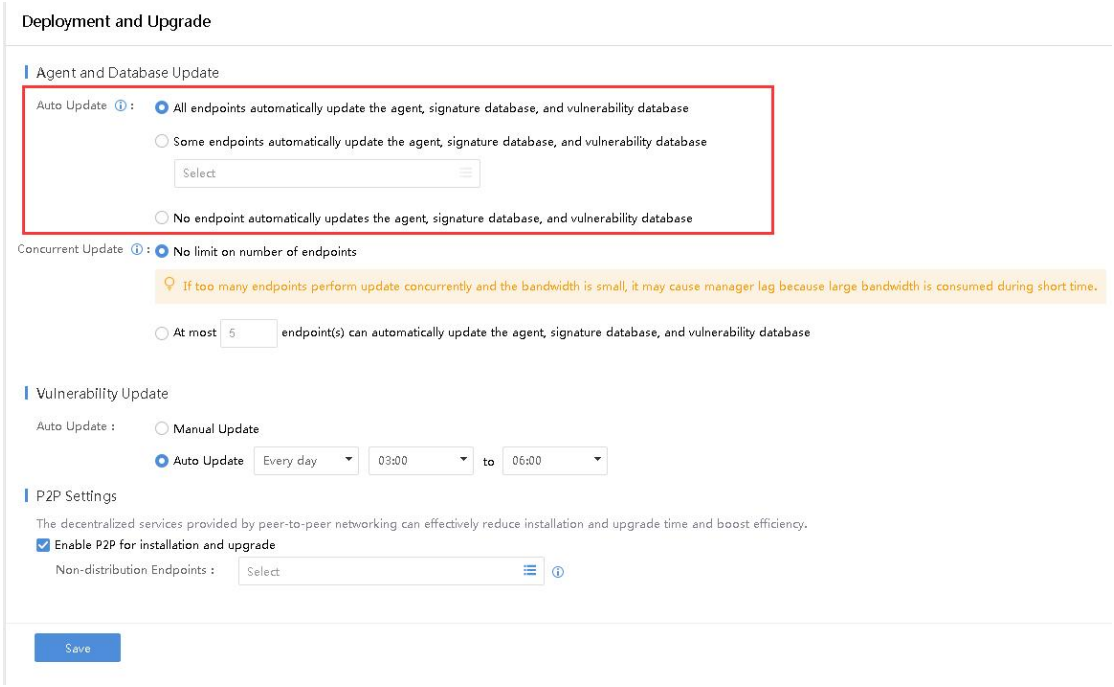
## 5.2 Agent Update

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 **System** > **System Updates > Manager and Agent > Agent Update**. To ensure stable and efficient Agent updates, you should use grayscale and staggered updates.

### 5.2.1 Auto 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.

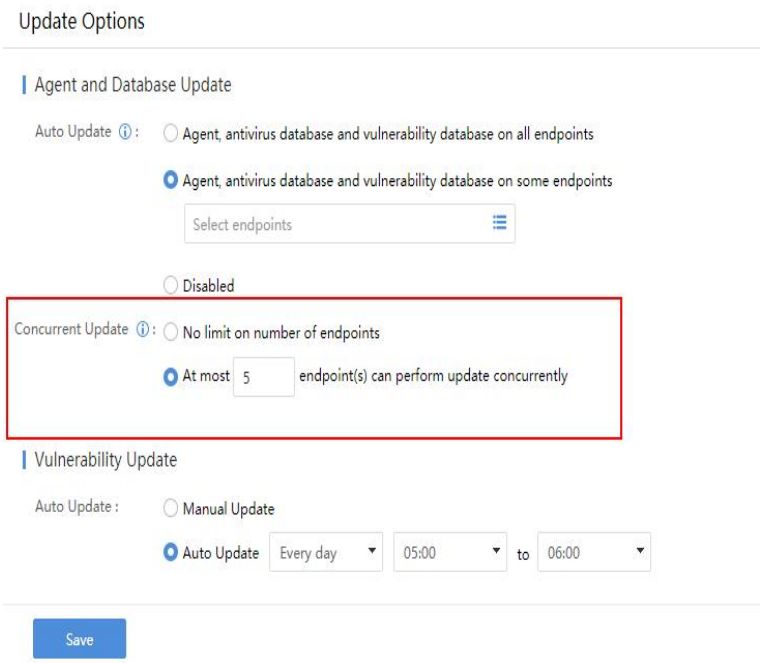
To configure Auto update, choose **System** > **System** > **Deployment and Upgrade**. Then, under **Auto Update,** select **All endpoints automatically update the agent, signature database, and vulnerability database**, as shown in the following figure.




## 5.2.2 Concurrent Update

To prevent network congestion caused by many Agents' updates, 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** > **Deployment and Upgrade**, 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

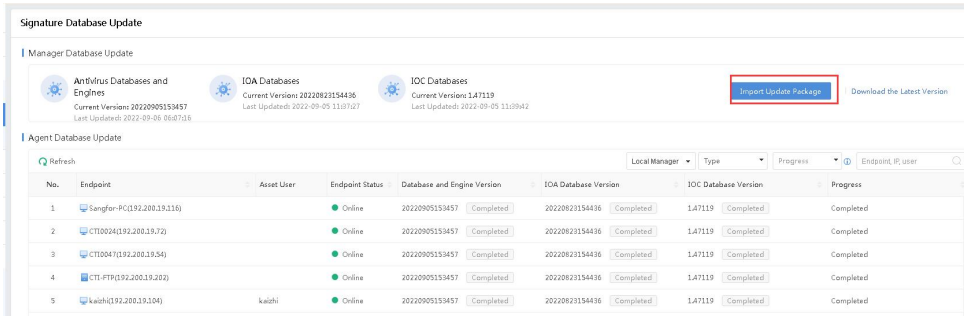
If the Manager is in an isolated network environment, it cannot access the Internet. Therefore, you need to use the manual offline update mode. The update procedure is as follows:

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

   To download the antivirus database, visit https://community.forenova.com and choose **Self-Service** > **Download** > **Endpoint** > **Anti-virus Database**.

2. Log in to the Manager, navigate to **System** > **System Updates** > **Signature Database Update**, 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.




## 5.3.3 IOA Databases and IOC Databases Update

The IOA and IOC databases can be updated in online and manual offline update modes.

**Online update:**

The antivirus database and engine are automatically updated online if the Manager can access the Internet.

