ForeNova NovaGuard

User Manual

Product Version	6.0.4R4
Document Version	02
Released on	Jul. 28, 2025



Copyright © ForeNova Technologies Inc. 2025. 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

Send information about errors or any product related problem to:

support@forenova.com

About This Document

This document describes the User Manual of NovaGuard.

Intended Audience

This document is intended for:

- All users

Note Icons

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. NOTICE addresses practices not related to personal injury.
	Calls attention to important information, best practices, and tips. NOTE addresses information not related to personal injury or equipment damage.

Change Log

Date	Change Description
Mar. 20, 2025	This is the first release of this document.

Contents

Technical Support 1
Change Log 2
1 Product Introduction 9
1.1 Product Overview 9
1.2 Key Features 10
2 Installation and Deployment 11
2.1 NovaGuard Manager Deployment 11
2.1.1 Software Deployment 11
2.1.1.1 Installation Package Download 12
2.1.1.2 OVA Image-Based Deployment 13
2.1.1.3 ISO Image-Based Deployment 16
2.1.1.4 Script-Based Deployment 18
2.1.2 Cascade Deployment 24
2.2 Product Activation 34
2.2.1 On-Premises NovaGuard Activation 34
2.2.2 Saas NovaGuard Activation 34
2.3 NovaGuard Agent Deployment 35
2.3.1 P2P Deployment 35
2.3.1.1 Feature Description 35
2.3.1.2 Scenarios 36
2.3.2 Deployment on Windows 40
2.3.2.1 Manual Installation 40
2.3.2.2 Silent Installation 45
2.3.2.3 Redirection to the Agent Installer Download Page 47
2.3.2.4 Installation via an AD Domain 49
2.3.2.5 Installation via Desktop Management Software 60
2.3.2.6 Installation on Virtual Machines 61
2.3.3 Deployment on Linux 64
2.3.3.1 Installation via the Command Line 64
2.3.3.2 Manual Installation 65
2.3.3.3 Redirection to the Agent Installer Download Page 66
2.3.3.4 Installation via the Linux Bulk Deployment Tool 67
2.3.3.5 Installation on Virtual Machines 70
2.3.4 Deployment on macOS 74
2.3.4.1 Installation on Physical Machines 74
2.3.4.2 Redirection to the Agent Installer Download Page 76
2.3.5 Pre-installation 77

2.3.6 Verification of Installation 78
2.3.7 Uninstallation of Incompatible Third-Party Antivirus Software 79
2.4 NovaGuard Agent Uninstallation 80
2.4.1 Uninstall from a Windows Endpoint 80
2.4.2 Uninstall from a Linux Endpoint 82
2.4.3 Uninstallation on NovaGuard Manager 83
2.5 Environments 84
2.5.1 NovaGuard manager Installation Environment 85
2.5.2 NovaGuard agent Installation Environment 85
2.5.3 Network Connectivity Requirements 86
File Whitelist Setting 86
3 Product Upgrade 87
3.1 Upgrade to a New Version 88
3.1.1 Import an Upgrade Package 88
3.2 Update Service Packs 91
3.3 Update the Signature Databases 93
3.3.1 Update the Antivirus Database 93
3.3.2 Update the IOA or IOC Database 94
3.3.3 Offline update Signature Database 94
3.4 Update the Vulnerability Database 95
4 Getting Started 95
4.1 Login Page of NovaGuard manager 95
4.2 Detection and Response 96
4.2.1 Security Events 97
4.2.1.1 Overview 97
4.2.1.2 WebShell 97
4.2.1.3 Memory Backdoors 99
4.2.1.4 Brute-Force Attacks 101
4.2.1.5 Suspicious Logins 103
4.2.1.6 Suspicious Scans 105
4.2.1.7 Advanced Threats 107
4.2.1.8 Reverse Shells 116
4.2.1.9 Remote Command Execution 117
4.2.1.10 Local Privilege Escalation 119
4.2.1.11 PowerShell Execution 120
4.2.2 Target Endpoints 121
4.2.3 Threat Hunting 123
4.2.3.1 Search with a Single Condition 123
4.2.3.2 Search with Group Conditions 125

4.2.4 Response 130
4.2.4.1 Endpoint Isolation 130
4.2.4.2 File Quarantine 132
4.2.4.3 Access Blocking 132
4.2.4.4 Process Killing 132
4.2.4.5 Domain Blocking 132
4.2.4.6 Coordinated Response 133
4.2.4.6.1 Lateral Movement Containment 133
4.2.4.6.2 Behavioral Containment 134
4.2.4.6.3 Threat Remediation 134
4.3 Risk Assessment 135
4.3.1 Windows Update 135
4.3.1.1 Patching 135
4.3.1.1.1 Assets 135
4.3.1.1.2 Patches 137
4.3.1.2 Scan Tasks 138
4.3.2 Vulnerabilities 140
4.3.2.1 Vuln List 140
4.3.2.1.1 Vulns 140
4.3.2.1.2 Scan Tasks 142
4.3.3 Compliance Checks 143
4.3.3.1 Tasks 143
4.4 Defense 145
4.4.1 Malware Scan 145
4.4.1.1 Malware 146
4.4.1.1.1 Virus-Infected Files 146
4.4.1.1.2 Ransomware and Threats 150
4.4.1.2 Tasks 151
4.5 Endpoints 155
4.5.1 Endpoint Groups 155
4.5.1.1 Create Groups 155
4.5.1.2 Import Groups 157
4.5.1.3 LDAP Sync 158
4.5.1.4 Allow Users to Assign Groups 163
4.5.1.5 Manage Endpoints 166
4.5.1.6 Batch operation of terminals 177
4.5.2 Endpoint Inventory 178
4.5.2.1 Listening Ports 179
4.5.2.2 Processes 181

4.5.2.3 Software 181
4.5.2.4 Database Apps 183
4.5.2.5 Middleware 183
4.5.2.6 Web Apps 184
4.5.2.7 Websites 184
4.5.2.8 Web Services 185
4.5.2.9 Web Frameworks 185
4.5.2.10 System Installation Packages 186
4.5.2.11 JAR Files 187
4.5.2.12 Python Packages 187
4.5.2.13 NPM Packages 188
4.5.2.14 OS 188
4.5.2.15 Users 190
4.5.2.16 Environment Variables 191
4.5.2.17 Kernel Modules 192
4.5.2.18 Services 192
4.5.2.19 Startup Items 193
4.5.2.20 Scheduled Tasks 193
4.5.2.21 Sharing 194
4.5.2.22 Registry 194
4.5.2.23 Connections 195
4.5.2.24 Trusted Certificates 195
4.5.2.25 Trusted Root CA 196
4.5.3 Endpoint Discovery 198
4.5.3.1 Unmanaged Endpoints 198
4.5.4 Integrity Monitoring 199
4.5.4.1 Hardware Changes 199
4.6 Policies 200
4.6.1 General Policies 200
4.6.1.1 Basic Config 201
4.6.1.2 Anti-Malware 206
4.6.1.3 Realtime Protection 211
4.6.1.4 Anti-Ransomware 219
4.6.1.4.1 Scenario 1: Protect the System 227
4.6.1.4.2 Scenario 2: Protect the Specified Directories 230
4.6.1.5 Trust List 231
4.6.1.6 General Settings 232
4.6.1.7 Vuln Remediation 238
4.6.1.8 Endpoint Control 242

4.6.1.9 Customization 254
4.6.2 Detection Policies 256
4.6.2.1 File Hashes 256
4.6.2.2 WebShell Directories 256
4.6.3 Exclusions 257
4.6.3.1 Excluded Extensions 257
4.6.3.2 Excluded Paths 258
4.6.3.3 Excluded IOAs 258
4.6.3.4 Event Whitelists 259
4.6.4 Behavior Control 260
4.6.4.1 Watermark 260
4.6.5 App Control 260
4.6.5.1 Application Blacklists 261
4.6.5.2 Application Signature Database 262
4.6.5.3 Metering Policies 264
4.6.5.4 Software Uninstallation 266
4.7 System 268
4.7.1 Agent Deployment 268
4.7.1.1 Agent Download 268
4.7.2 System Updates 268
4.7.3 Integrated Devices 269
4.7.3.1 Traffic Forwarding 270
4.7.4 Branches 272
4.7.5 Administrators 272
4.7.5.1 Administrator Roles 272
4.7.5.2 Manager Login Authentication 273
4.7.5.3 Login Restriction Based on IP Addresses 276
4.7.6 Licensing 276
4.7.6.1 License Types 276
4.7.7 Logs 279
4.7.7.1 Security log 279
4.7.7.2 Coordinated Action 280
4.7.7.3 Operations Logs 280
4.7.7.4 Control Logs 281
4.7.7.5 Admin Logs 281
4.7.7.6 Reports 281
4.7.8 Data Sync 283
4.7.8.1 Syslog Reporting 283
4.7.8.2 Kafka Reporting 283

4.7.9 System 284
4.7.9.1 General 284
4.7.9.2 Data Backup 289
4.7.9.3 Network 290
4.7.9.4 Logging Options 295
4.7.9.5 Deployment and Upgrade 296
4.7.9.6 Alert Options 298
4.7.9.7 LDAP Sync 300
4.7.9.8 Customization 300
4.7.9.9 Tools 301
4.7.10 Troubleshooting 304
4.7.10.1 Upload Script File 304
4.7.10.2 Troubleshooting Logs 305
4.7.10.3 Agent FAQ 305
5 High-Risk Operations 305
6 FAQs 310
6.1 Installation and Deployment 310
6.2 Virus Scanning 312

1 Product Introduction

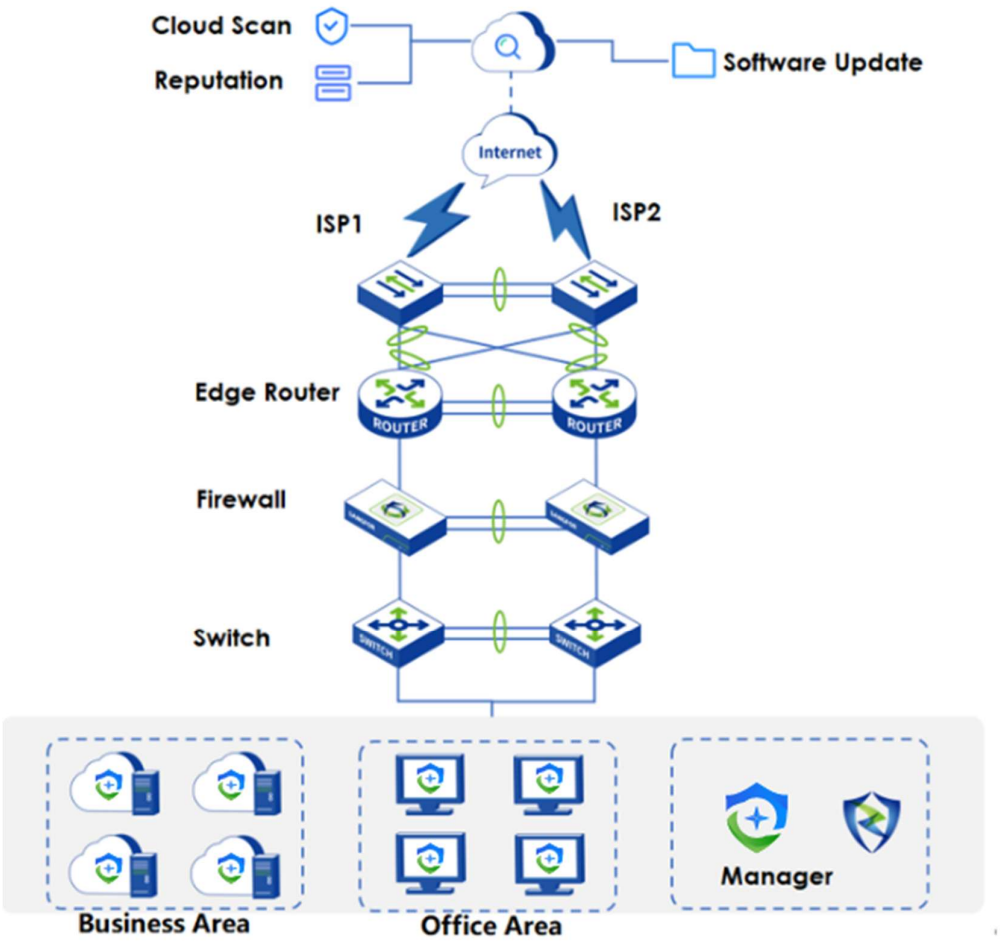
ForeNova NovaGuard consists of the **NovaGuard manager** and the **NovaGuard agent**.

The NovaGuard manager supports unified endpoint asset management, security, and compliance checks. It collects endpoint behavioral data at the system and application layers, reports collected data to the platform locally for comprehensive correlation analysis and accurate attack prediction, and depicts attacks by visualizing the attack process chain. Its threat-hunting feature precisely defends all endpoints against residual attacks based on extensive collected data. Its micro-segmentation feature offers centralized management of access control policies and one-click segmentation of security events.

The NovaGuard agent provides antivirus protection, intrusion defense, firewall isolation, data collection and reporting, and one-click security event handling.

1.1 Product Overview

NovaGuard supports on-premises deployment, where the NovaGuard manager is deployed on Linux servers for centralized management of NovaGuard agents. The NovaGuard manager collaborates with the ForeNova security cloud over the Internet, whereas the NovaGuard agent on each endpoint connects to NovaGuard over an internal network. It provides accurate security intelligence and solutions to local endpoint users, with data encrypted during communication. The deployment is shown in the following figure.



1.2 Key Features



NovaGuard offers pre-event, during-event, and post-event services based on its four capabilities: discovery, detection, defense, and response.

Discovery: Provides pre-event risk assessment capabilities, including fingerprint-based asset inventory, shadow asset discovery, vulnerability patch management, security compliance check, exposure surface analysis, application/system/account risk assessment, security enhancement, USB device control.

Detection: Provides threat detection capabilities, including funnel-style detection, AI-powered ForeNova Engine Zero, ransomware defense, advanced threat prevention, application behavioral profiling, and abnormal behavior identification.

Defense: Provides defense capabilities, including secondary authentication, micro-segmentation, virtual patching, vulnerability remediation, and automatic fix of viruses, ransomware, web shells, and brute-force attacks.

Response: Provides fundamental response capabilities, including process, DNS, IP address blocking, and file and host isolation. Integrate NovaGuard with other network security products, offering capabilities such as closed-loop threat fix, threat investigation, attack tracing, defense enhancement, and threat hunting.

2 Installation and Deployment

2.1 NovaGuard Manager Deployment

2.1.1 Software Deployment

You can implement software deployment for the NovaGuard manager in three ways: OVA image-based, ISO image-based, and script-based. Their scenarios are as follows.

1. **OVA image-based deployment:** Applicable to scenarios involving virtualization platforms such as VMware and ForeNova Hyper-Converged Infrastructure (HCI).
2. **ISO image-based deployment:** Applicable to scenarios involving physical servers or virtualization platforms.

3. **Script-based deployment:** Applicable to environments that do not support OVA and ISO image-based deployment.

Recommendations and differences:

1. **Strongly recommended: OVA image-based deployment**. As the OVA package contains the NovaGuard manager and the underlying Ubuntu system, you can directly use the NovaGuard manager after importing the OVA package. **The NovaGuard manager and the underlying Ubuntu system are installed after deployment.**
2. **Recommended: ISO image-based deployment**. The ISO package contains the NovaGuard manager and the underlying Ubuntu system. After installing the ISO package using a CD/DVD drive, USB device, or disk, the Ubuntu system is first installed, followed by the installation of the NovaGuard manager. This method takes longer than OVA image-based deployment and is recommended for environments not supporting OVA image-based deployment. **The NovaGuard manager and the underlying Ubuntu system are installed after deployment.**
3. **Not recommended: Script-based deployment**. This method will be phased out in future versions. Avoid using it whenever possible. This method applies to scenarios not supporting OVA and ISO image-based deployment. If the customer wants to adopt this method, apply for a special installation package containing only the NovaGuard manager. Since the underlying operating system is from the customer, the deployment may fail due to missing dependencies, missing drivers, or version incompatibility. The **NovaGuard manager is installed after the deployment.**

2.1.1.1 Installation Package Download

Download URL: Please ask your ForeNova contact for the details

NOTE

1. For OVA image-based deployment, download the OVA installation package.

2. For ISO image-based deployment, download the ISO installation package.

3. Download the NovaGuard upgrade package of the corresponding architecture for version upgrade.

2.1.1.2 OVA Image-Based Deployment

NOTE

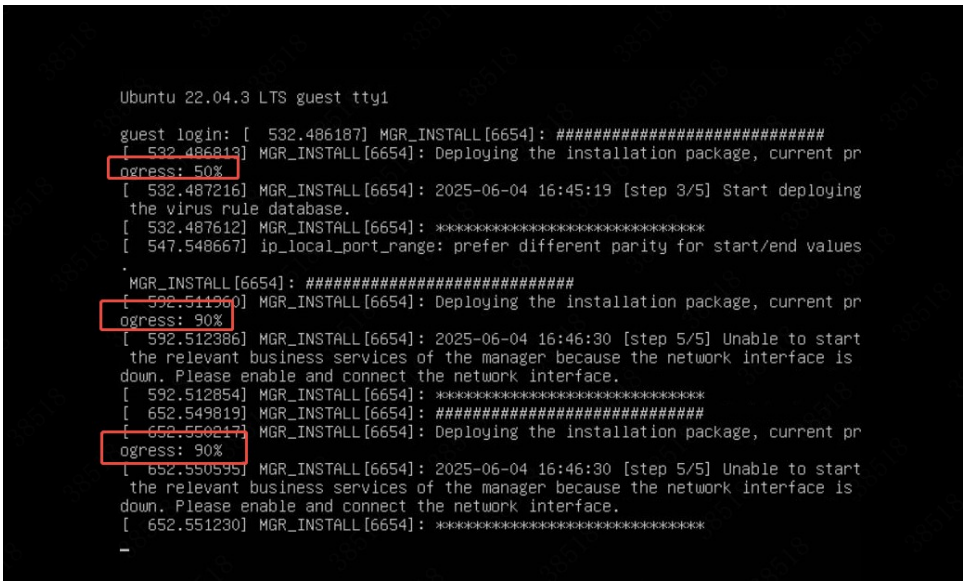
1.The following procedure is based on a VMWare / Proxmox, which is an example for your reference when using other virtualization platforms.

2.When creating a virtual machine, please allocate a network card in advance. Otherwise, the installation will fail.