**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 method. The update procedure is as follows:

1. Download the IOA database and verify the MD5 value.

IOA database can be downloaded from: https://community.forenova.com and choose **Self-Service** > **Download** > **Endpoint** > **IOA Database**.

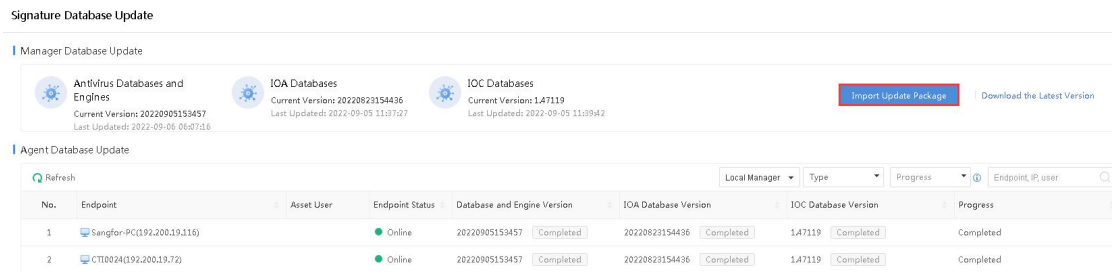
---

NOTE

IOA database is still not available in the ForeNova community currently. We will update the document and community when it is ready.

---

2. Log in to the NovaGuard platform, go to **System** > **System Updates** > **Signature Database Update** page, click **Import Update Package**, and select the database downloaded in step 1. After the IOA databases are successfully imported, the Agent will automatically update the IOA database, as shown below.




**NOTE**

The IOC database can only be updated online.

# 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.

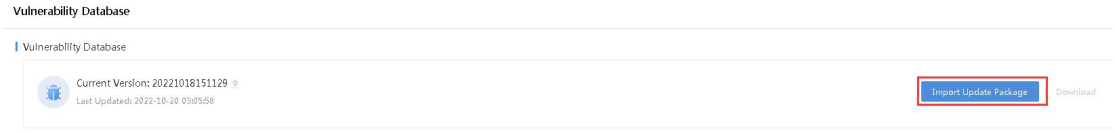
## 5.4.1 Automatic Online Update

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.forenova.com and choose **Self-Service** > **Download** > **Endpoint** > **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.


Vulnerability Database
Vulnerability Database
Current Version: 20221018151129
Last Updated: 2022-10-20 03:05:58
Import Update Package
Download

# 6 Maintenance

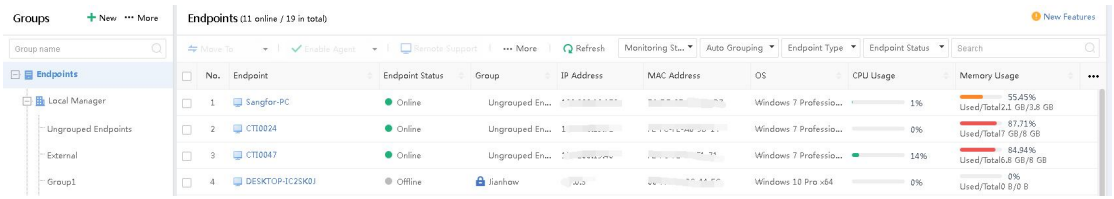
## 6.1 Endpoints

### 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 NovaGuard 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:

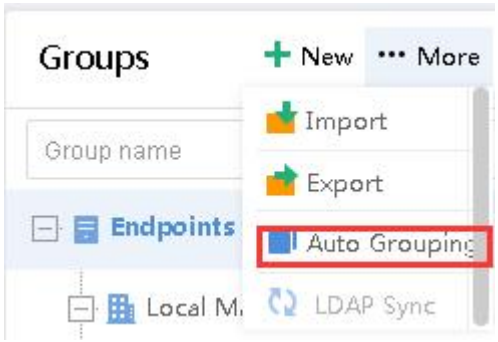
1. **Creating Groups by Organizational Structure**

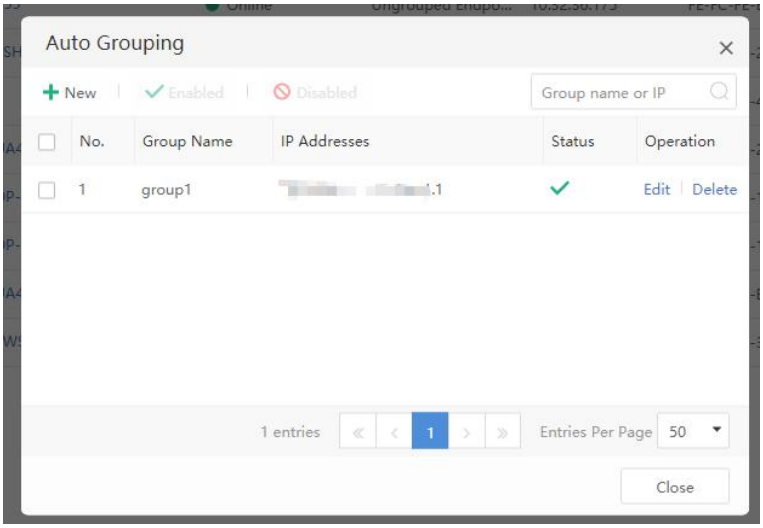
Choose **Endpoints** > **Groups** and create groups by organizational structure, as shown in the following figure.




2. **Grouping Endpoints by IP Addresses**

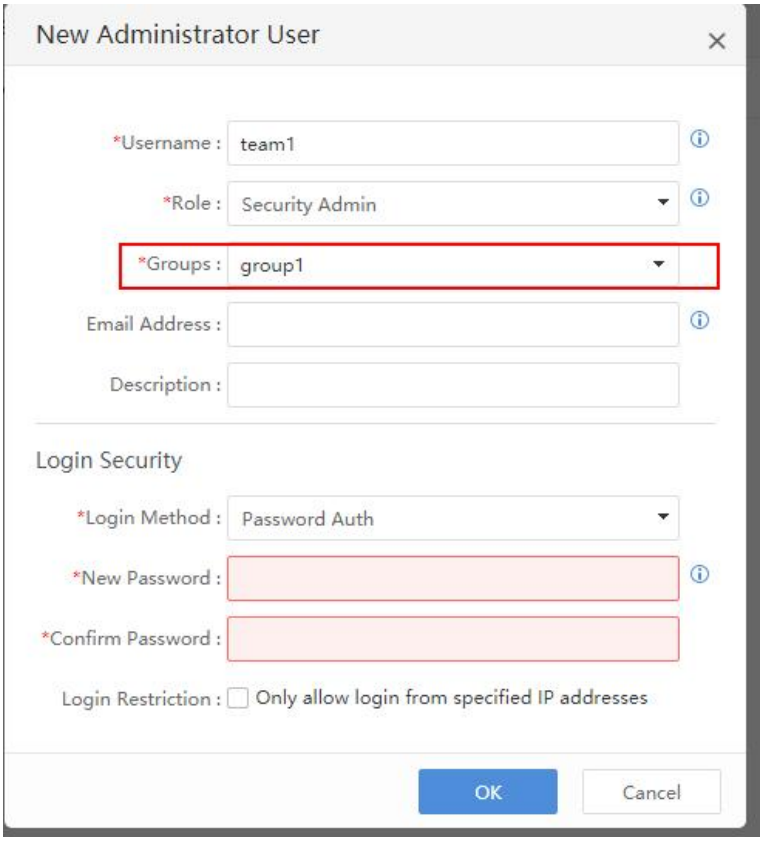
Choose **Endpoints** > **Groups**, click **More** and choose **Auto Grouping**, as shown in the following figure. Next, configure auto grouping of new endpoints by IP addresses.






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

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

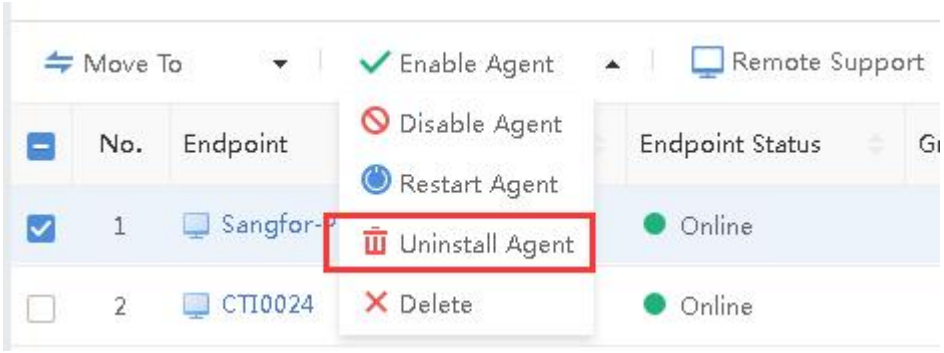



# 6.2 Licenses

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

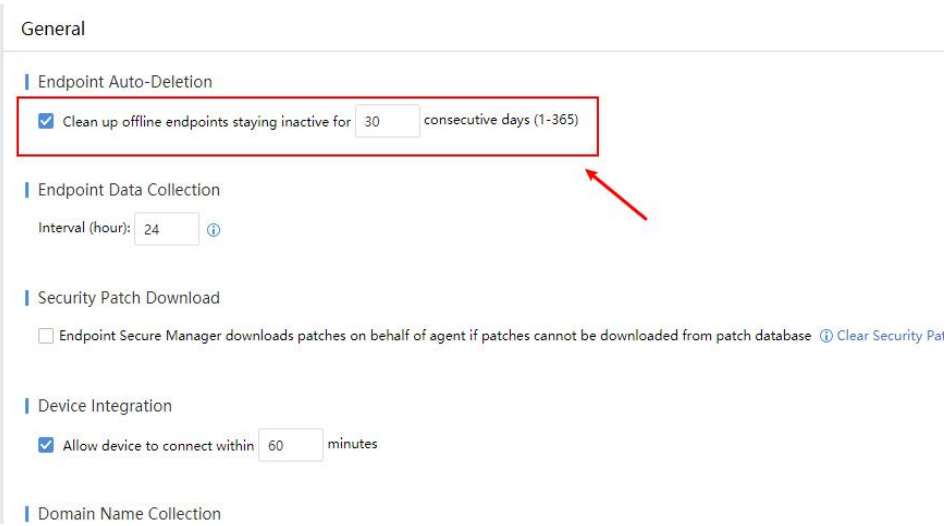
1. **Uninstall Agent Manually**

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




2. **Auto-Deletion**

Choose **System** > **System** > **General**, select **Endpoint Auto-Detection**, and set the duration to clean up the inactive endpoints, 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 checks, exit and uninstall password change, Manager account and password management, remote access protection password change, Manager login IP address restriction, endpoint security and integrity check, vulnerability scan, and policy optimization.

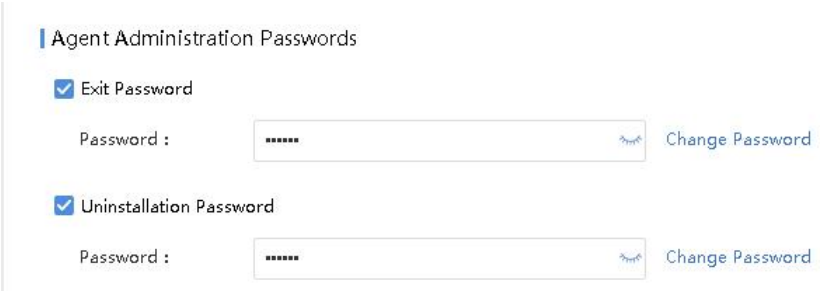
### 6.3.1 Version and Database Check

The administrator must check the product version and antivirus database version periodically. You are advised to use the latest product and antivirus database versions. For the latest product and antivirus database versions, visit http://community.forenova.com and choose **Self-Service > Download** > **Endpoint**.

### 6.3.2 Exit Password and Uninstallation Password

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

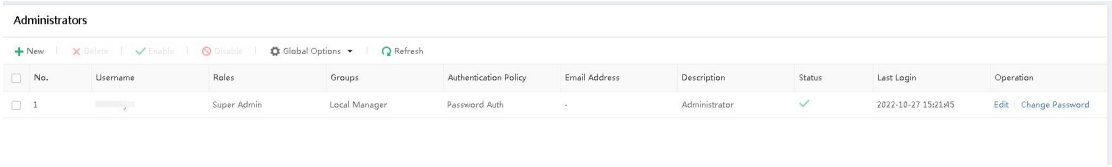
To change the exit password or uninstall password, choose **Endpoints** > **Security Protection** > **Basic Config** and set the exit password or uninstall password in the **Agent Administration Passwords** area, as shown in the following figure.