Steps

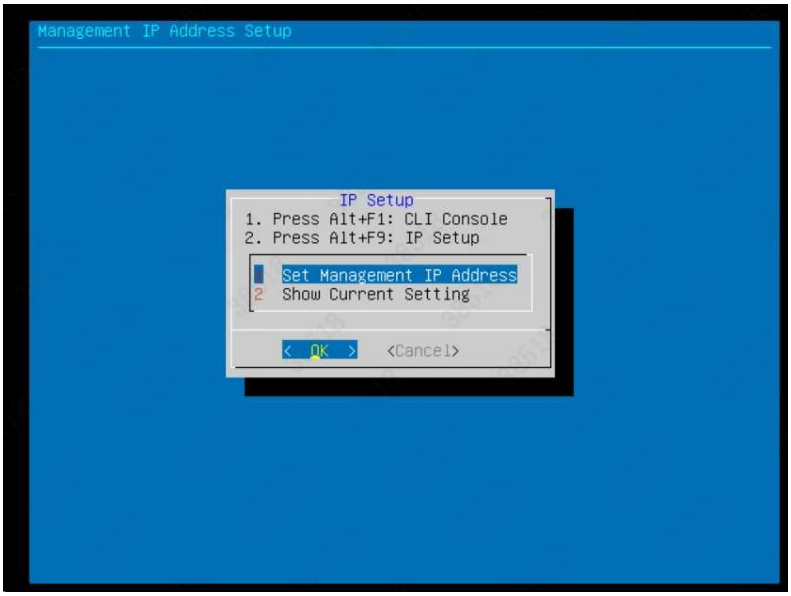
Step 1. Import the Open Virtual Appliance (OVA) template.

During the image import process, the console will display the installation progress.The deployment finishes after the import is complete, without the need to perform additional operations.

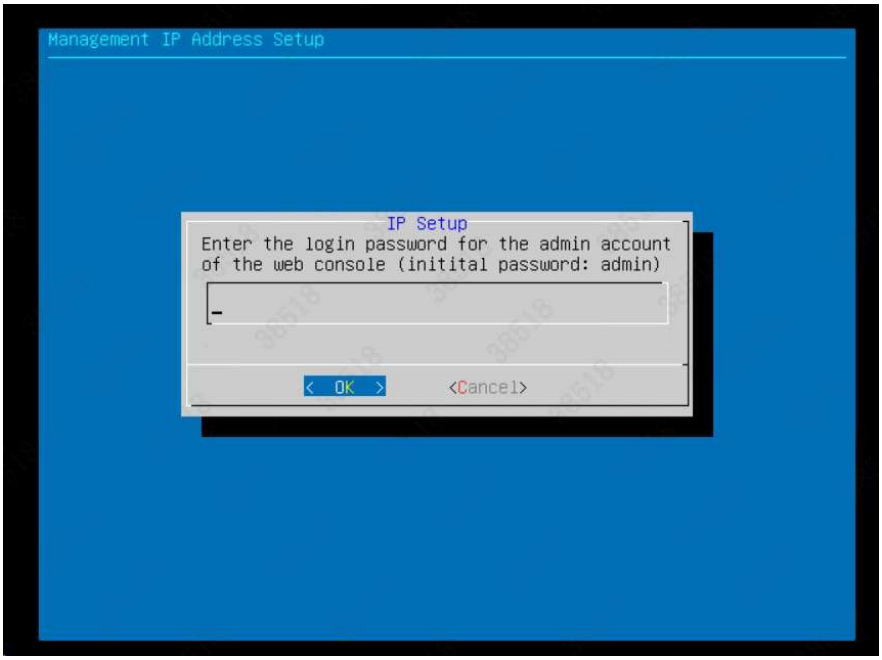


Step 2. Configure network settings.

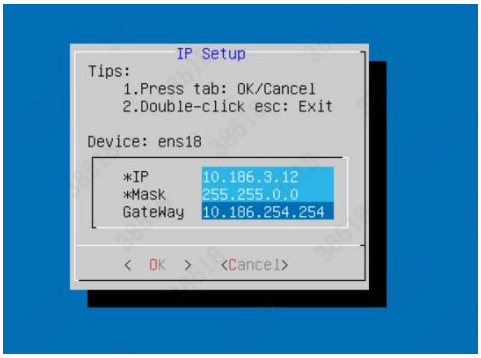
1. Log in to the web console of the NovaGuard manager, press Alt+F9 to go to the IP address configuration page, select **Set Management IP Address**, and click **OK**, as shown in the following figure.

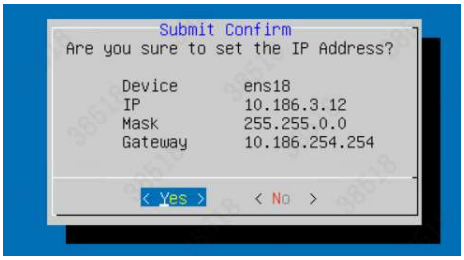


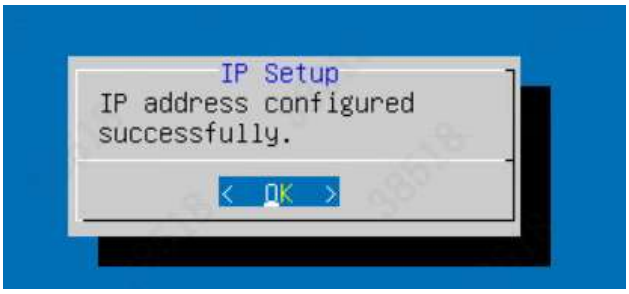
2. Enter the password of the admin account, and click **OK**. The default account and password both are "admin".



3. Configure the corresponding IP address, subnet mask, and gateway IP address as instructed, and save the configurations.





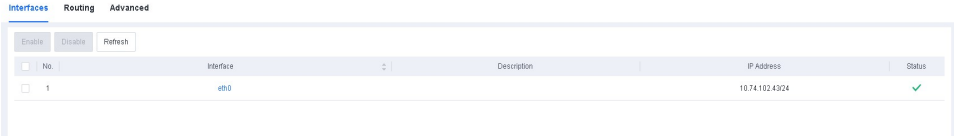


Step 3. Configure the DNS network.

NOTE

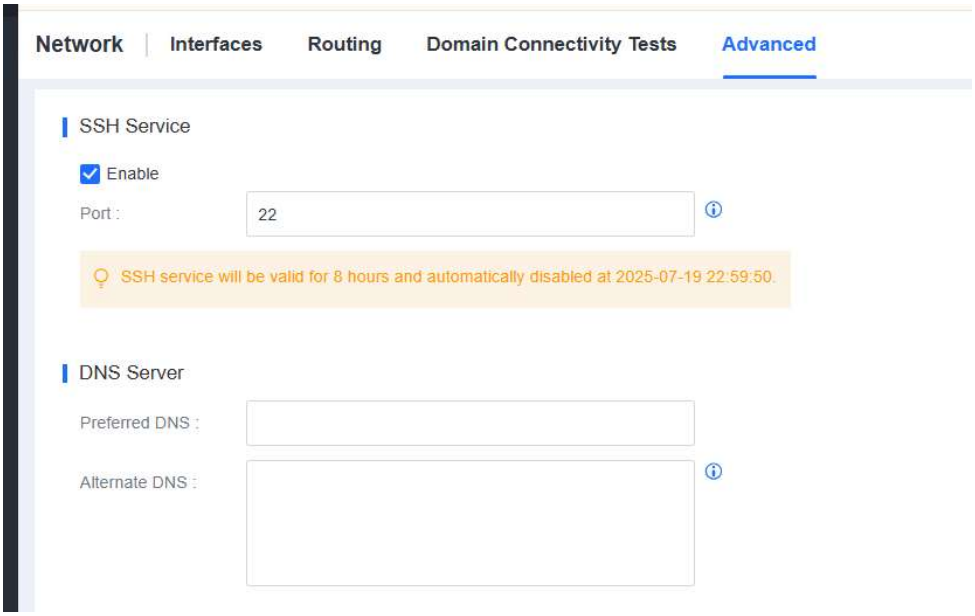
Supported browsers include Internet Explorer 10 and later, Firefox, Google Chrome, 360, and Microsoft Edge.

1. Based on the modified IP information, log in to the EPP manager (https://x.x.x.x). The default account is "admin" and the default password is "admin".
2. Go to **System** > **System** > **Network** > **Interfaces**, and specify the IP address configured for the management interface of the NovaGuard manager, as shown in the following figure.



3. Configure DNS servers.

Go to **System** > **System** > **Network** > **Advanced**, and configure a preferred DNS server and an alternate DNS server, as shown in the following figure.

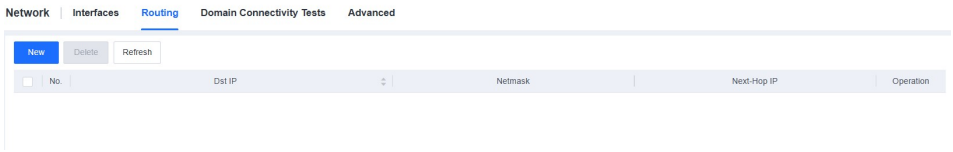


NOTE

The NovaGuard manager requires DNS servers to resolve domain names for antivirus database updates.

Step 4. Configure routing information.

Go to **System** > **System** > **Network** > **Routing**, and configure a route, as shown in the following figure.



NOTE

The NovaGuard manager requires a route to connect to the Internet and communicate with endpoints.

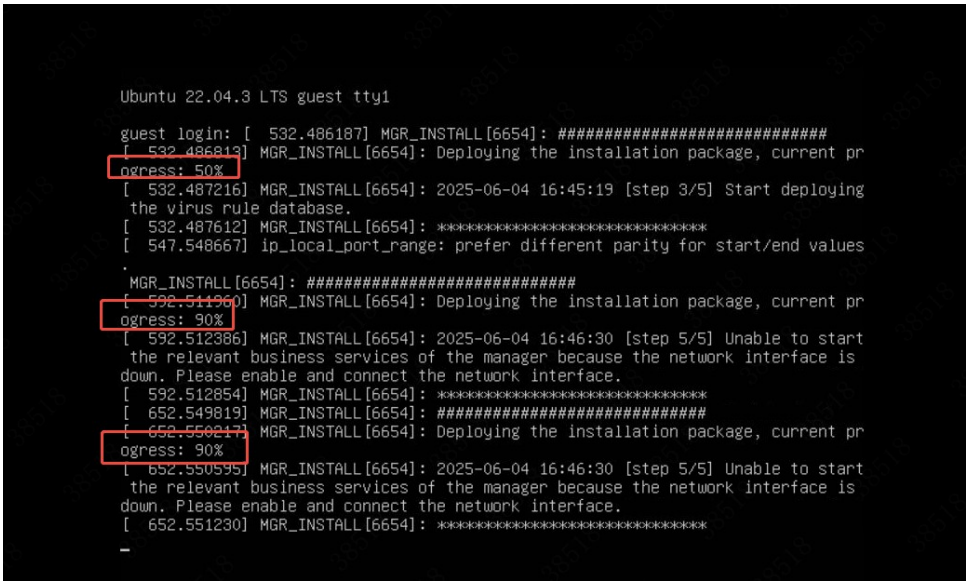
2.1.1.3 ISO Image-Based Deployment

Step 1. Prepare for the installation.

For installation on **physical servers**, use software such as UltraISO to burn the ISO template to a blank USB device or DVD. For installation on **virtual machines**, directly import the ISO image or mount a disk first.

Step 2. Install the NovaGuard manager.

During the image import process, the console will display the installation progress.The deployment finishes after the import is complete, without additional operations.



You do not need to log in to the server as the root user. If you have special requirements, call +60 12711 7129 (7511) to obtain the root password.

Step 3. Configure network settings.

Refer to Step 2 in Chapter 2.2.1.2 "OVA Image-Based Deployment".

2.1.1.4 Script-Based Deployment

NOTE

Prioritize OVA and ISO images for the NovaGuard manager deployment and use script-based deployment only in environments that do not support OVA/ISO image-based deployment.

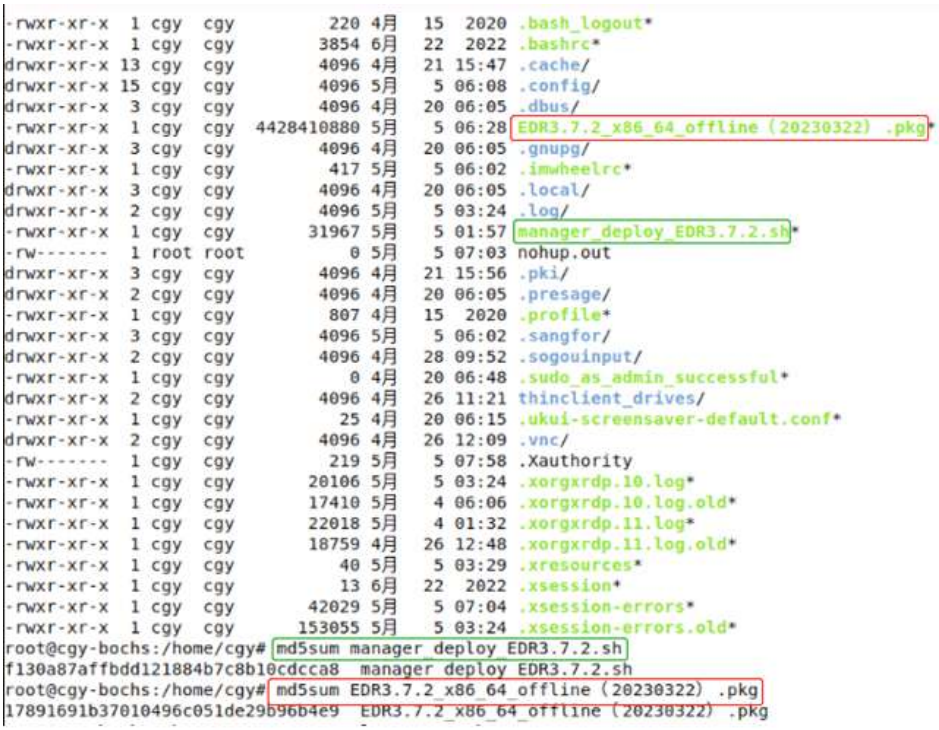
Before script-based deployment, prepare a server, install a compatible operating system on the server, configure network settings (including the server IP address, routing information, gateway, and DNS servers) for the server, and test the network connectivity of the server.

Step 1. Upload the installation package.

Upload the installation package (with the extension **.pkg**) and the installation script (with the extension **.sh**) to the same directory on the server, verify the MD5 checksum after the upload is complete to ensure package integrity and run the **chmod u+x manager_deploy.sh** command to make the installation script executable.

NOTE

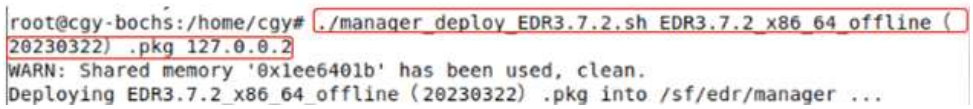
Packages whose name includes "**offline**" indicate offline installation packages. Select an offline NovaGuard installation package based on your operating system and architecture.



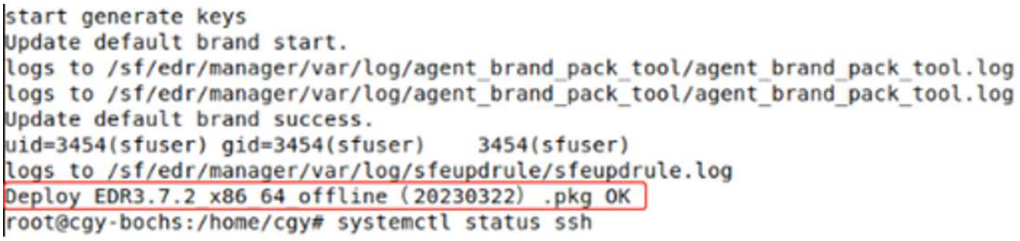
Step 2. Run the installation script.

Run the installation script by using the following command. Replace the package name and keep 127.0.0.2 unchanged:

./manager_deploy.sh package_name.pkg 127.0.0.2



The installation is complete once the prompt "**Deploy XXX.pkg OK**" appears.



Step 3. Configure network settings.

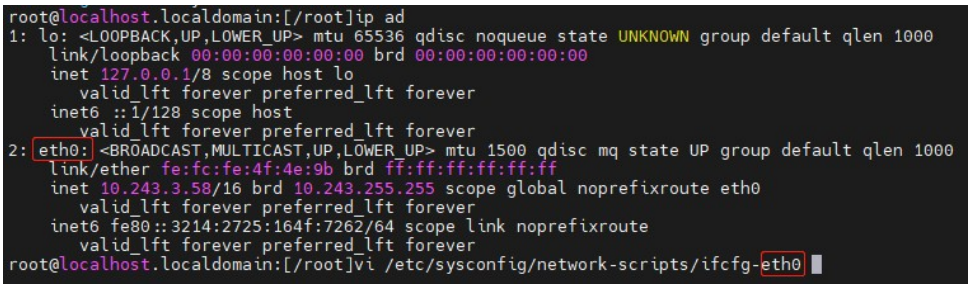
Network settings vary with the underlying operating systems and system versions. The following examples demonstrate how to configure interfaces and restart services on common operating systems.

Linux: vi /etc/sysconfig/network-scripts/ifcfg-XXX, systemctl restart network.service

Ubuntu: vi /etc/netplan/XX-network-manager-all.yaml, netplan apply

Example 1: Linux

Check the interface information and find the management interface eth0.



Open the configuration file of eth0. Set **BOOTPROTO** to **static**, set **ONBOOT** to **yes** to start the interface at boot time, and specify network settings (**IPADDR**, **NETMASK**, **GATEWAY**, and **DNS**). After the modifications, press **ESC**, type

"**:wq**", and then press **Enter** to quit the file.

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=eth0
UUID=a5a294f9-4a61-4adb-8e0b-35175fdca1e2
DEVICE=eth0
ONBOOT=yes
IPADDR=10.243.3.58
NETMASK=255.255.0.0
GATEWAY=10.243.255.254
DNS=8.8.8.8
DNS1=114.114.114.114
~
~
~
"/etc/sysconfig/network-scripts/ifcfg-eth0" 20L, 375C
```

Run **systemctl restart network** or **service network restart** to restart the network service for the interface configurations to take effect.