## 6.3.3 Manager Accounts and Passwords

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

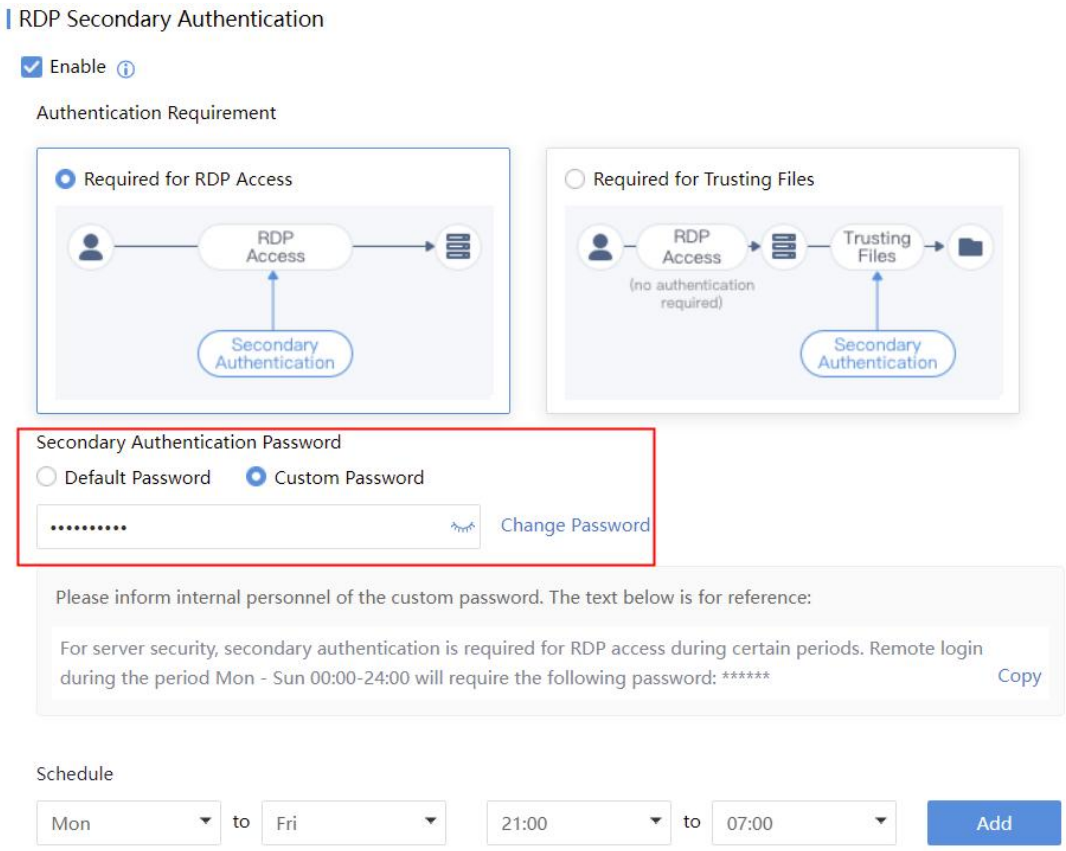
1. Check whether invalid Manager accounts exist. If yes, delete them.
2. Periodically change passwords of Manager accounts and ensure that strong passwords are used.




## 6.3.4 Remote Access Protection Password

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

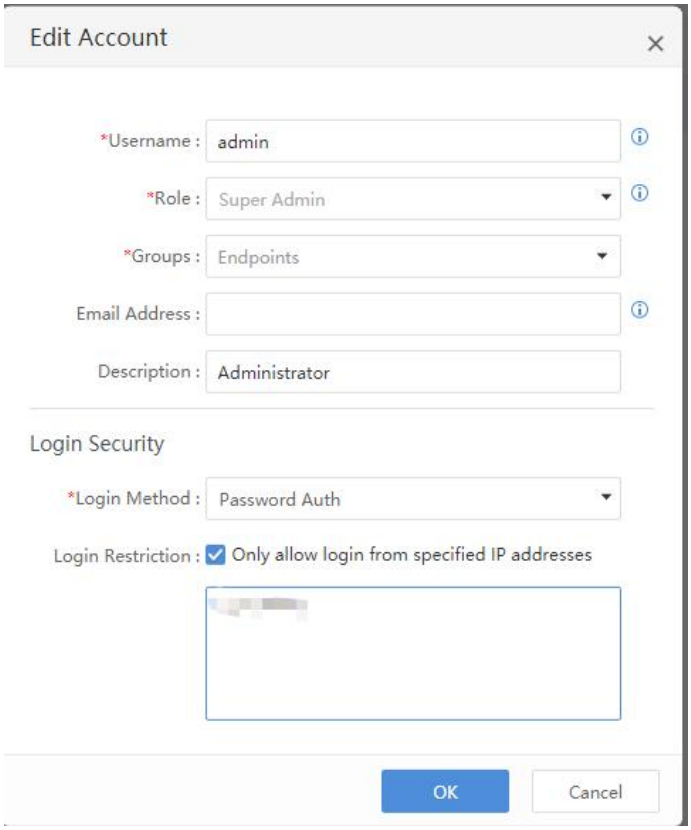
To change the remote access protection password, choose **Endpoints** > **Security Protection** > **Anti-Ransomware** and enter the password in the **Secondary Authentication Password** text box, as shown in the following figure.




## 6.3.5 Administrator Login IP Address Restriction

You are advised to restrict the IP addresses from which Administrator accounts can log in. Users can only log in to the Administrator accounts through a specified IP address.

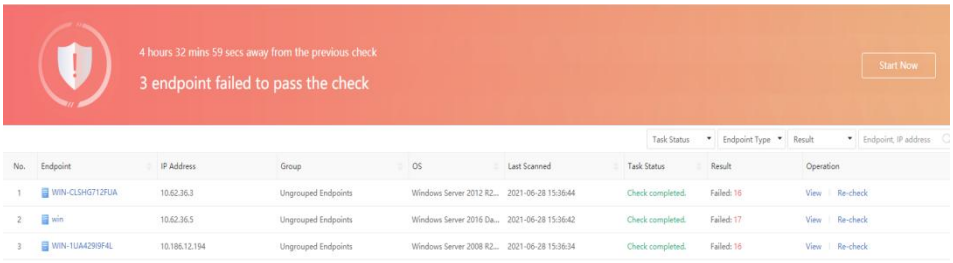
To restrict login IP addresses, choose **System** > **Administrators**, click **Edit** in the **Operation** column of an account, check the **Only allow login from specified IP addresses** checkbox, and enter the IP addresses, as shown in the following figure.