```
root@localhost.localdomain:[/root]service network restart
```

```
root@localhost.localdomain:[/root]systemctl restart network
```

Run **ifconfig** to check the interface configurations.

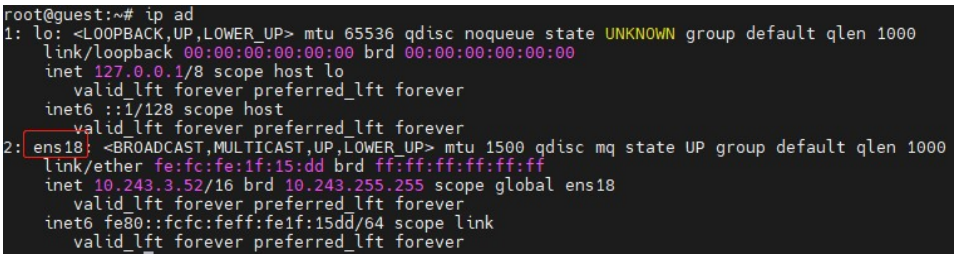
```
root@localhost.localdomain:[/root]ifconfig
eth0      Link encap:Ethernet  HWaddr FE:FC:FE:4F:4E:9B
          inet addr:10.243.3.58  Bcast:10.243.255.255  Mask:255.255.0.0
          inet6 addr: fe80::3214:2725:164f:7262/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:53576436 errors:0 dropped:45884 overruns:0 frame:0
          TX packets:13469675 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:32577334482 (30.3 GiB)  TX bytes:6124351127 (5.7 GiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:361903678 errors:0 dropped:0 overruns:0 frame:0
          TX packets:361903678 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:64713653999 (60.2 GiB)  TX bytes:64713653999 (60.2 GiB)

root@localhost.localdomain:[/root]
```

Example 2: Ubuntu

Check the interface information and find the management interface **ens18**.

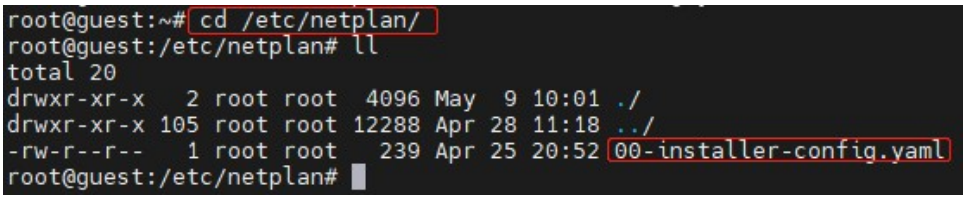


Run **vi /etc/netplan/00-installer-config.yaml**.



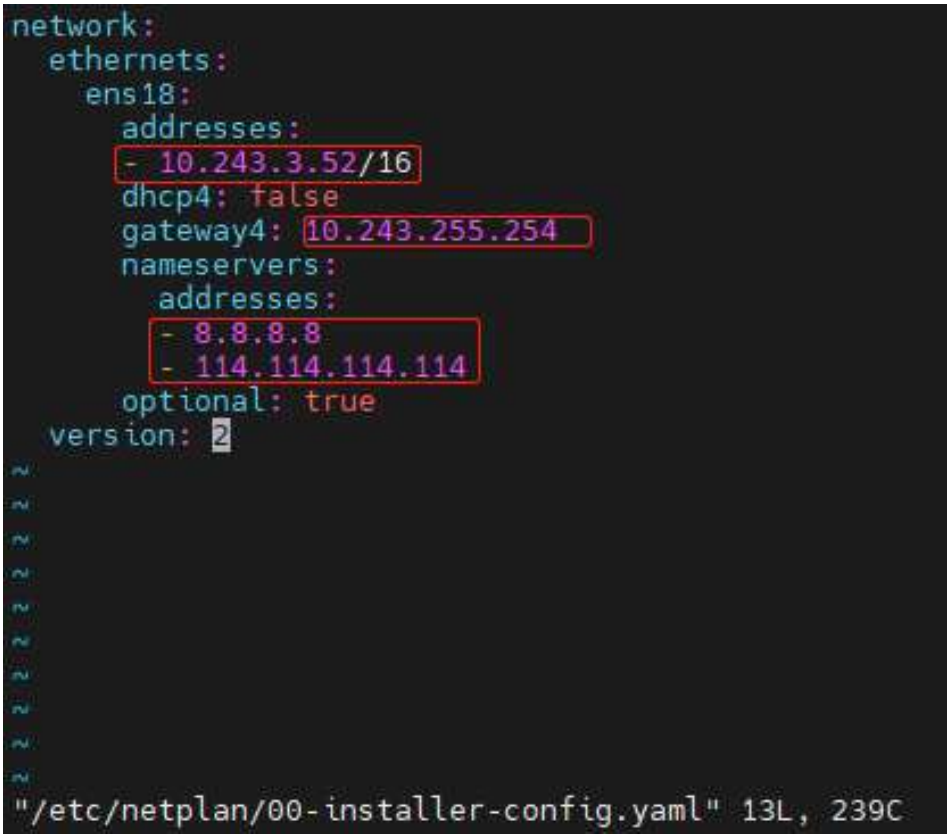
NOTE

The number in the preceding command may vary with the environment. Go to the directory **/etc/netplan/** for the accurate file name.



Modify the network settings, including **addresses (IP address and subnet mask**), **gateway4 (gateway),** and **nameservers (DNS servers**). After the

modifications, press **ESC** and type "**:wq**" to quit the file.



Run **netplan apply** to restart the network service for the interface configurations to take effect.

```
root@guest:/etc/netplan# netplan apply
```

Run **ifconfig** to check the interface configurations.

```
root@guest:/etc/netplan# ifconfig
ens18: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.243.3.52  netmask 255.255.0.0  broadcast 10.243.255.255
        inet6 fe80::fcfc:feff:fe1f:15dd  prefixlen 64  scopeid 0x20<link>
        ether fe:fc:fe:1f:15:dd  txqueuelen 1000  (Ethernet)
        RX packets 6140835  bytes 714255080 (714.2 MB)
        RX errors 0  dropped 43  overruns 0  frame 0
        TX packets 1432670  bytes 5086896441 (5.0 GB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

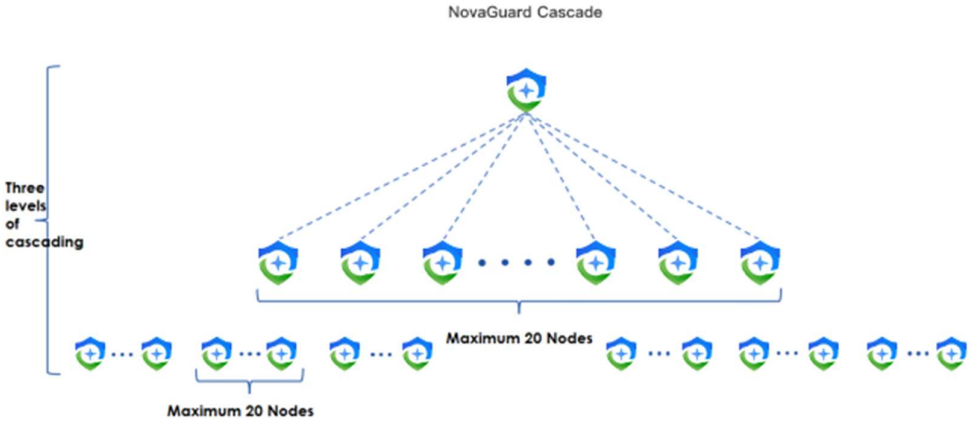
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 99325262  bytes 18266456614 (18.2 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 99325262  bytes 18266456614 (18.2 GB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2.1.2 Cascade Deployment

Scenarios

For example, a group company with headquarters and multiple branches has over 10,000 endpoints. You can deploy NovaGuard at headquarters and branches for endpoint management. It enables the headquarters to centrally and dynamically allocate licenses to or revoke licenses from the branches. It allows a higher-level NovaGuard manager to view the security status and connected endpoints of a lower-level NovaGuard manager.

Cascade deployment supports up to three levels, and each NovaGuard can connect to up to 20 NovaGuard managers. The following figure shows a cascade NovaGuard environment.



Deployment requirements:

Cascade deployment requirements are as follows.

1. Deploy the NovaGuard manager at both the headquarters and branches.
2. Activate all licenses for headquarters NovaGuard and allocate licenses from headquarters NovaGuard to branch NovaGuard.
3. Evaluate the number of licenses each branch needs based on the number of PCs and servers.

Cascade configuration:

1. **Deploy the NovaGuard manager at both the headquarters and branches.**

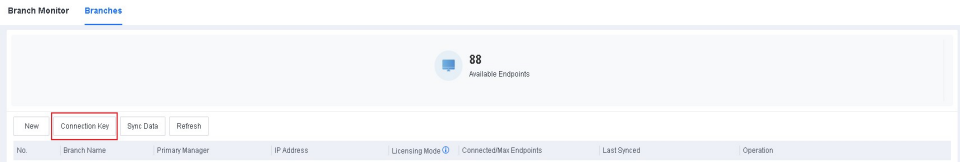
Select servers for the headquarters and branches based on their endpoint quantities and deploy the NovaGuard manager on these servers.

2. Activate headquarters NovaGuard.

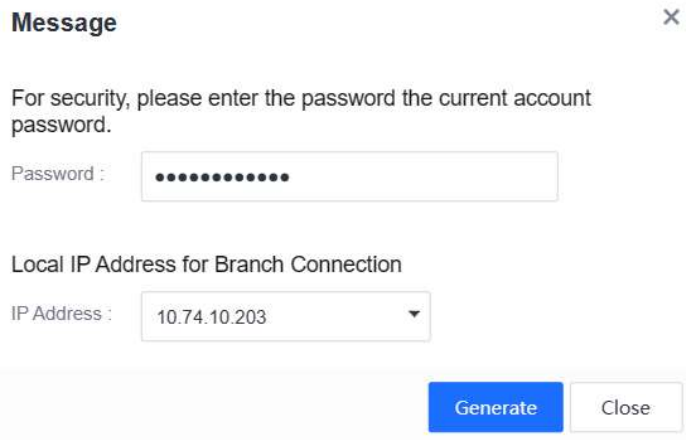
Activate all licenses for headquarters NovaGuard and allocate licenses from headquarters NovaGuard to branch NovaGuard.

3. Generate a connection key on the branch NovaGuard manager.

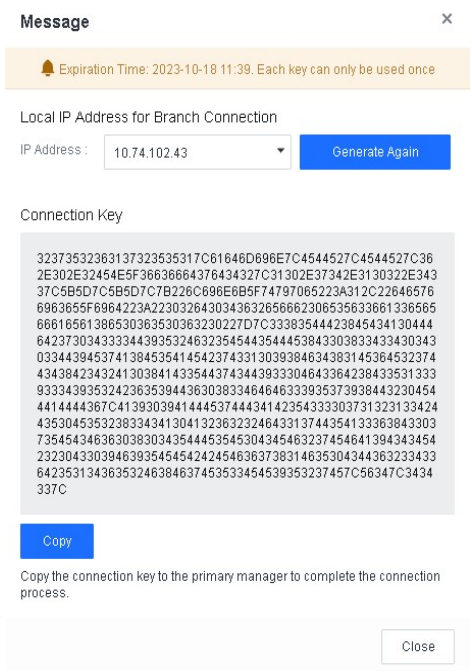
Log in to a **lower-level** NovaGuard manager, go to **System** > **Branches** > **Branches**, and click **Connection Key**, as shown in the following figure.



Enter the current account's password, and click **Generate**, as shown in the following figure.

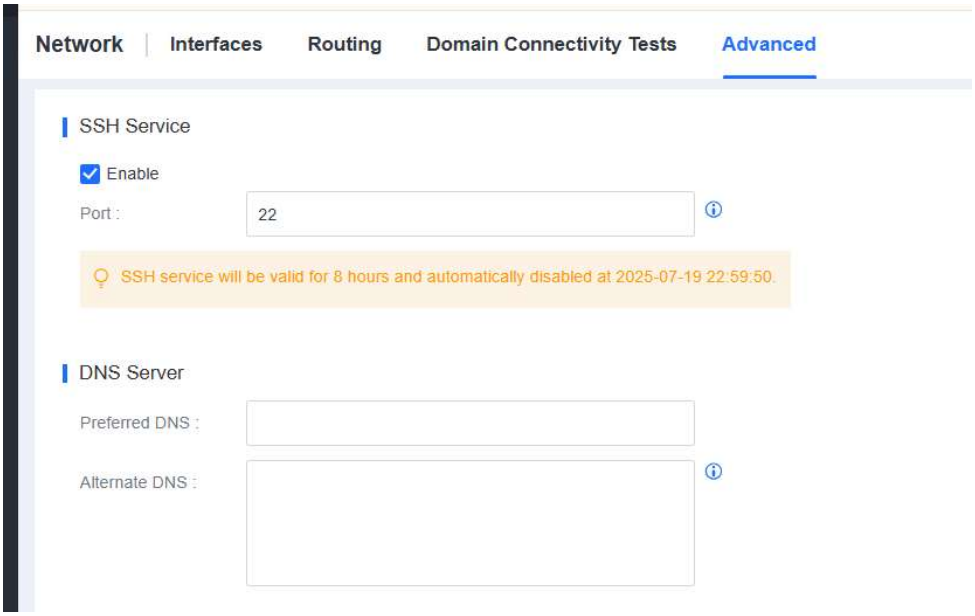


Click **Copy** to copy the connection key to a **higher-level** NovaGuard manager to complete the connection process.



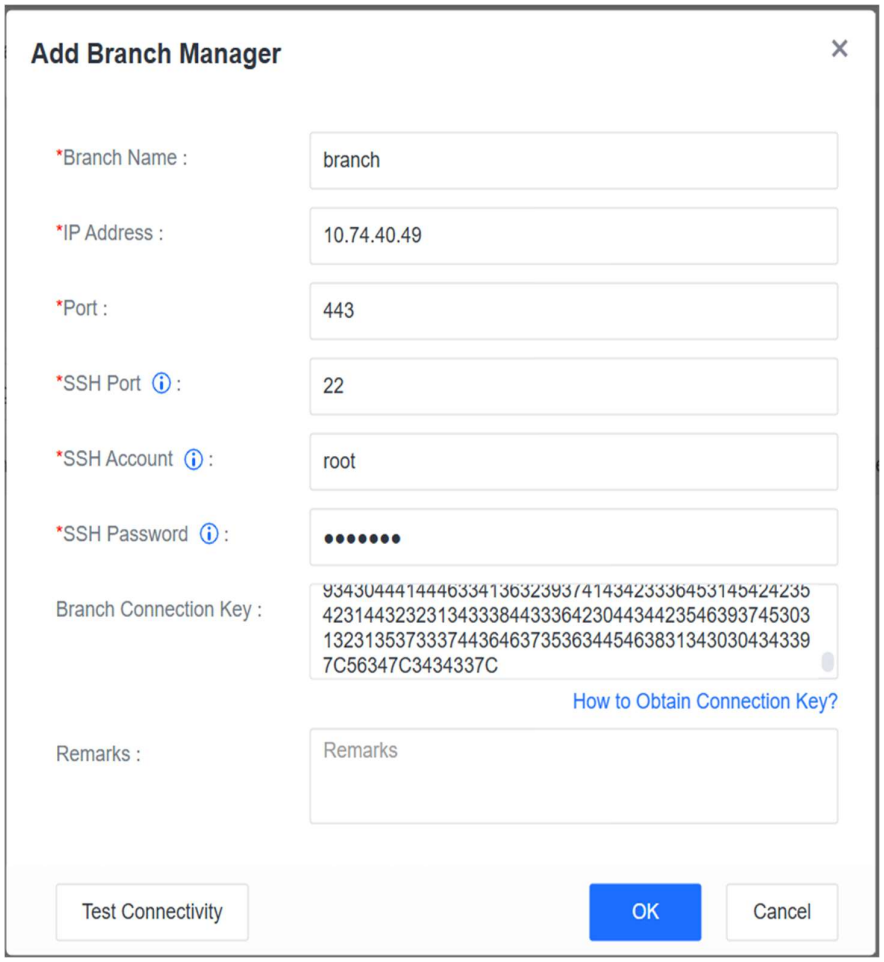
4. **Enable the Secure Shell (SSH) service for the branch NovaGuard manager.**

Log in to a **lower-level** NovaGuard manager, go to **System** > **System** > **Network** > **Advanced**, and check **Enable** in **SSH Service**, as shown in the following figure.

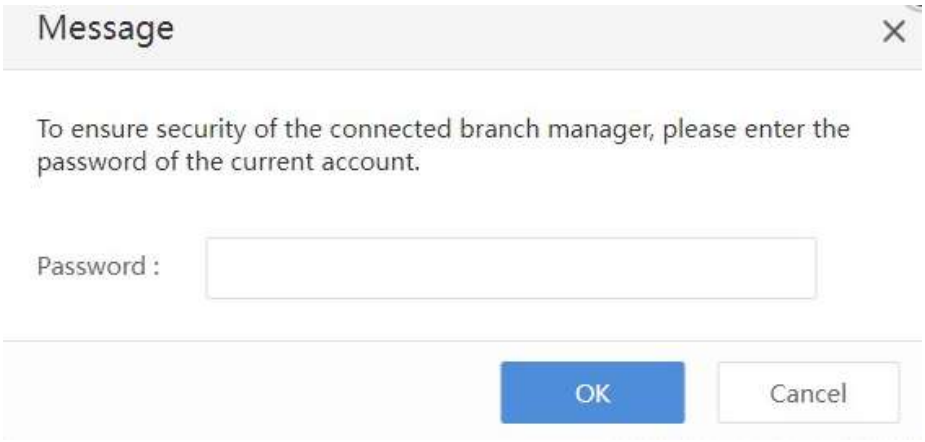


5. **Connect the branch NovaGuard manager to the headquarters NovaGuard manager.**

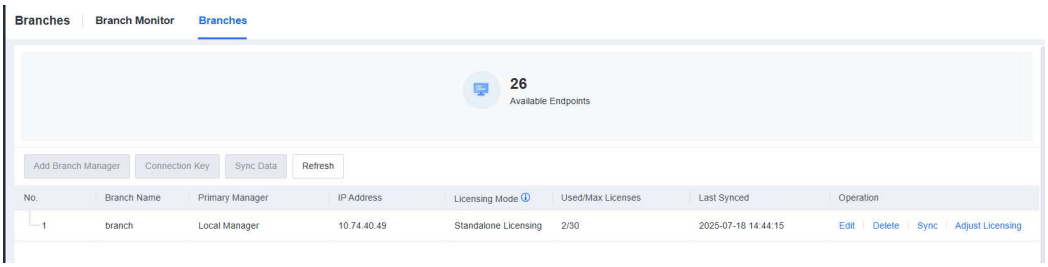
Log in to a **higher-level** NovaGuard manager, go to **System** > **Branches** > **Branches**, and click **Add Branch Manager**, as shown in the following figure.



Specify the branch name, IP address, port, SSH port, administrator account username and password, and branch connection key, and click **OK**, as shown in the following figure.



Enter the password of the current account, and click **OK.** Then, you can see the added branch NovaGuard manager, as shown in the following figure.



The Branches page includes the **Branch Name**, **IP Address**, **Licensing Mode**, **Connected/Max Endpoints**, **Last Synced**, and **Operation** columns.

Licensing Mode: There are two licensing modes for lower-level NovaGuard managers in cascade deployment scenarios: **standalone licensing** and **cascade licensing**. In standalone licensing mode, lower-level NovaGuard managers have independent licenses, which the relevant higher-level NovaGuard manager cannot adjust dynamically. In cascade licensing mode, licenses of lower-level NovaGuard managers are allocated by the relevant higher-level NovaGuard manager, and the high-level NovaGuard manager can adjust these licenses dynamically according to actual needs.

Connected/Max Endpoints: The number of connected endpoints and the maximum number of endpoints allowed on lower-level NovaGuard managers.

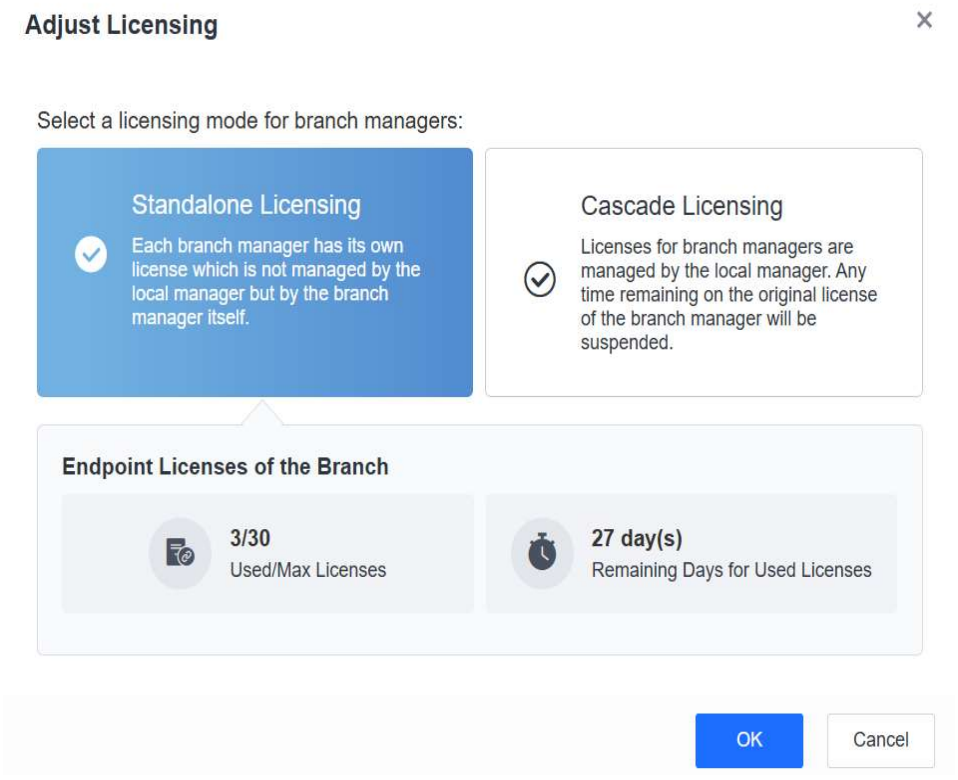
6. Allocate licenses from headquarters NovaGuard to branch NovaGuard.

Evaluate the number of licenses each branch needs and allocate licenses from headquarters NovaGuard to branch NovaGuard.

Go to **System** > **Branches** > **Branches**, as shown in the following figure.

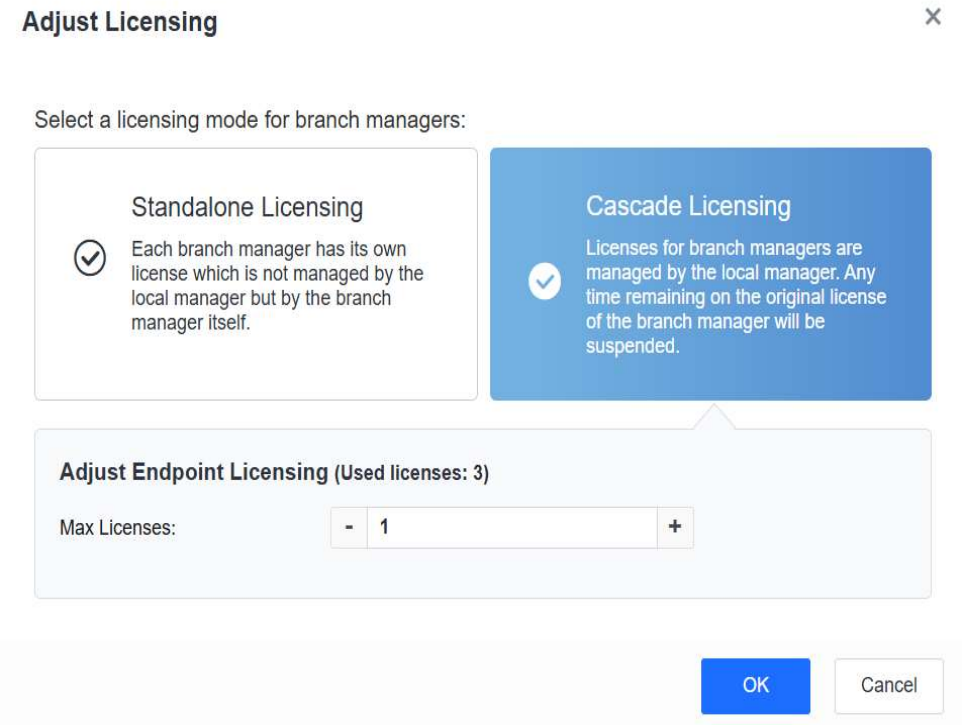


Select a branch, and click **Adjust Licensing** to go to the **Adjust Licensing** page, as shown in the following figure.



You can select **Standalone Licensing** or **Cascade Licensing** as the licensing mode of the lower-level NovaGuard manager. In standalone licensing mode, lower-level NovaGuard managers have independent licenses, which the relevant higher-level NovaGuard manager cannot adjust dynamically. In this example, select **Cascade Licensing**, and then specify the maximum number of endpoints and servers and the license period for the lower-level NovaGuard

manager.



After you adjust cascade licensing successfully, the following page appears.

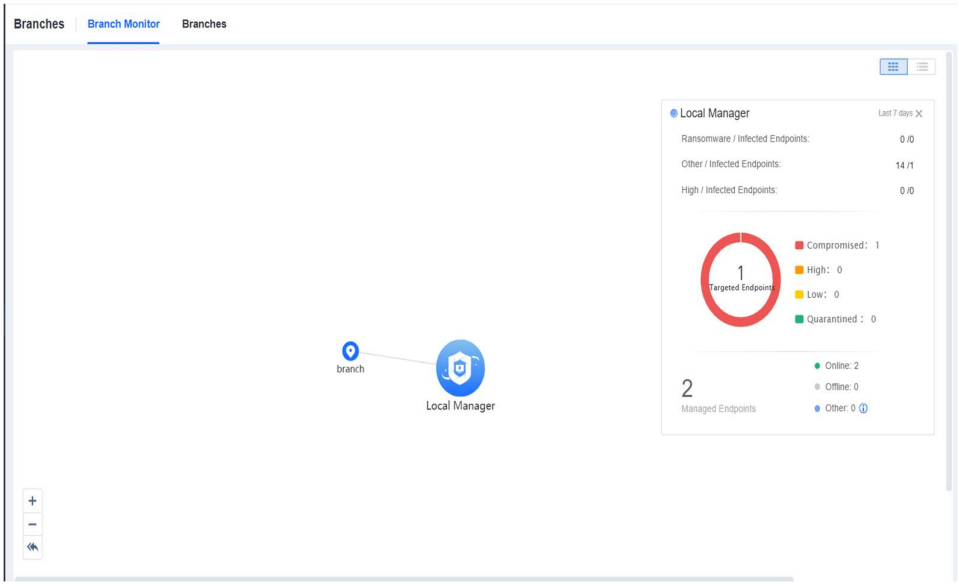


7. **Install the NovaGuard agent at both the headquarters and branches.**

The effect of the Cascade deployment:

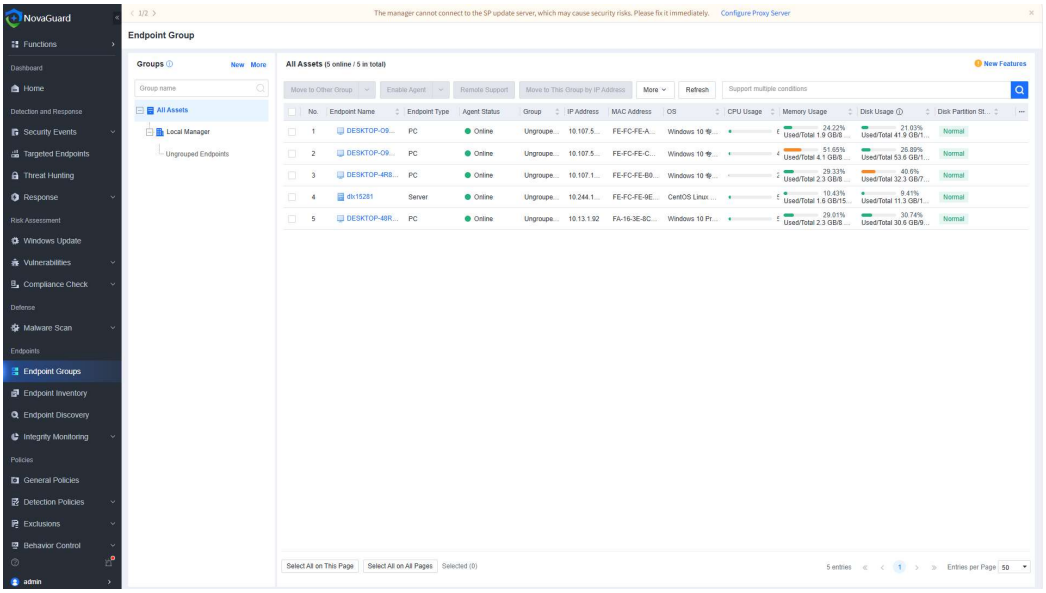
1. **View the security status of a lower-level NovaGuard manager.**

Go to **System** > **Branches** > **Branch Monitor**, and move the pointer over the icon of a lower-level NovaGuard manager to view its security status or click **Visit Branch Manager** to go to its login page, as shown in the following figure.



2. View the connected endpoints of a lower-level NovaGuard manager.

Go to **Endpoints** > **Endpoint Groups**, as shown in the following figure.



2. Implement cascade licensing.

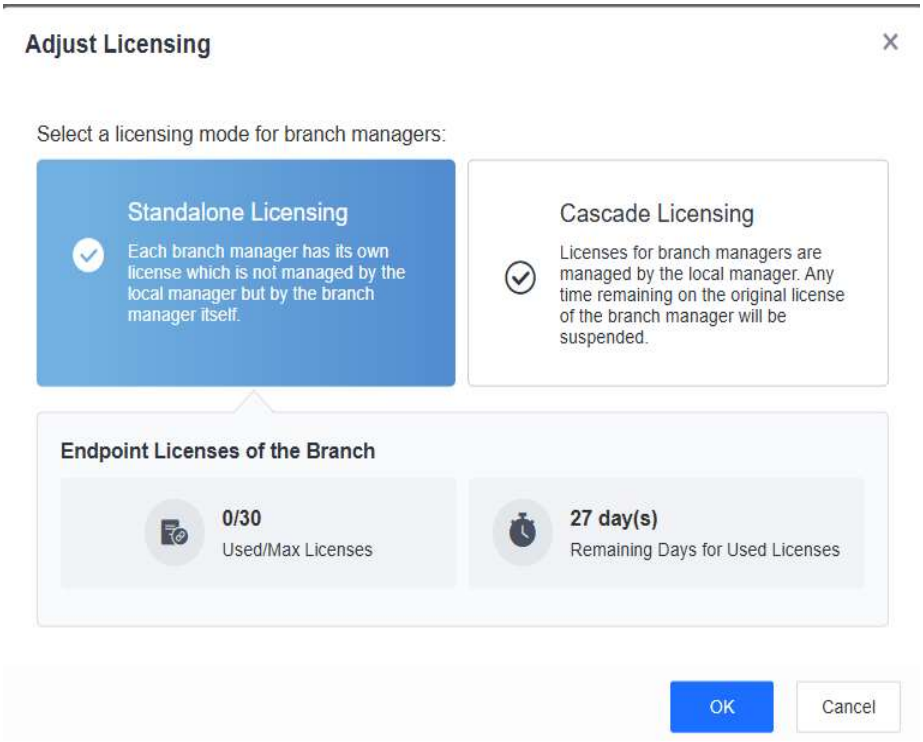
Cascade licensing is suitable for scenarios where a certain number of licenses need to be allocated and revoked dynamically across branches.

After activating a certain number of licenses for a higher-level NovaGuard manager without activating any license for lower-level NovaGuard managers, you can allocate licenses to or revoke licenses from lower-level NovaGuard managers on the higher-level NovaGuard manager.

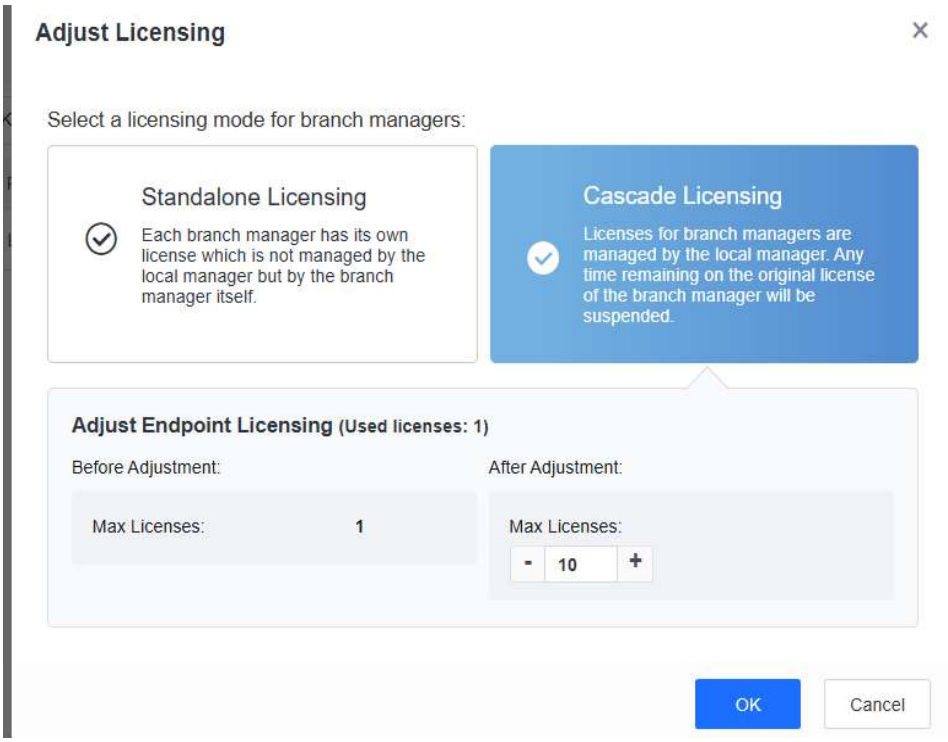
Go to **System** > **Branches** > **Branches**, as shown in the following figure.



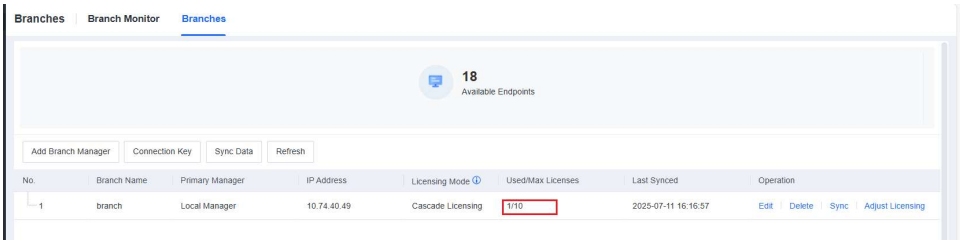
Select a branch, and click **Adjust Licensing** to go to the **Adjust Licensing** page, as shown in the following figure.



You can select **Standalone Licensing** or **Cascade Licensing** as the licensing mode of the lower-level NovaGuard manager. In standalone licensing mode, lower-level NovaGuard managers have independent licenses, which the relevant higher-level NovaGuard manager cannot adjust dynamically. In this example, select **Cascade Licensing**, and then specify the maximum number of PCs and servers and the license period for the lower-level NovaGuard manager.

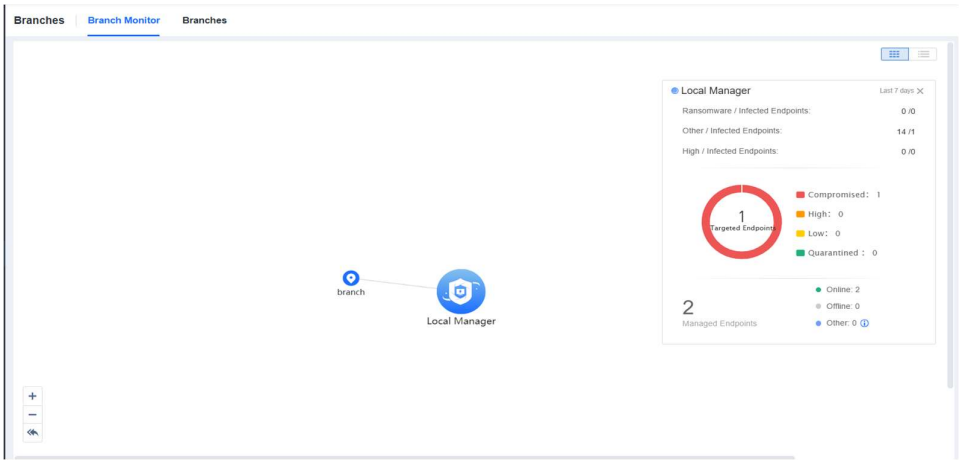


After you adjust cascade licensing successfully, the following page appears.



3. Go to a lower-level NovaGuard manager from the higher-level NovaGuard manager for management operations.

As shown in the following figure, you can go to the management page for a lower-level NovaGuard manager by clicking **Visit Branch Manager** on the **Branch Monitor** tab of the relevant higher-level NovaGuard manager.



NOTE

1. If the updated number of licenses for a lower-level NovaGuard manager is smaller than the number of connected PCs and servers, excess licenses are revoked in the following order: disabled endpoints > offline endpoints > online endpoints.

2. Endpoints in **Endpoint Groups** whose status is **Not Licensed** or **Agent Uninstalled** do not consume licenses.

3. In cascade licensing scenarios, you need to activate licenses for a higher-level NovaGuard manager. Then, you can dynamically adjust licenses for lower-level NovaGuard managers on the higher-level NovaGuard manager node.