## 6.3.6 Security Compliance Check

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

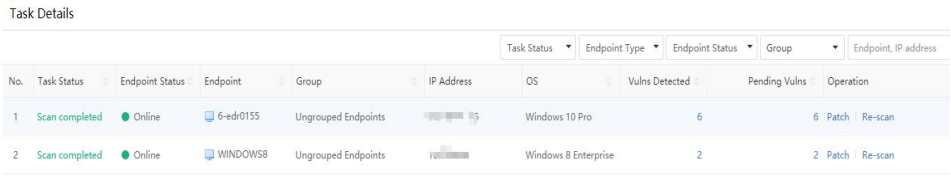
To perform **Security Compliance Check**, navigate to **Detection** > **Security Compliance**, as shown in the following figure.




## 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, navigate to **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 process protection | Enabled as needed | Configure it as needed. |
| Remote access protection | Enabled by default | Retain the default configuration. |
| Trusted files | Enabled as | Configure it as needed. |

| | | |
|---|---|---|
| | 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. |

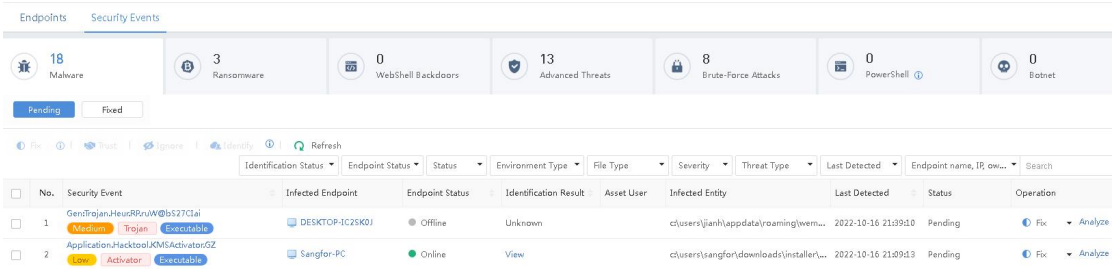
Table 9: Policy optimization

# 6.4 Security Event Handling

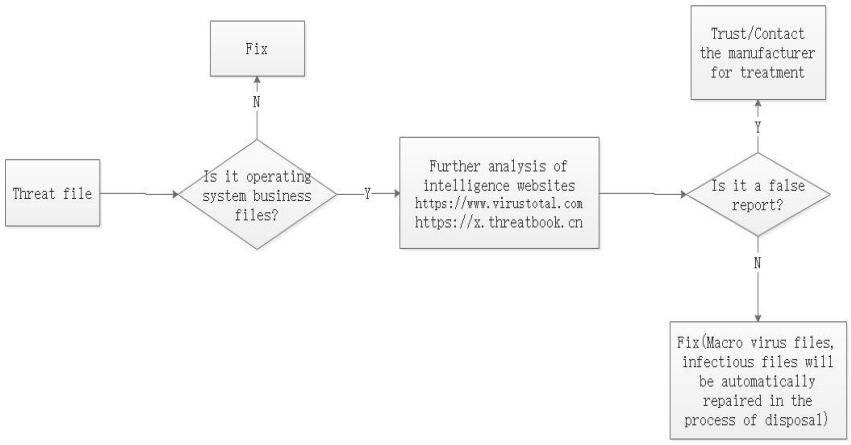
## 6.4.1 Rules

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.



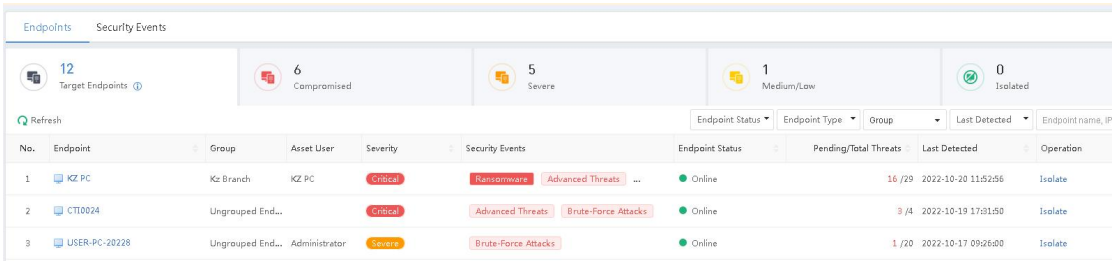

We must handle the security events in the following sequence: critical, severe, and medium or low endpoints.




## 6.4.2 Case

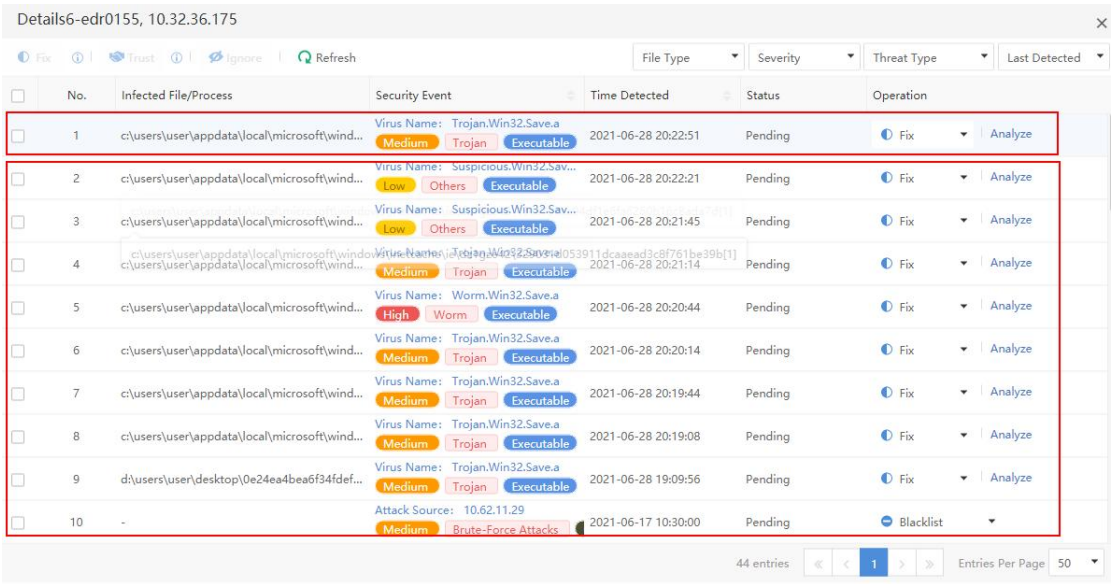
We will use a case to describe how to handle malicious files in this section.

Files that are not automatically isolated will be reported to the **Response** > **Threat Response** page, as shown in the following figure. We must handle the security events in the following sequence: critical, severe, and medium or low endpoints.



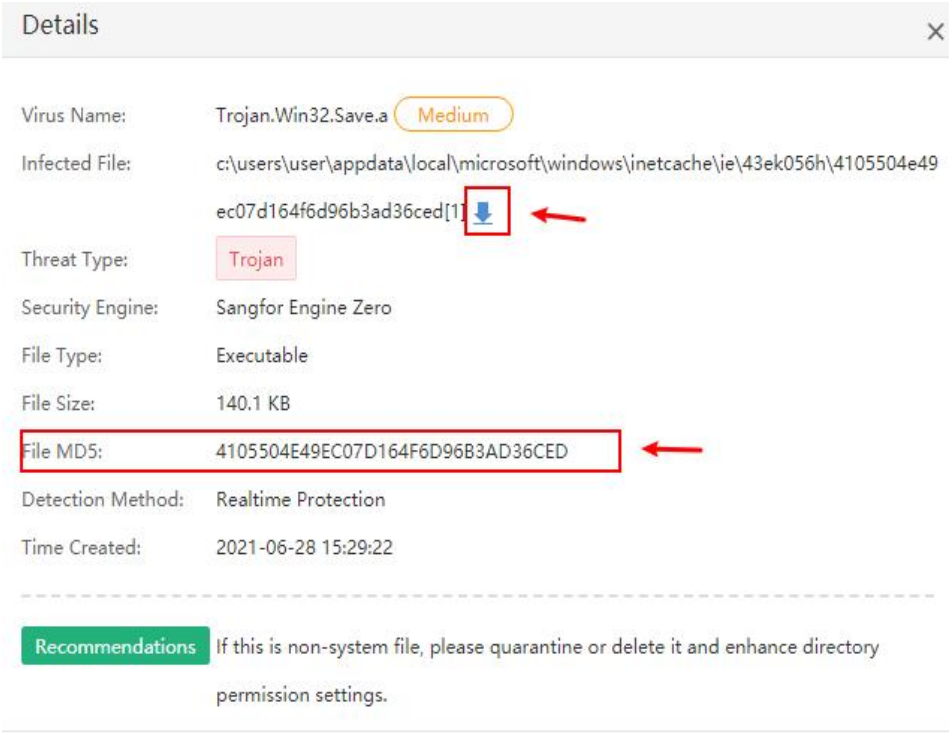

**Step 1.** Determine whether a malicious file is a business file.

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.



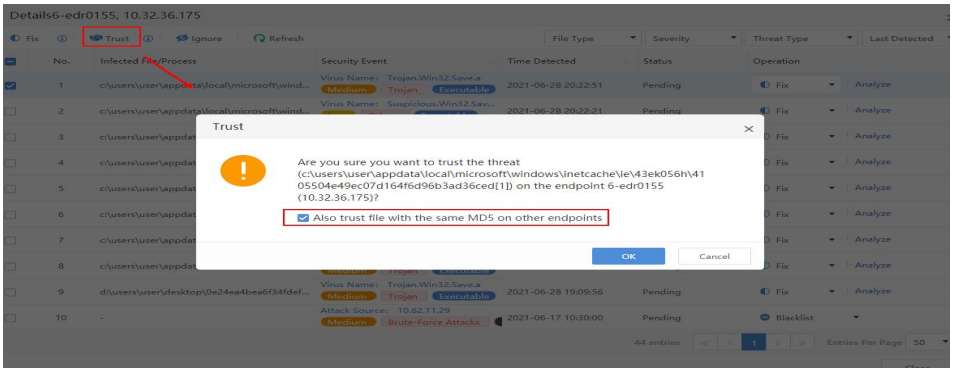

**Step 2.** Obtain the suspicious file for further analysis.

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.** Process the file based on the threat analysis result.

According to the analysis result of ThreatBook Cloud Sandbox, the file is secure and can be added as a trusted file.


Details6-edr0155, 10.32.36.175
Fix
Trust
Ignore
Refresh
File Type
Severity
Threat Type
Last Detected
No.
Infected File/Process
Security Event
Time Detected
Status
Operation
Trust
Are you sure you want to trust the threat (c:\users\user\appdata\local\microsoft\windows\inetcache\ie\43ek056h\4105504e49ec07d164f6d96b3ad36ced[1]) on the endpoint 6-edr0155 (10.32.36.175)?
Also trust file with the same MD5 on other endpoints
OK
Cancel

# 7 High-risk Operations

The following table describes high-risk operations that need to be avoided when using NovaGuard. 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 Protection | Realtime Protection | Set the action for detected malicious files in the **Realtime File Protection** area to **Enhanced**. | The customer's business files may be isolated due to false positives, resulting in business | High | Set the action for detected malicious files to **Standard**. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | exceptions. | | |
| 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 NovaGuard Manager and cannot access any other networks. If a server is isolated, services will be affected. | High | Choose **Response** > **Threat Response**, click **Isolated** on the **Endpoints** tab, and 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. Instead, restart a server |

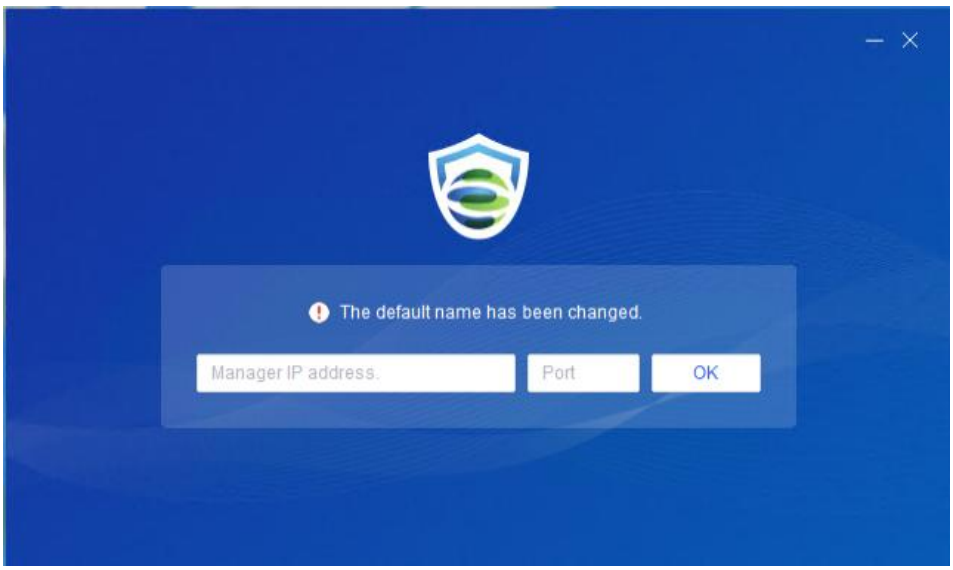
| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | manually at a specific time when services are not affected. |
| Endpoints | Security Protection | Server Protection | Enable server protection or critical directory protection but do not add service processes of the server to the trusted processes. | Key services of the server do not run, resulting in service interruption. | High | Add service processes of the server to trusted processes. |