2.2 Product Activation

After the deployment of the NovaGuard manager, activate NovaGuard before installing the NovaGuard agent. This section describes how to activate official and trial licenses for NovaGuard.

2.2.1 On-Premises NovaGuard Activation

Please contact your local sales or technical team to help activate your product.

2.2.2 Saas NovaGuard Activation

Please contact your local sales or technical team to help activate your product if you are using Saas NovaGuard.

2.3 NovaGuard Agent Deployment

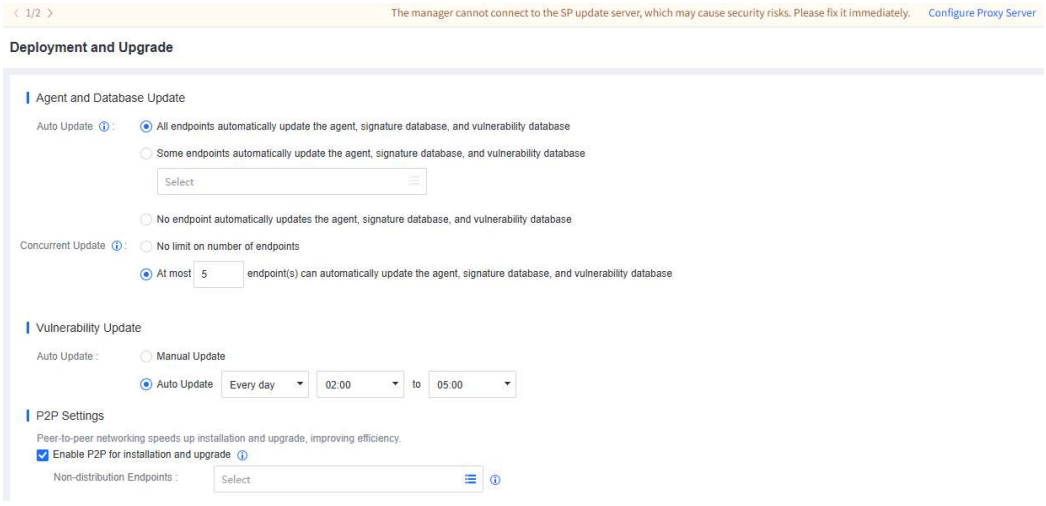
You can deploy the NovaGuard agent on Windows, Linux, or macOS endpoints. Other than macOS endpoints, the rest supports P2P NovaGuard agent deployment.

2.3.1 P2P Deployment

2.3.1.1 Feature Description

P2P deployment allows you to download the NovaGuard agent in parts from multiple seed nodes that have the NovaGuard agent installed. Compared to the previous single-channel NovaGuard agent download from the NovaGuard manager, this deployment method accelerates installation and upgrade and reduces the bandwidth usage of the NovaGuard manager. P2P deployment is disabled by default. However, it is recommended to enable P2P deployment and use it in combination with the installation methods described in the subsequent sections.

Go to **System** > **System** > **Deployment and Upgrade**, and select **Enable P2P for installation and upgrade**, as shown in the following figure.



Non-distribution Endpoints: Seed nodes will enable the HTTP service to provide multipart downloads. Select the endpoints you do not want to use as seed nodes for this field.

Download resources from ForeNova server first: By default, endpoints download resources from the NovaGuard manager when there are no distribution endpoints. Once enabled, endpoints download resources from the ForeNova server (CDN cache) first when they have Internet access and download resources from the NovaGuard manager when there is no Internet access.

Excluded IP Addresses: Exclude endpoints directly communicating with the NovaGuard manager to avoid business interruption caused by excessive Internet bandwidth usage during NovaGuard agent deployment or upgrade.

NOTE

1. P2P deployment is not supported in scenarios where the NovaGuard manager is exposed to the Internet through port mapping.

2. P2P deployment is supported on Windows and Linux endpoints **but not on Mac endpoints.**

3. P2P deployment is supported for NovaGuard agent installation, NovaGuard agent upgrade, and antivirus database update.

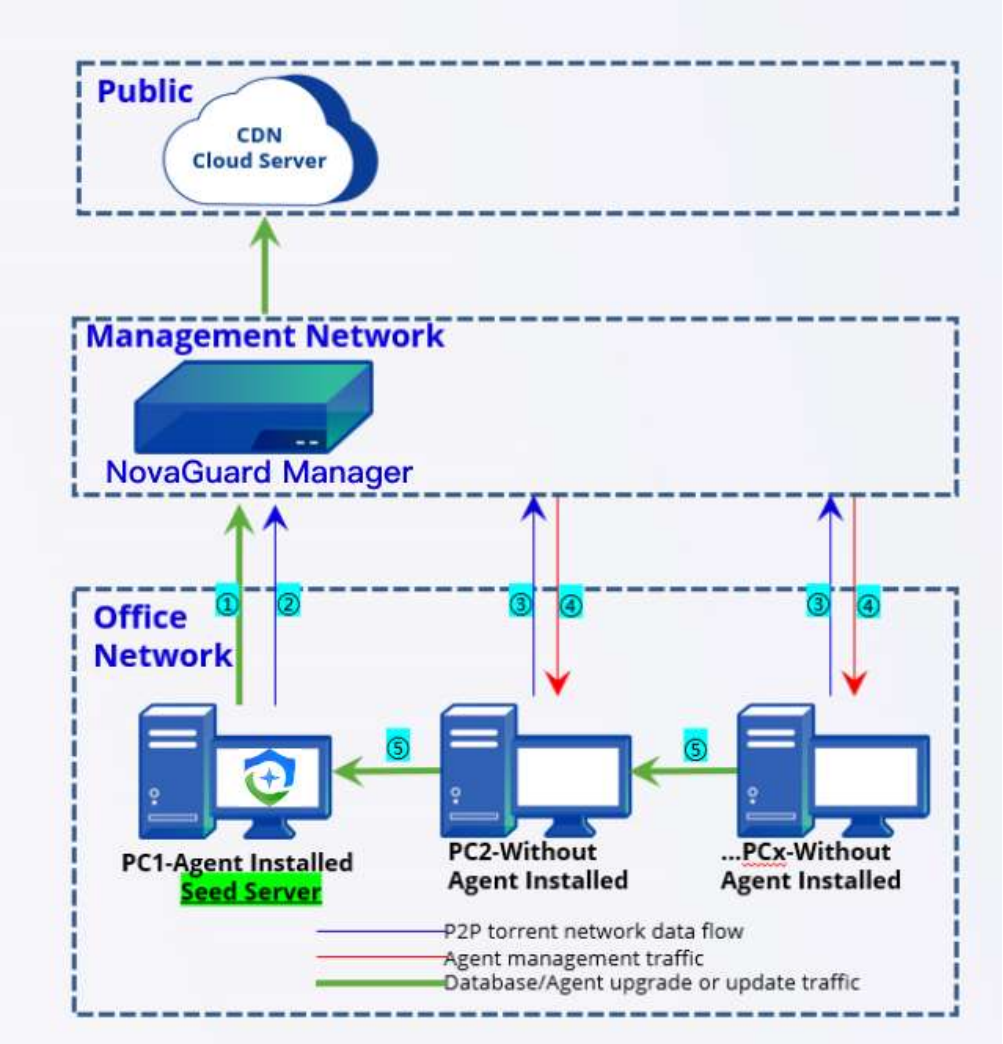
2.3.1.2 Scenarios

Scenario 1: The network bandwidth between the NovaGuard manager and NovaGuard agent is insufficient, and the bandwidth of the egress interface for Internet access is also insufficient.

Policy for NovaGuard agent: Update the NovaGuard agent and databases based on P2P deployment to reduce the bandwidth usage between the NovaGuard manager and the office network. Implement this policy first on non-critical business endpoints and then on critical business endpoints.

Policy settings for the NovaGuard manager:

1. Do not select **Download resources from the ForeNova server first**.
2. Select critical business endpoints for **Non-distribution Endpoints.**



Establishment of a seed node network for P2P deployment:

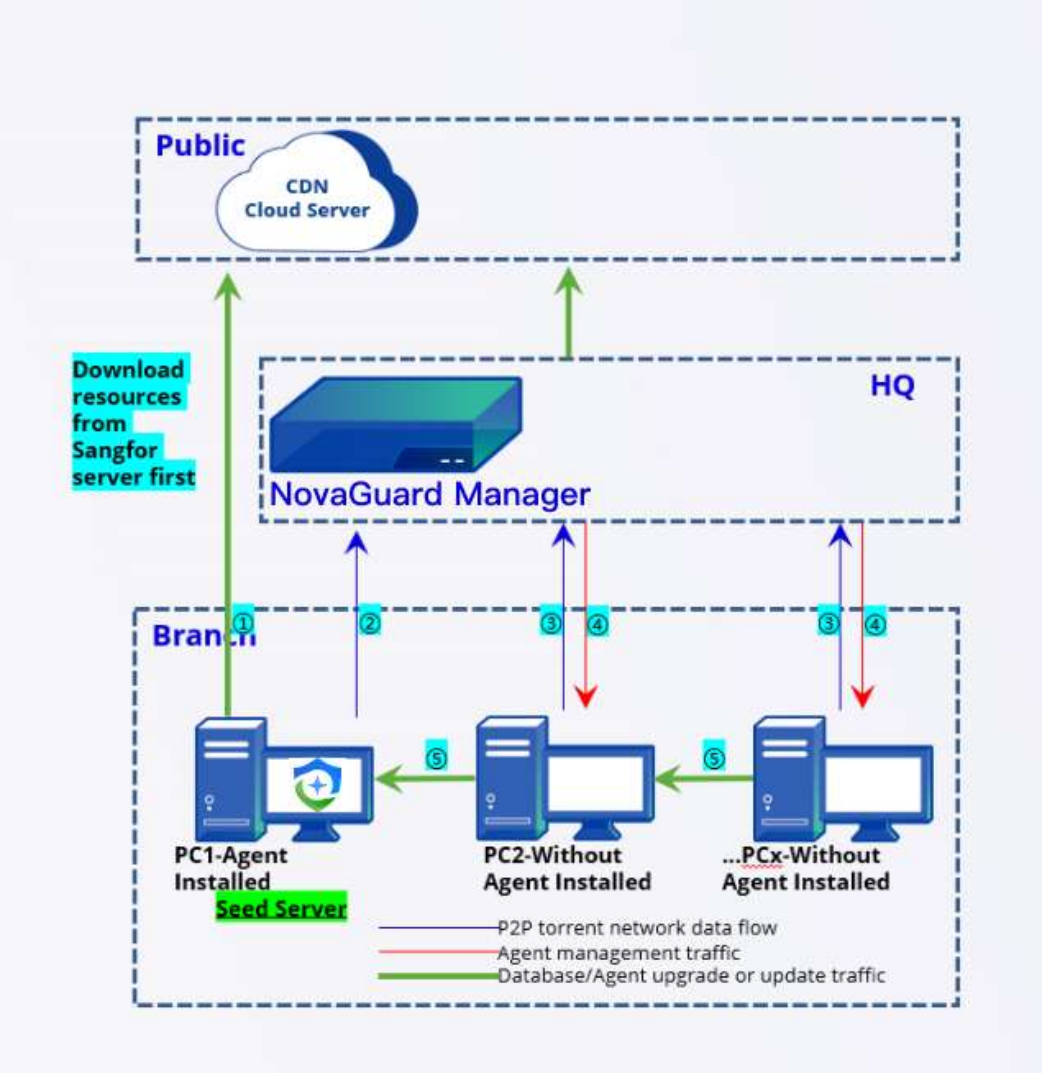
1. PC 1: Obtains the databases and upgrade package of the NovaGuard agent from the **NovaGuard manager** during the installation of NovaGuard.
2. PC 1: Sends a request to the NovaGuard manager to become **a seed node** after the installation. NovaGuard manager: Adds PC 1 to the seed node list.
3. PC 2: Checks with the NovaGuard manager to determine whether seed nodes are in the seed node list during the installation of NovaGuard.
4. NovaGuard manager: Queries the seed node list. If a **seed node** is in the same network segment (such as PC 1), the NovaGuard manager pushes down the P2P policy for PC 2 to download resources from PC 1.
5. PC 2: Downloads the databases and the upgrade package from PC 1 after receiving the P2P policy, starts the installation, and repeats Step 2.

Scenario 2: The bandwidth of the dedicated network or VPN between the headquarters and a branch is insufficient, but the bandwidth of the egress interface for Internet access at the branch is sufficient.

Policy for the NovaGuard agent: Update the NovaGuard agent and databases based on P2P deployment to reduce the bandwidth usage between the headquarters and the branch. Implement this policy first on non-critical business endpoints and then on critical business endpoints.

Policy settings for the NovaGuard manager:

1. Do not check **Download resources from ForeNova server first**.
2. Specify critical business endpoints for **Excluded IP Addresses** to avoid business interruption caused by excessive Internet bandwidth usage during NovaGuard agent upgrade.
3. Select critical business endpoints for **Non-distribution Endpoints.**



Establishment of a seed node network for P2P deployment:

1. PC 1: Obtains the databases and upgrade package of the NovaGuard agent from the **ForeNova server** during the installation of NovaGuard.
2. PC 1: Sends a request to the NovaGuard manager to become **a seed node** after the installation. NovaGuard manager: Adds PC 1 to the seed node list.
3. PC 2: Checks with the NovaGuard manager to determine whether **seed nodes** are in the seed node list during the installation of NovaGuard.
4. NovaGuard manager: Queries the seed node list. If **a seed node** is in the same network segment (such as PC 1), the NovaGuard manager pushes down the P2P policy for PC 2 to download resources from PC 1.
5. PC 2: Downloads the databases and the upgrade package from PC 1 after receiving the P2P policy, starts the installation, and repeats Step 2.

Comparison of the two scenarios:

1. **Similarities between Scenario 1 and Scenario 2:** Both scenarios have limited bandwidth between the headquarters and branches. **Seed nodes** are created based on P2P deployment during the early policy implementation stage, reducing the bandwidth usage of the dedicated network or VPN.
2. **Advantages of Scenario 2 over Scenario 1:** Using **Download resources from ForeNova server first** can distribute most of the traffic to the branch's egress interface for Internet access during the early stage, avoiding the impact of excessive bandwidth usage of the dedicated network or VPN on business systems. Adding the IP addresses of critical business systems in **Excluded IP Addresses** can prevent the impact of excessive Internet bandwidth usage on public access to these essential business systems.

2.3.2 Deployment on Windows

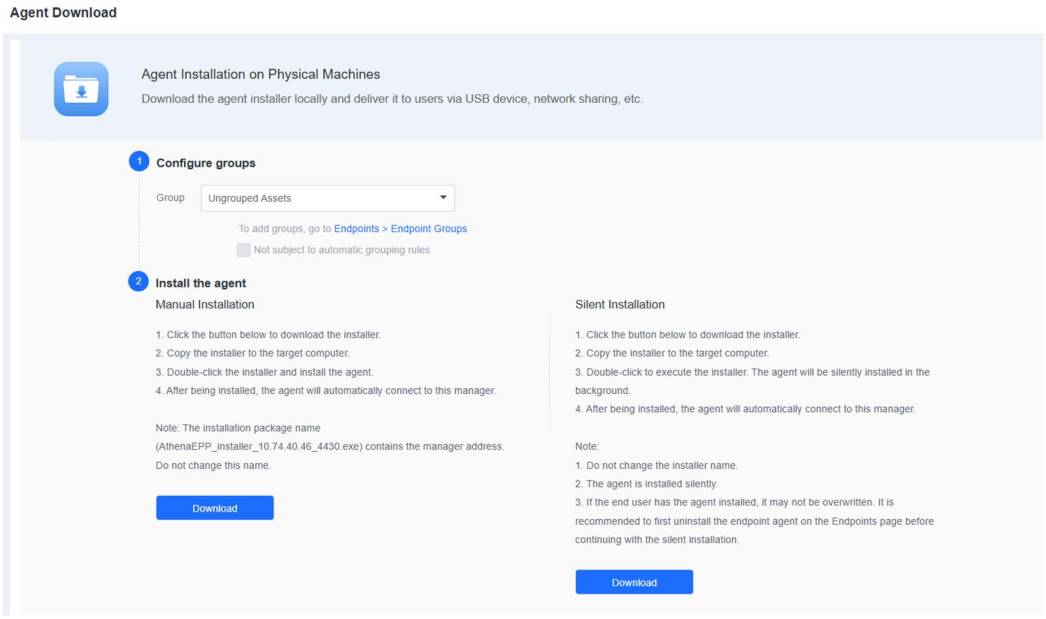
You can deploy the NovaGuard agent on Windows on a small or large scale.

1. **Small-scale deployment** methods (without third-party tools) include: manual installation, silent installation, installation on physical machines (full offline installer), and redirection to the NovaGuard agent installer download page.
2. **Large-scale deployment** methods (with a third-party tool) include: bulk installation via an Active Directory (AD) domain, bulk installation via desktop management software, bulk installation via integrated Internet access control devices, and bulk installation on virtual machines.

2.3.2.1 Manual Installation

Manual installation is the most commonly used method in small-scale deployment scenarios. Administrators download the NovaGuard agent installer from the NovaGuard manager and copy the installer to endpoints for installation using portable devices such as USB devices. The procedure is as follows:

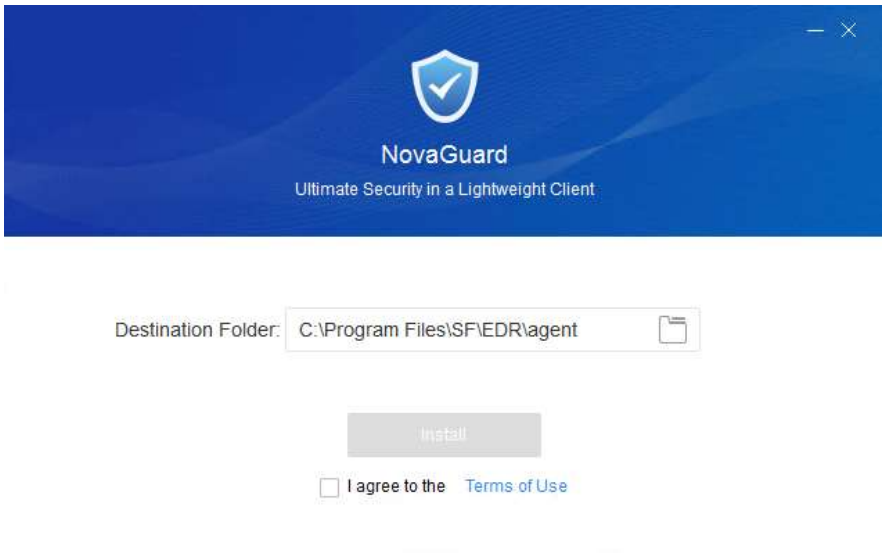
Step 1. Download the NovaGuard agent installer from the NovaGuard manager. Go to **System** > **Agent Deployment** > **Agent Download**, select **Windows** > **Agent Installation on Physical Machines**, and click **Download** under **Manual Installation**, as shown in the following figure.