Table 10: 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:**

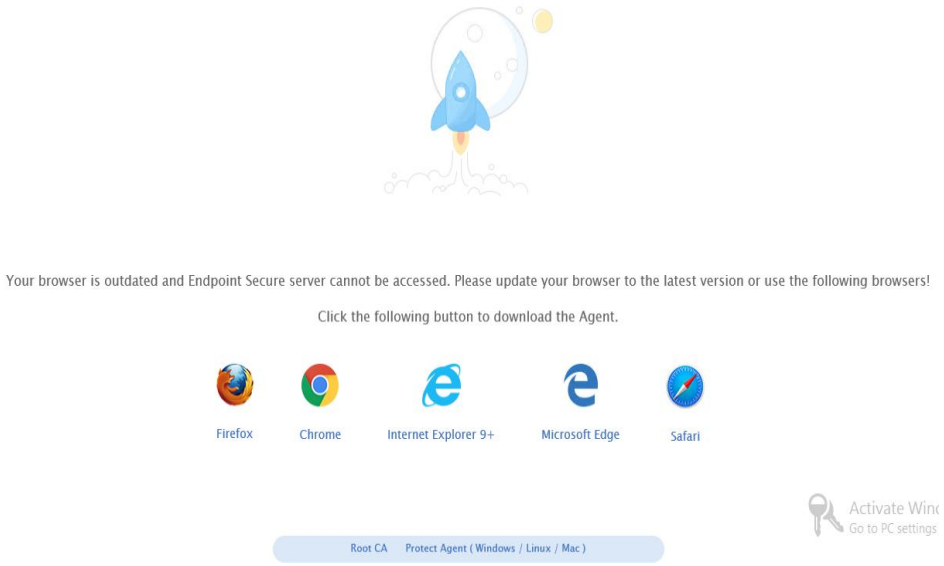
- The message is shown because the installer file name is modified. Enter the IP address of the NovaGuard Manager and port 443 in the dialog box to complete installation. Alternatively, download the installer without modifying the file name and use it to install the Manager.

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

**Solution:**

- Uninstall other security software on the computer and install the NovaGuard Agent.

3. What can I do if I fail to log in to the NovaGuard 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 NovaGuard Manager.

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

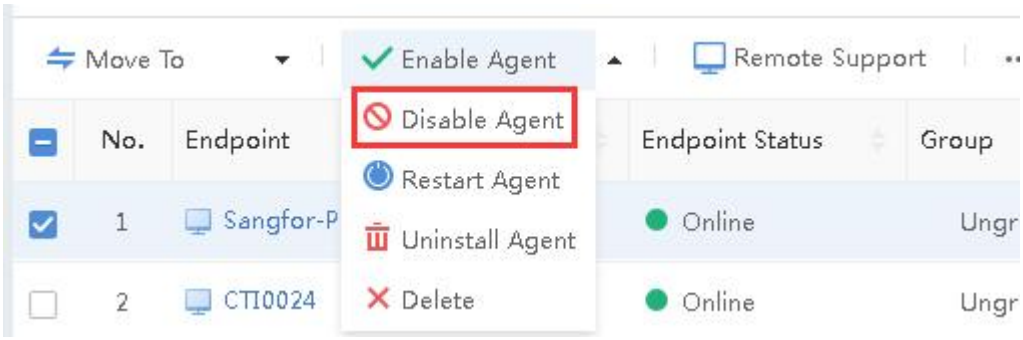
**Solution:**

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

5. What can I do if the computer is abnormal after installing the NovaGuard Agent?

**Solution:**

- Log in to the NovaGuard Manager, choose **Endpoints** > **Groups**, and 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.