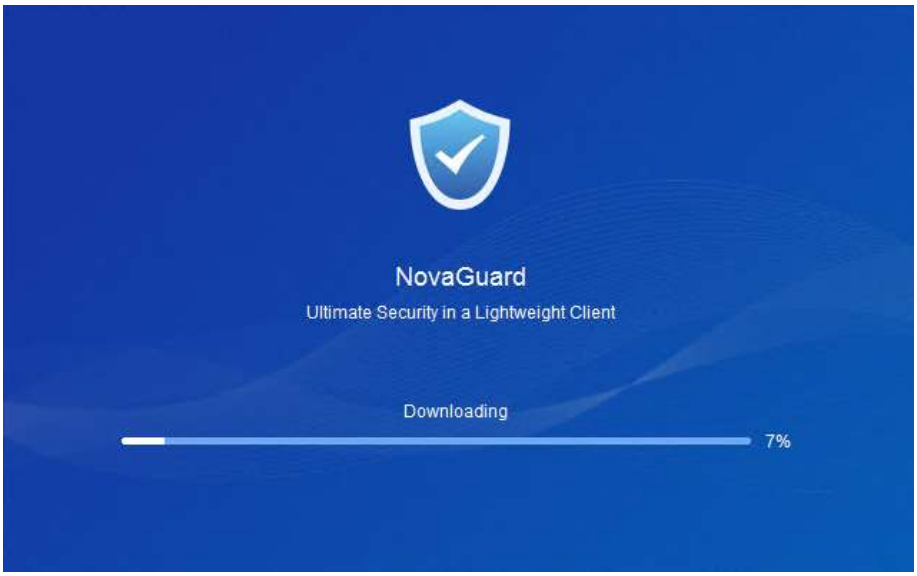
NOTE

The installer name (like NovaGuard_installer_[**Manager IP**]_4430.exe) contains the IP address of the EPP manager. **Do not change the installer's name**.

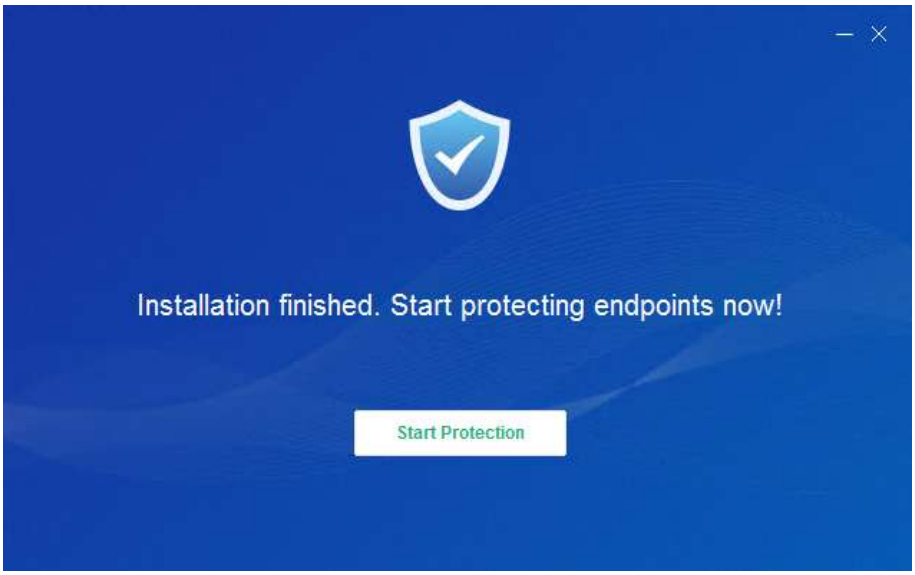
Step 2. Copy the installer to the target endpoint and double-click it to install. Reserve 5 GB of space for the installation. The default installation path is on the C drive. To install the NovaGuard agent on another drive, make sure you have super administrator permissions. Otherwise, use the default installation path.



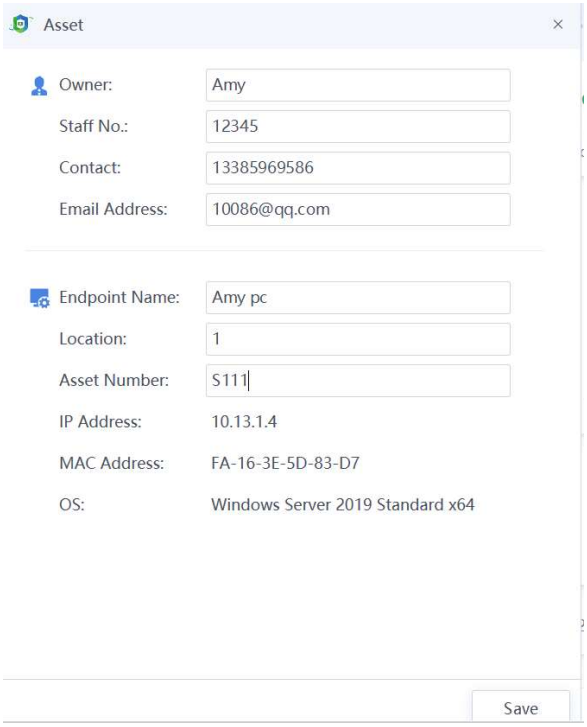
Read the terms of use, check **I agree to the Terms of Use**, and click **Install**. Then, the installer connects to the NovaGuard manager to download the necessary installation components, as shown in the following figure.



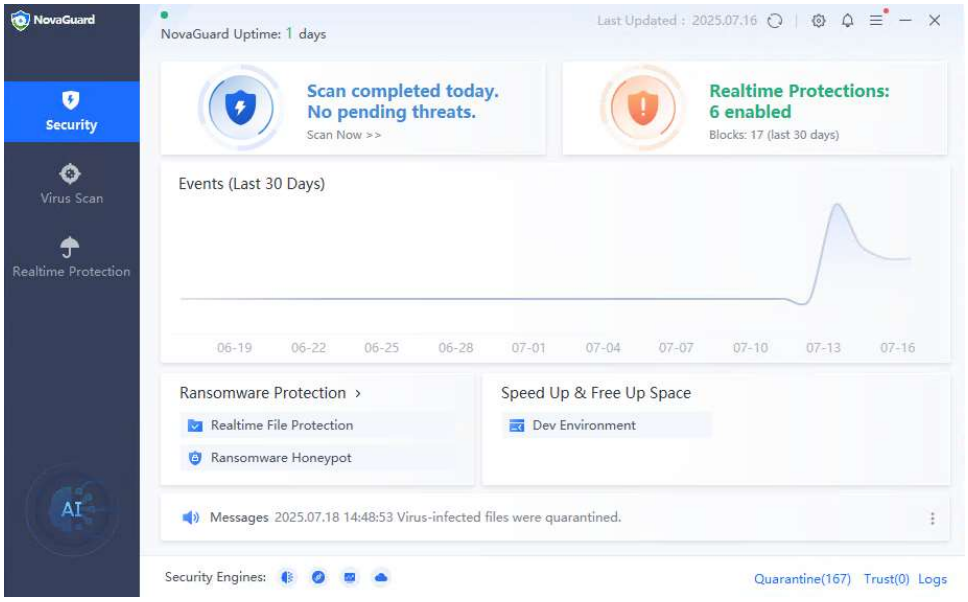
Wait for the installation of the components downloaded from the NovaGuard manager to complete.



After the installation, click **Start Protection** to register the asset, as shown in the following figure.

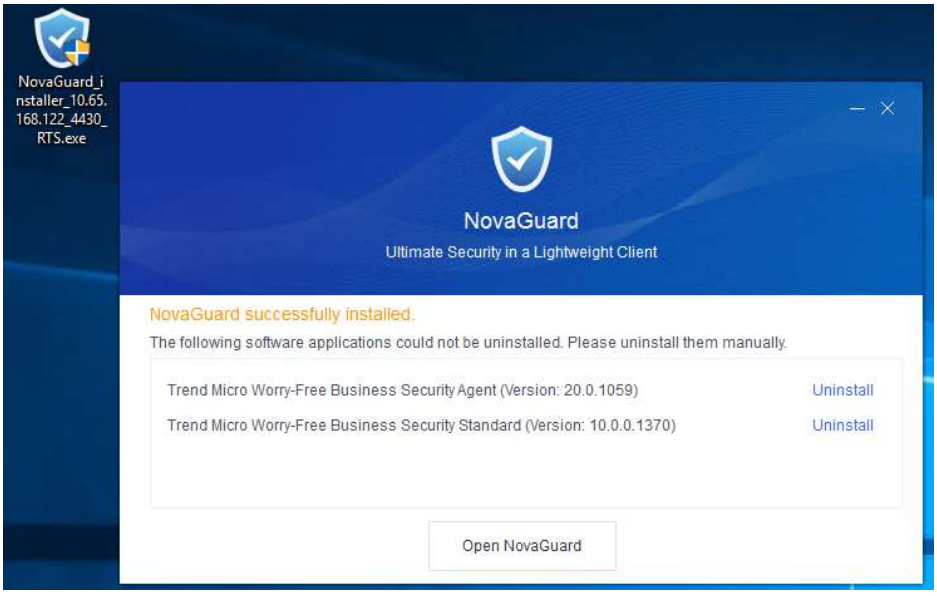


The NovaGuard agent is successfully installed once the NovaGuard homepage appears after the registration.



When you install the NovaGuard agent on an endpoint, NovaGuard automatically detects and uninstalls third-party antivirus software that is incompatible with the NovaGuard agent on the endpoint during the agent installation process.

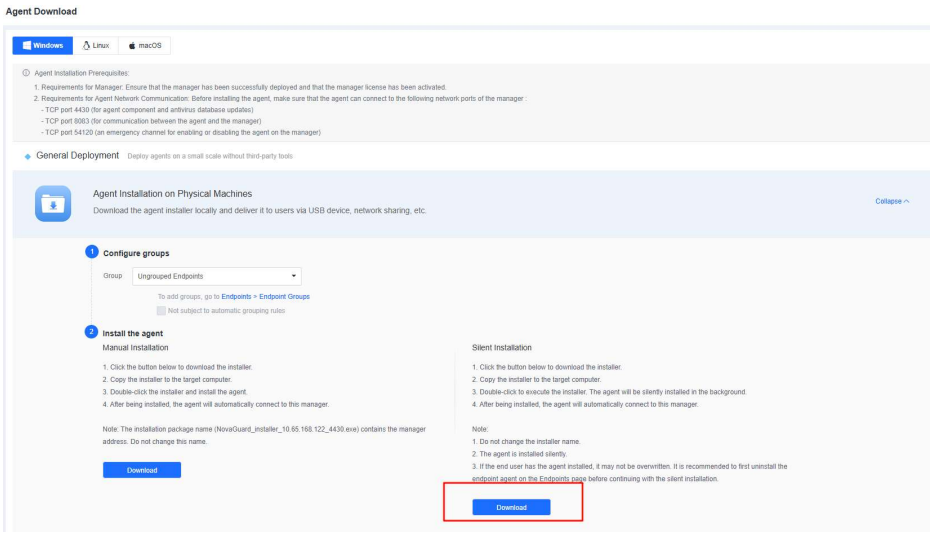
Modify the file name of the agent installation file and add the suffix **_RTS** at the end. It will uninstall the third-party EDR when the agent is installed. Otherwise, it will not uninstall the third-party EDR.



2.3.2.2 Silent Installation

Silent installation is an installation without the need for manual intervention. Administrators download the NovaGuard agent installer from the NovaGuard manager and copy the installer to endpoints for installation using portable devices such as USB devices. The procedure is as follows:

Step 1. Download the NovaGuard agent installer from the NovaGuard manager. Go to **System** > **Agent Deployment** > **Agent Download**, select **Windows** > **Agent Installation on Physical Machines**, and click **Download** under **Silent Installation**, as shown in the following figure.



Step 2. **Right-click the installer to execute it as an administrator or double-click the installer** for a silent, automatic installation. After the installation, the NovaGuard agent automatically connects to the NovaGuard manager, and you can find the online endpoint on the **Endpoints** > **Endpoint Groups** page of the NovaGuard manager.

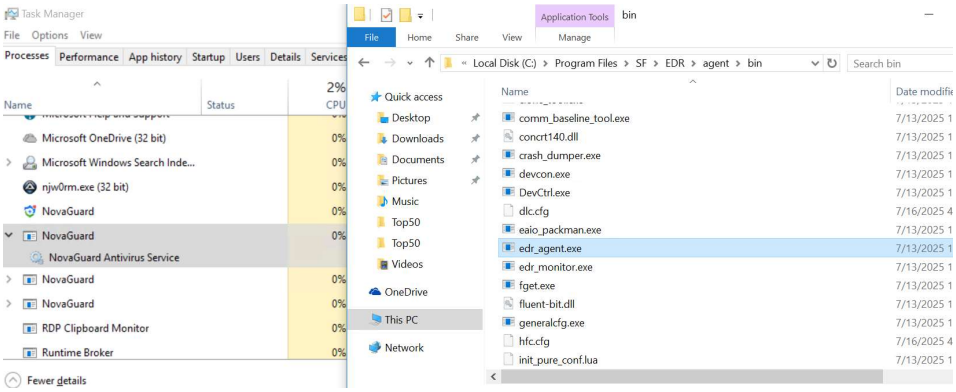


NOTE

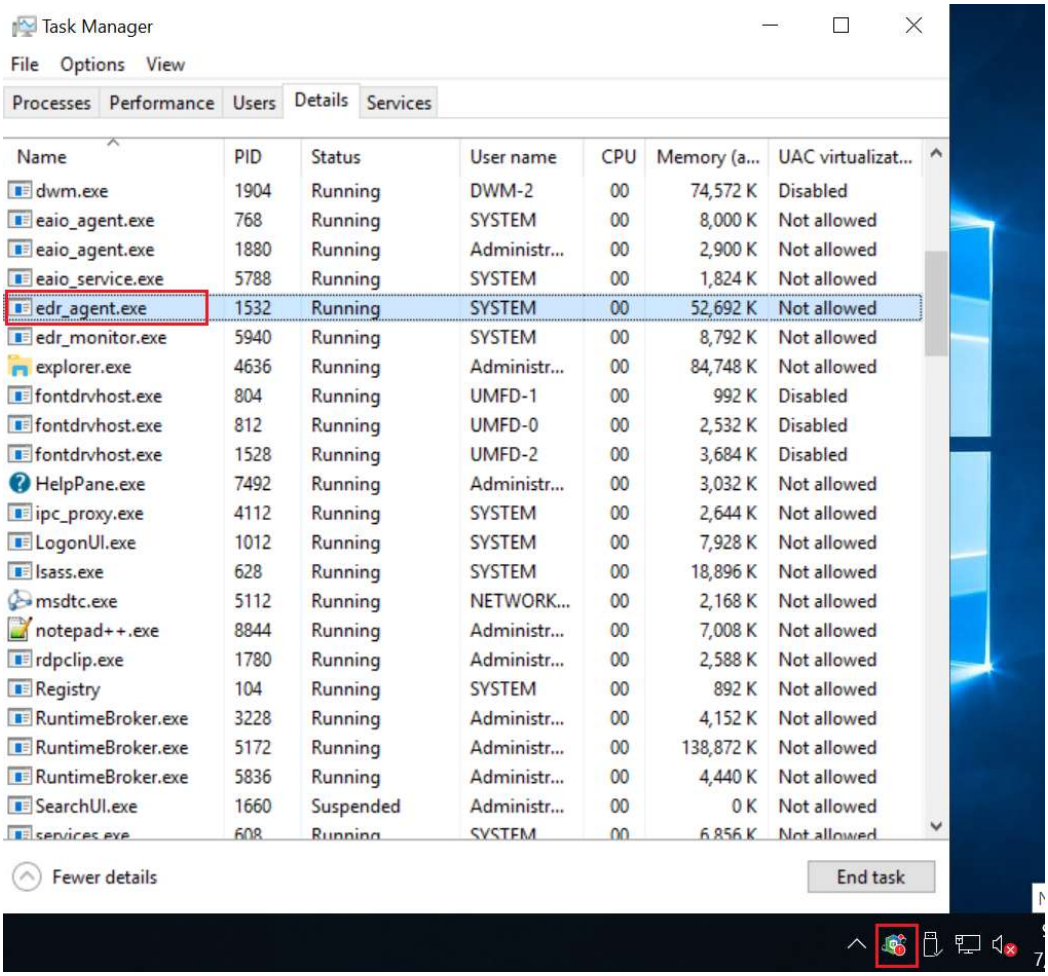
The installer name (like NovaGuard_installer_[**Manager IP**]_4430_silence.exe) contains the IP address of the NovaGuard manager and the word "**silence**". **Do not change the installer's name**.

NOTE

To check the silent installation process, open **Task Manager** to find the running **fget.exe** process. If the process is obtaining files, silent installation is in progress. Alternatively, open the default installation directory "**SF/EDR/agent/bin**" and refresh the page to check whether new files are created.



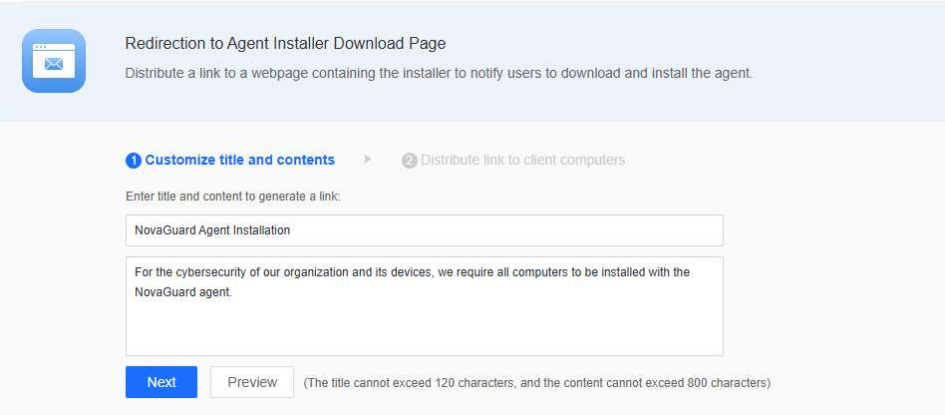
After the NovaGuard agent is successfully installed, the NovaGuard icon appears in the lower right corner of the screen, and the asset registration window pops up (whether filling in the information is required depends on the policy on the NovaGuard manager). You can also find the running edr_agent.exe and sfavui.exe processes in Task Manager.