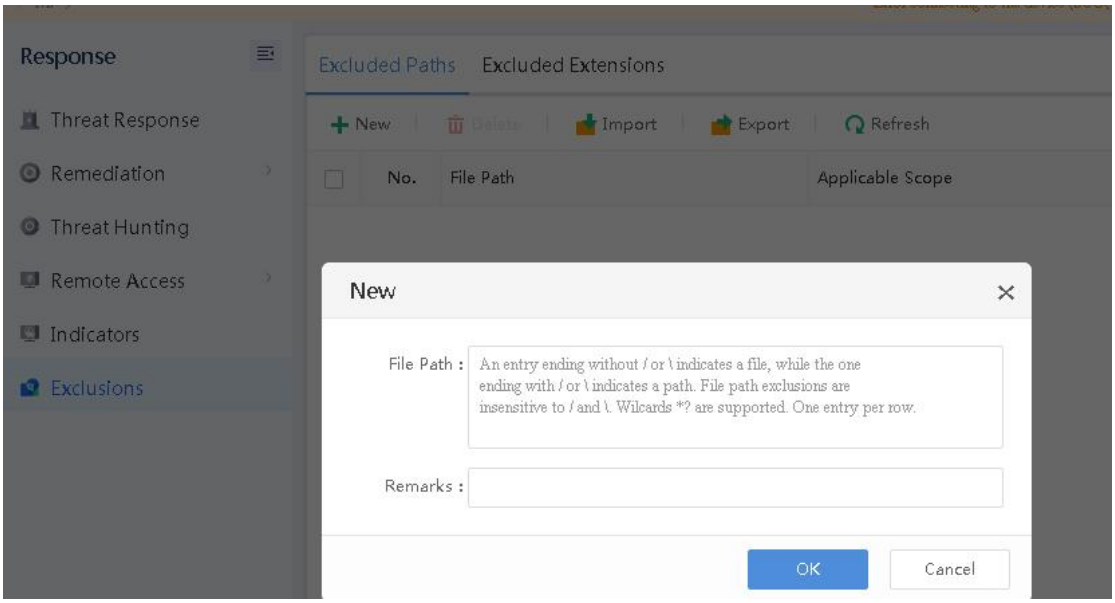

## 8.2 Anti-Malware

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

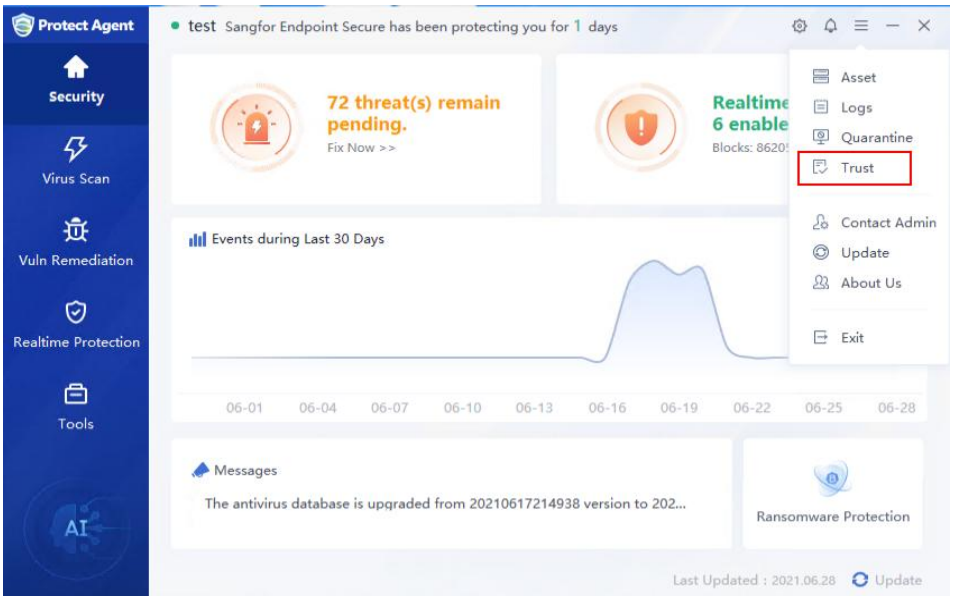
**Solution:**

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

- On the NovaGuard Manager, choose **Response** > **Exclusions** > **Excluded Paths**, click **New**, and select the business file, as shown in the following figure.




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




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

**Solution:**

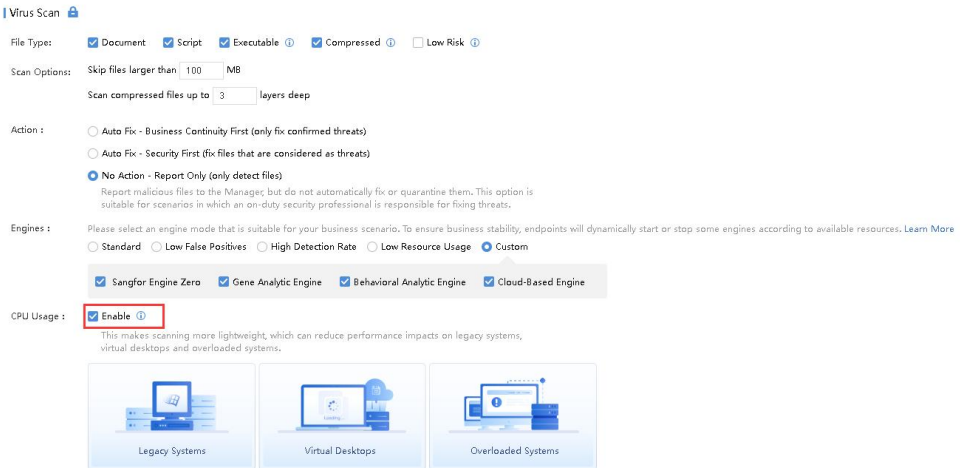
- NovaGuard supports virus scans for files in USB flash drives but not in network sharing paths.

3. What can I do if the CPU usage on a low-performance computer is high when

NovaGuard delivers an anti-malware task?

**Solution:**

- On the NovaGuard 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\sf\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 NovaGuard Manager or Agent.

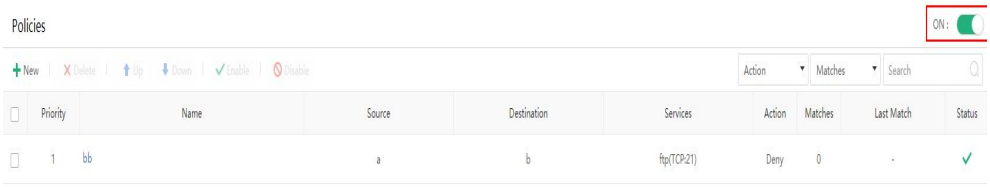
## 8.3 Micro-Segmentation

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



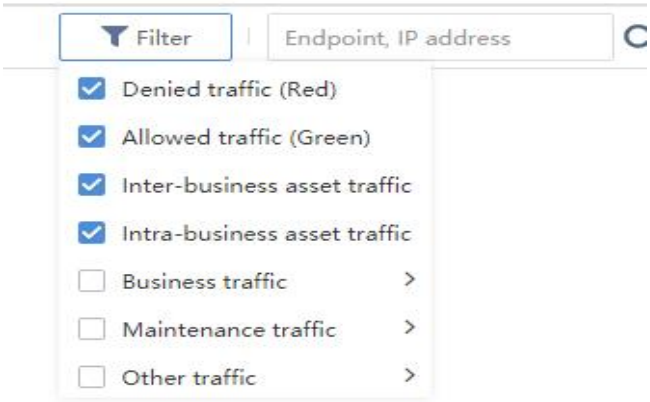

2. What can I do if micro-segmentation traffic statistics are not displayed?

**Solution:**

- Troubleshoot the fault as follows. If the fault persists, contact the service provider for processing.
- Log in to the NovaGuard Manager, choose **Micro-Segmentation** > **Other**, and check whether **Report traffic statistics** is enabled, as shown in the following figure.




- Log in to the NovaGuard 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 NovaGuard Manager, restoring the login password of the NovaGuard Manager, and migrating the

NovaGuard Manager to another server, contact the service provider for processing.

# 9 Acronyms and Abbreviations

| | **English Full Name** |
|---|---|
| CVE | Common Vulnerabilities & Exposures |
| CCom | Cyber Command |
| MDR | Manage Detection and Response |