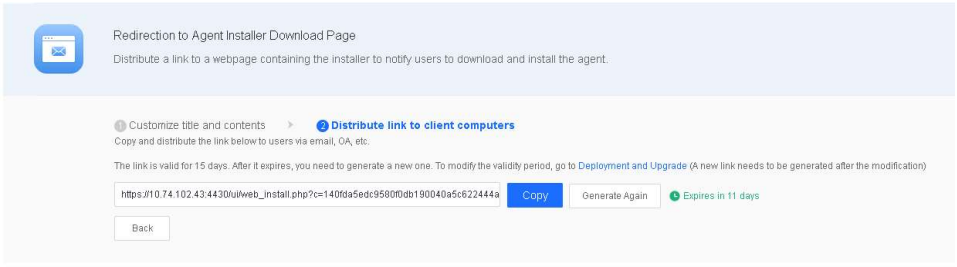
2.3.2.3 Redirection to the Agent Installer Download Page

Administrators can distribute a link to the installer download webpage to user endpoints via channels such as email and office automation (OA), **to remind the users to download and install the NovaGuard agent**.

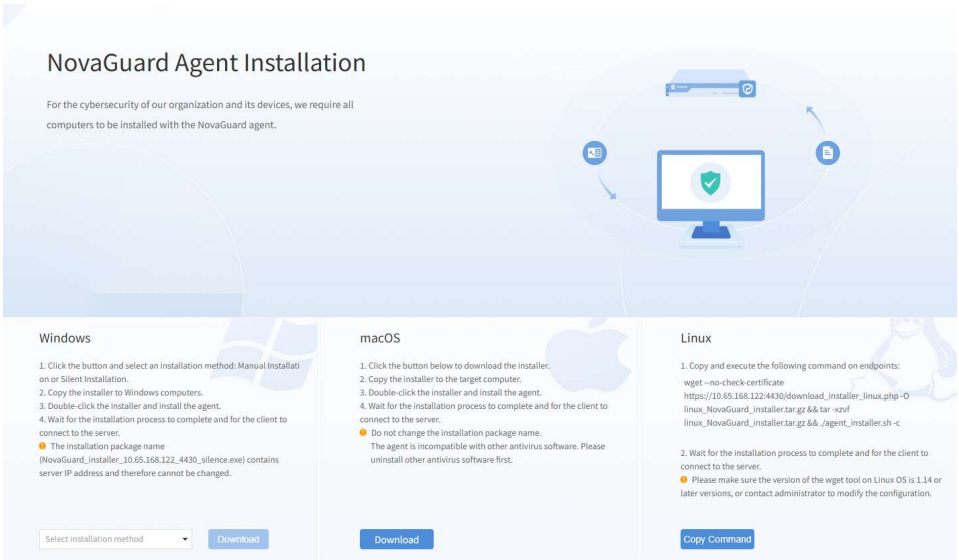
Go to **System** > **Agent Deployment** > **Agent Download**, select **Windows**, and then select **Redirection to Agent Installer Download Page** in **General Deployment**, as shown in the following figure.



Enter a title and the content on the **Customize title and contents** page and click **Next** to generate a link, as shown in the following figure.



Distribute the link to endpoints as an administrator via email, OA, or other channels for users to download and install the NovaGuard agent, as shown in the following figure.



2.3.2.4 Installation via an AD Domain

1. Scenario

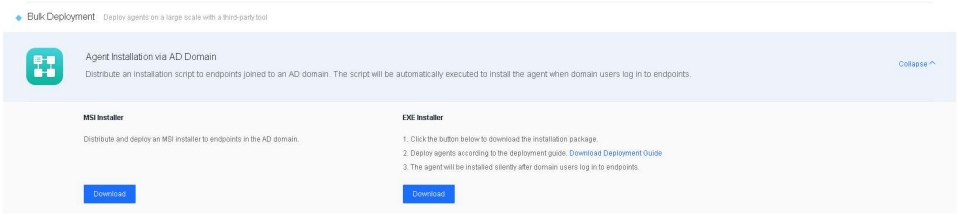
In scenarios where you have deployed a Microsoft AD domain controller in the internal network to which endpoints are connected for unified management, you can automatically install the silent NovaGuard agent package upon the startup of endpoints by distributing a group policy via the domain controller.

2. Procedure

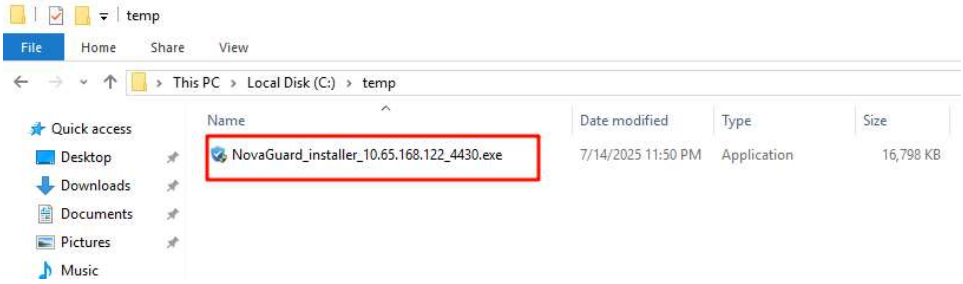
The procedure for NovaGuard agent installation via an AD domain is as follows:

Download the installer:

Download the installer and deployment guide, as shown in the following figure.

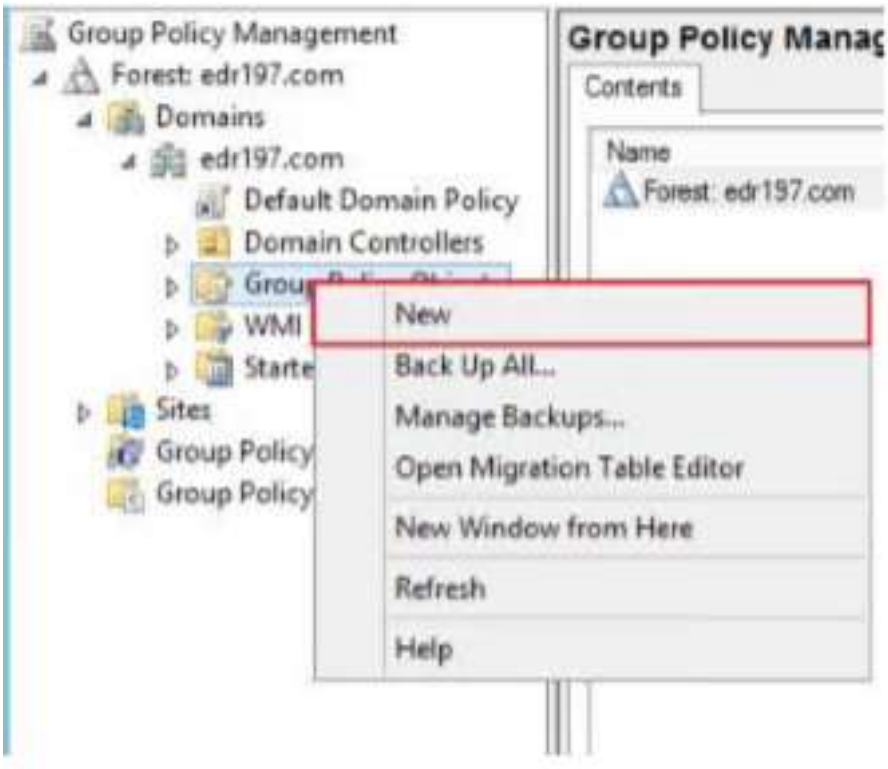


The name of the downloaded installer contains the **IP address** and the **port** to connect to the NovaGuard manager, as shown in the following figure. Do not change the installer's name. Otherwise, the installation will fail.



Create a group policy object:

Log in to the domain server, open **Group Policy Manager**, and create a **Group Policy Object**, as shown in the following figure.

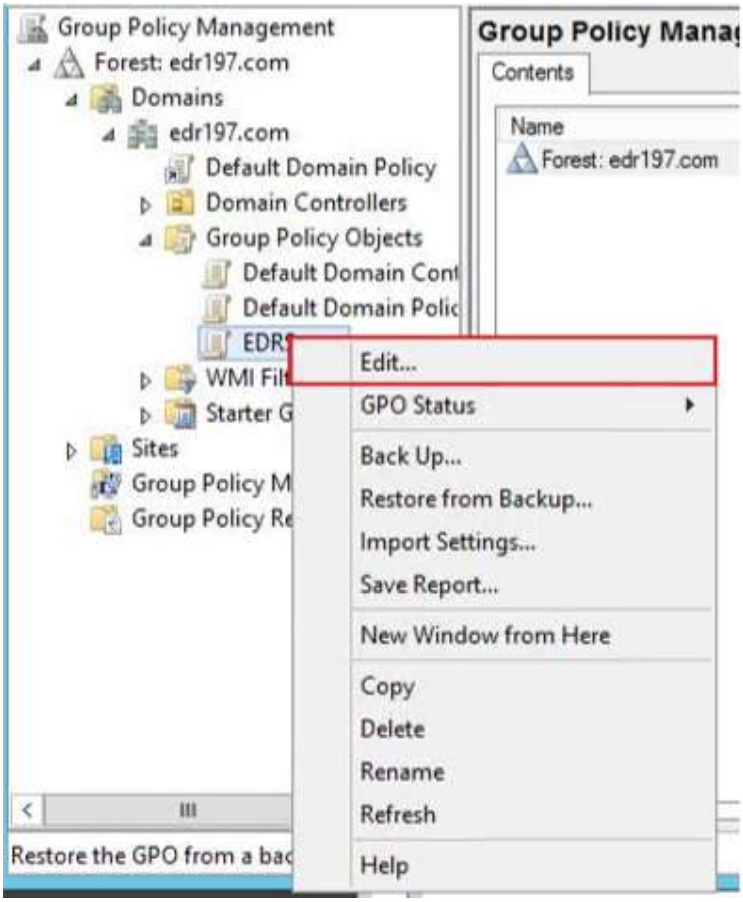


Enter a name for the group policy object and click **OK**.

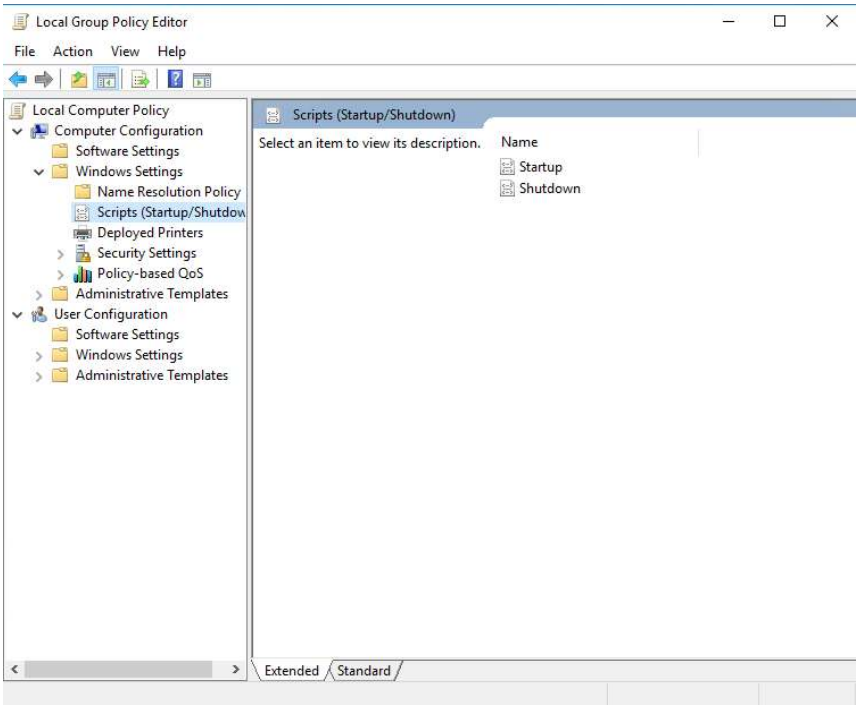


Edit the group policy object

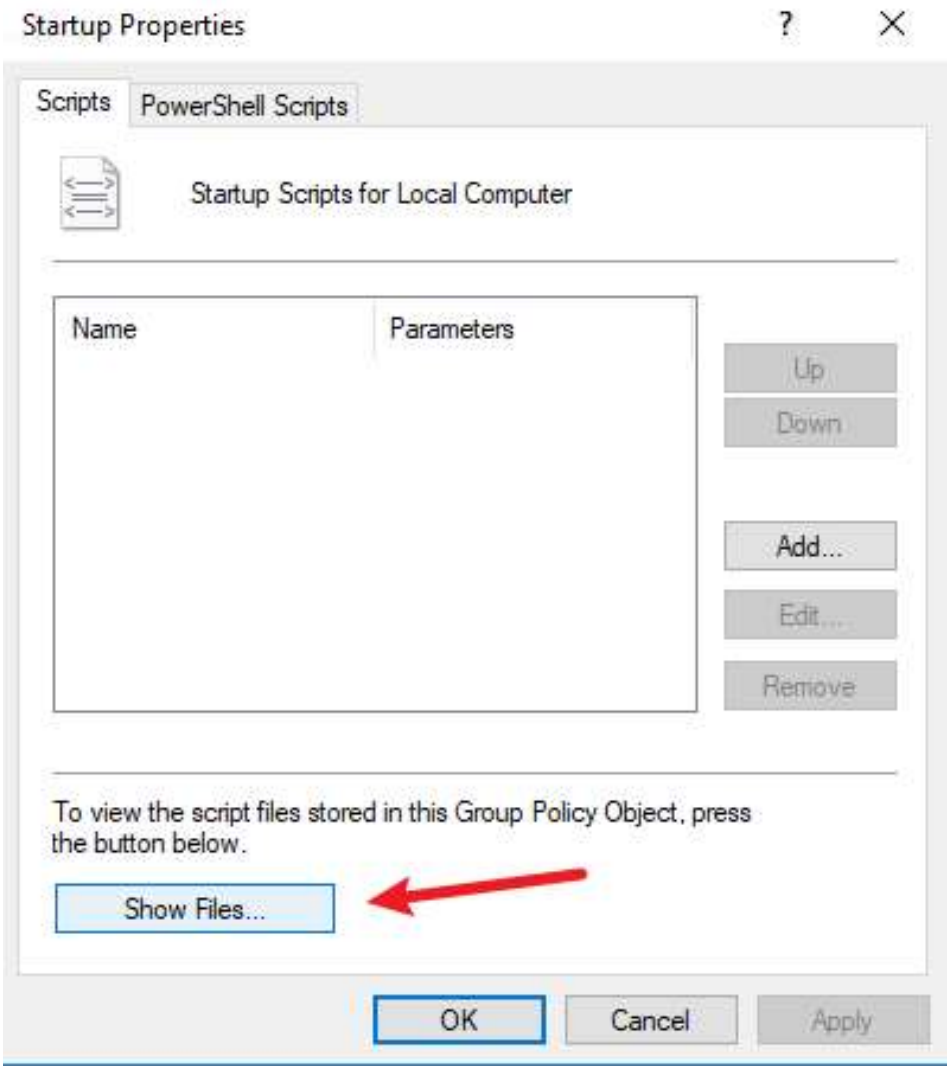
Right-click the newly created group policy object and select **Edit**.



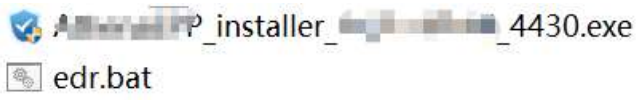
Go to **Computer Configuration** > **Windows Settings** > **Scripts (Startup/Shutdown)** and click **Startup**.



Click **Show Files** to open the startup script directory where the installer and the batch policy distribution script are to be placed, as shown in the following figure.

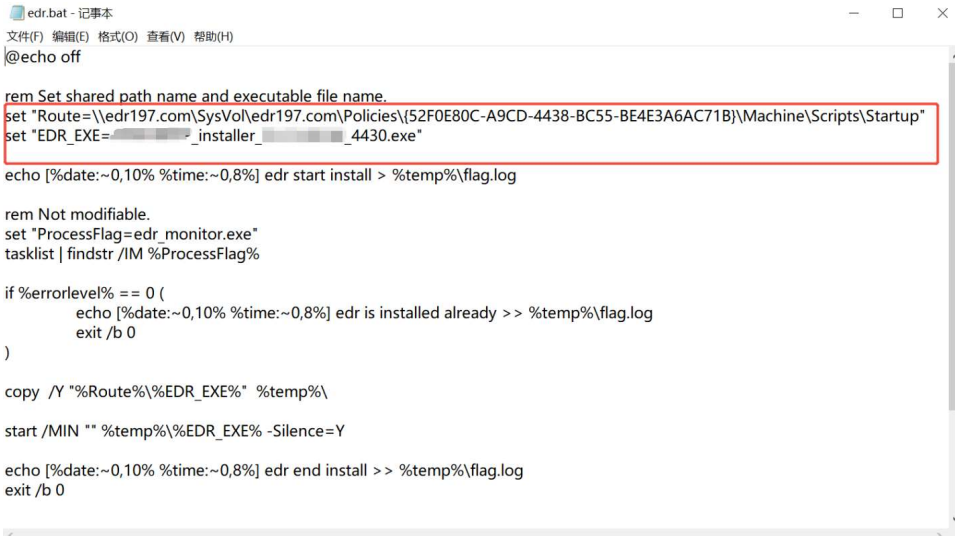


Place the installer and the batch policy distribution script in the startup script directory, as shown in the following figure.



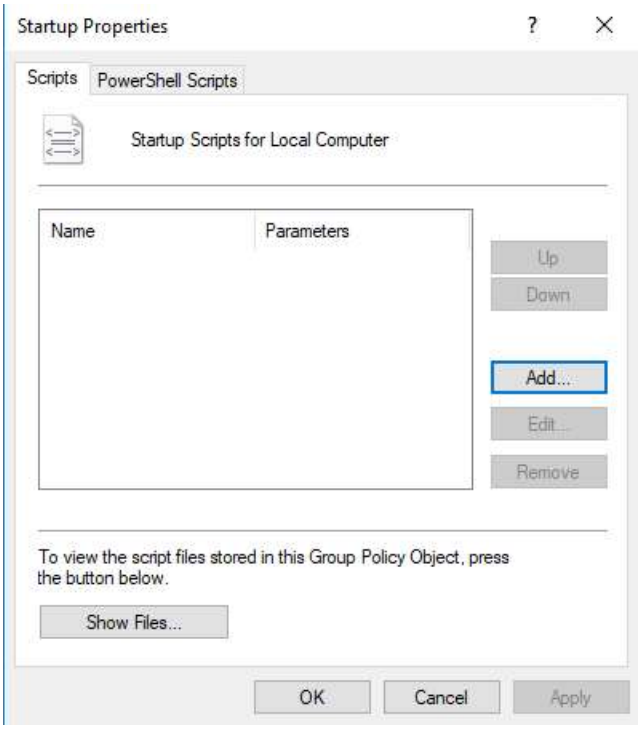
Copy the path to the startup script directory from the address bar for later use in edr.bat modification.

Open **edr.bat** with Notepad++ and make the following changes.

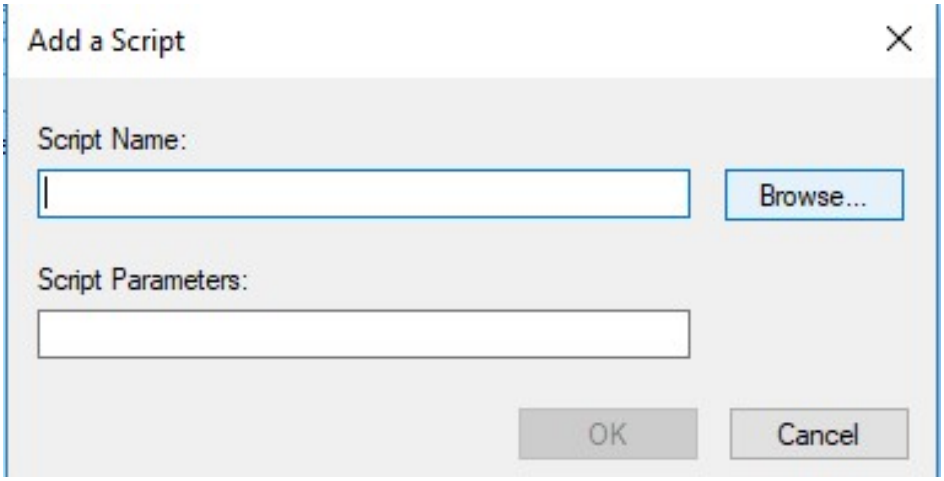


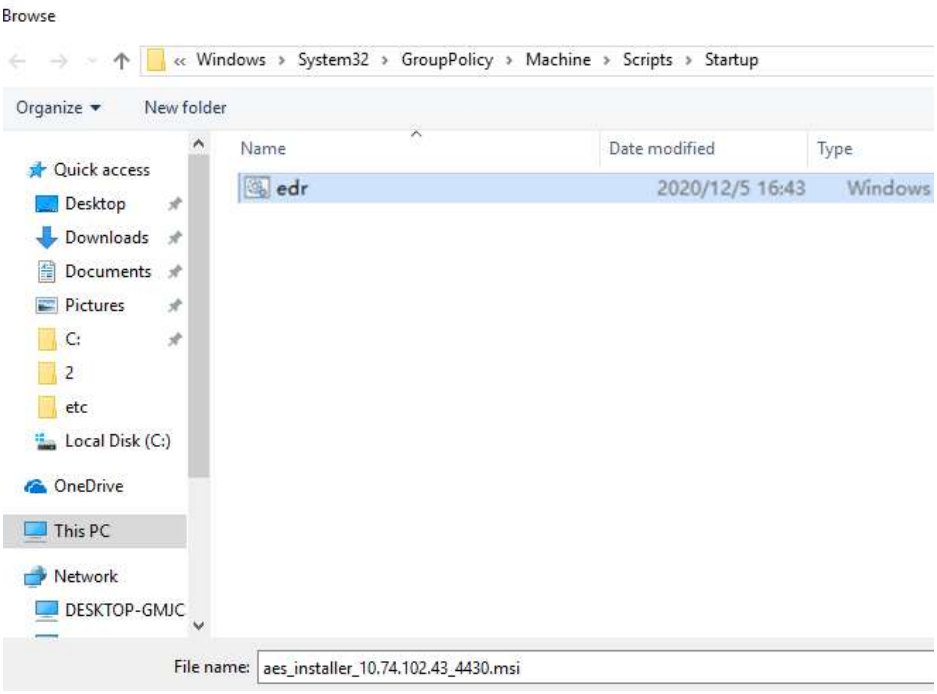
- Change the values of the **Route** and **EDREXE** parameters.
- Set **Route** to the startup script directory where the installer and the batch policy distribution script are stored.
- Set **EDR_EXE** to the installer name.
- Save the changes and close the script.

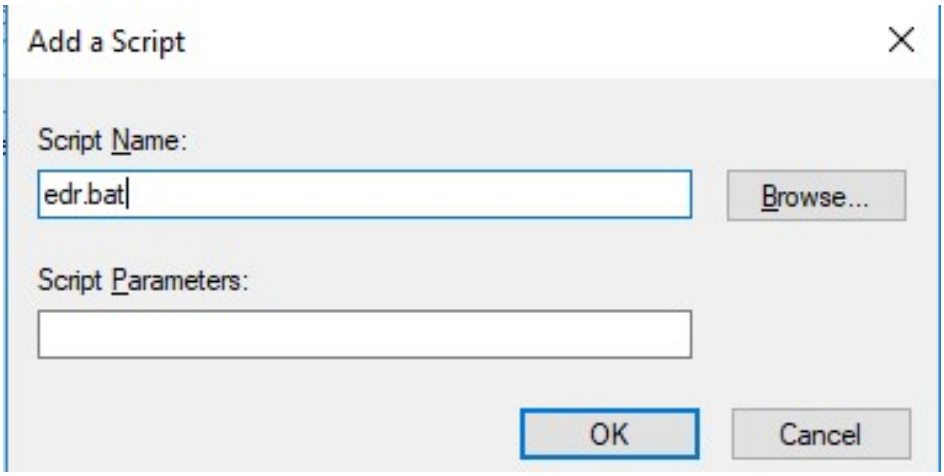
Click **Add...**, as shown in the following figure.



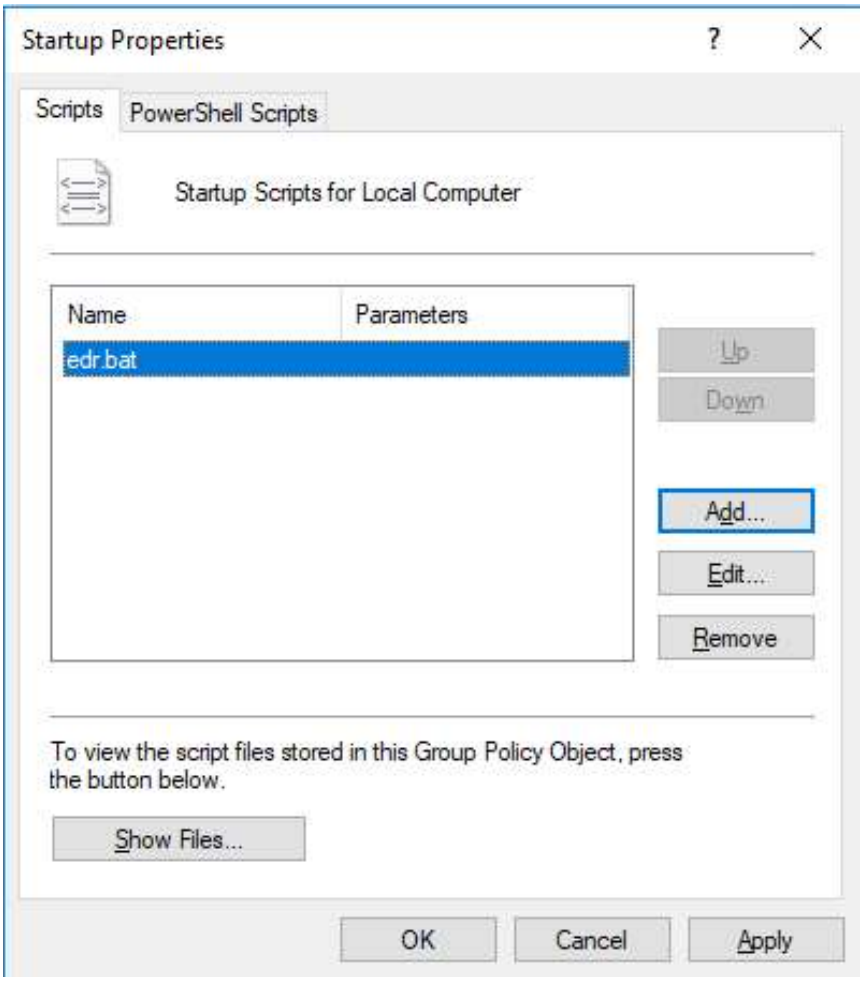
Click **Browse...** to select and add edr.bat.




Browse
« Windows › System32 › GroupPolicy › Machine › Scripts › Startup
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
C:
2
etc
Local Disk (C:)
OneDrive
This PC
Network
DESKTOP-GMJC
Name
Date modified
Type
edr
2020/12/5 16:43
Windows
File name:
aes_installer_10.74.102.43_4430.msi


Add a Script
Script Name:
edr.bat
Browse...
Script Parameters:
OK
Cancel

Click **OK**.



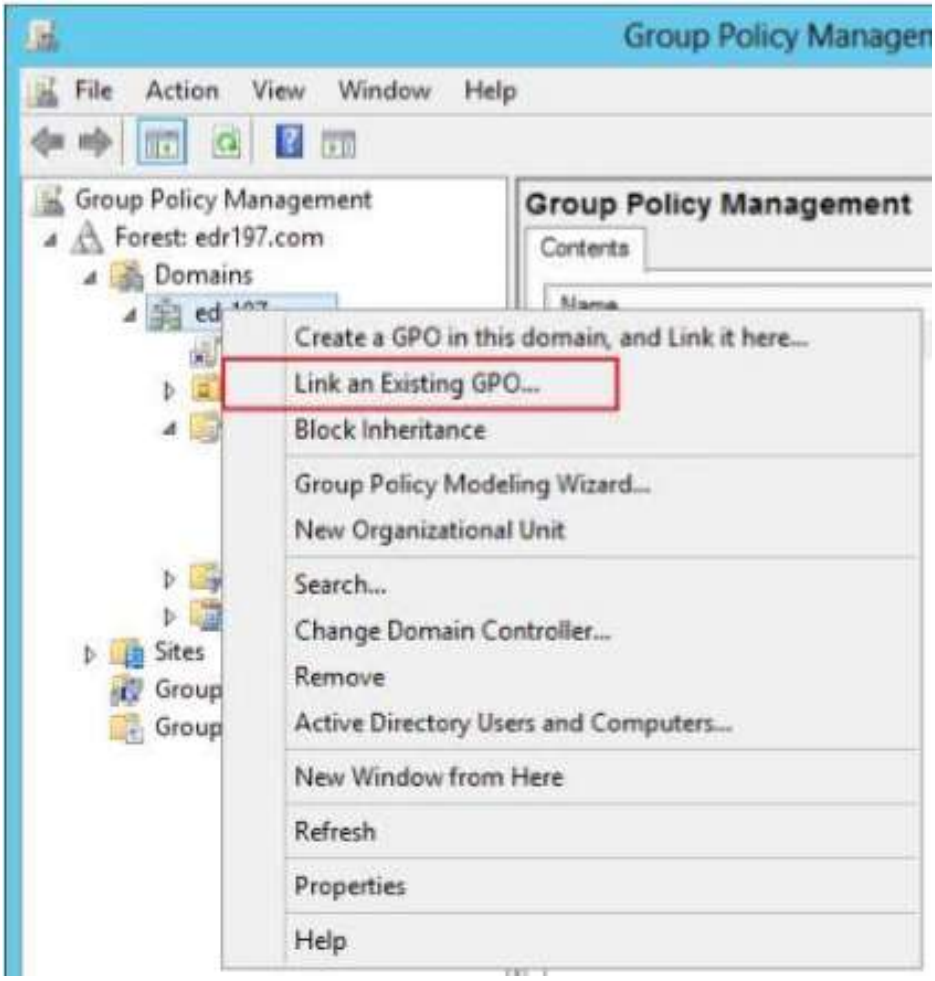
Link the group policy object:

Before applying the group policy to all computers in the domain, link the group policy object to a test organizational unit (OU) for a small-scale test.

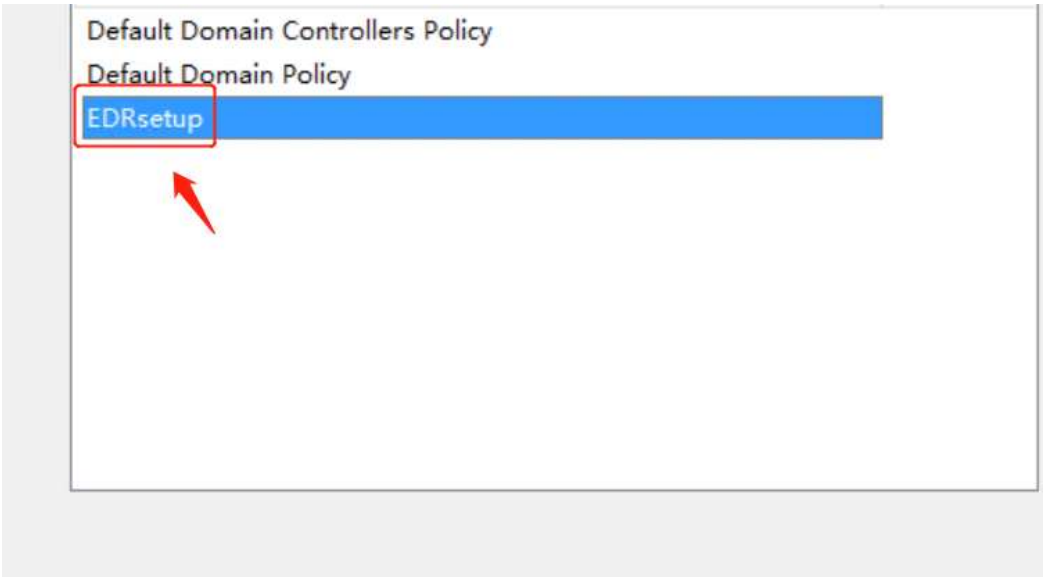
NOTE

The group policy takes effect only if there are computers in the OU. The group policy does not take effect if there are only domain users because it is for **Computer Configuration** rather than **User Configuration**.

For example, you can link the group policy object to the test OU in the domain, as shown in the following figure.

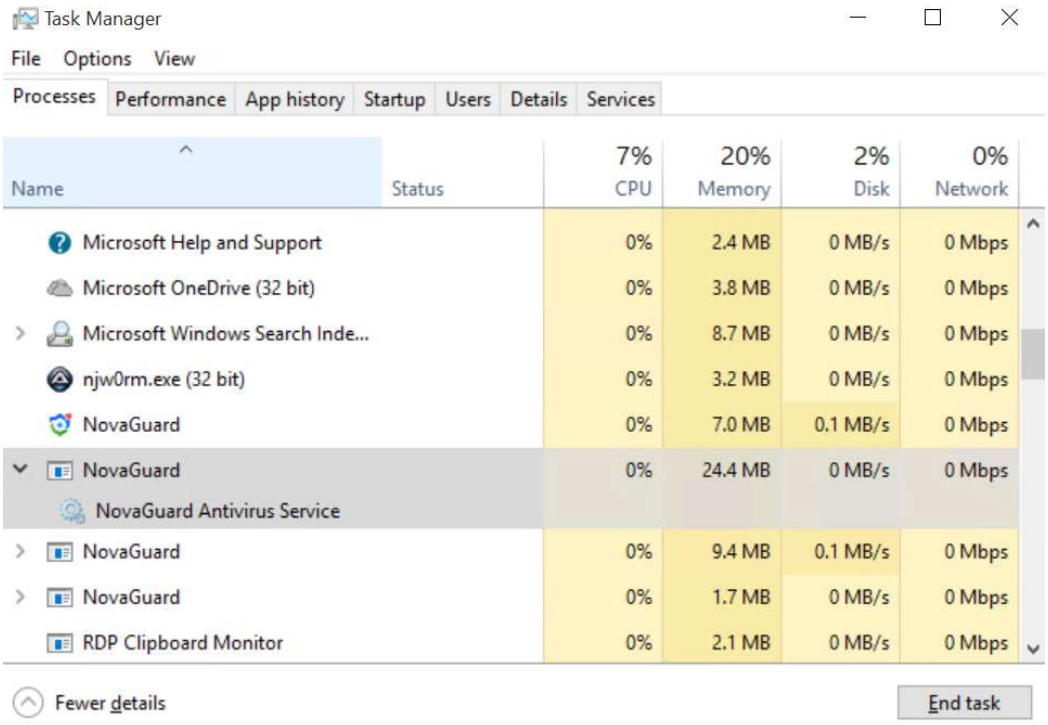


Select the newly created group policy object (such as EDRSetup), and click **OK** to complete the script-based deployment upon endpoint startup.



Verify the installation:

Restart the test endpoint to verify the installation of the NovaGuard agent. The NovaGuard agent is under installation if you find **NovaGuard Antivirus Service** in the endpoint **Task Manager.**

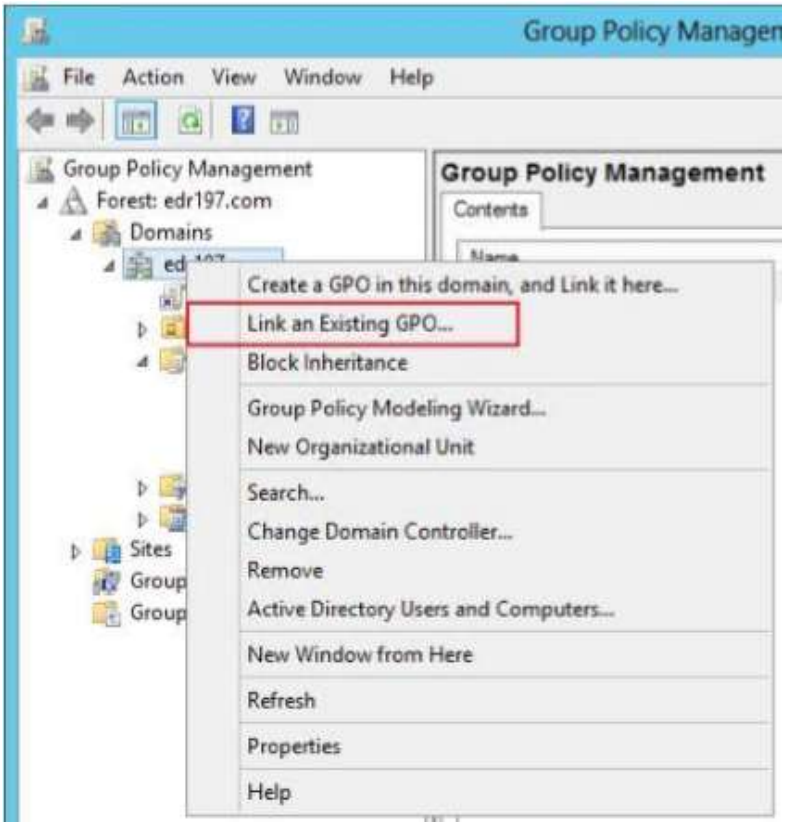


Wait for a few minutes for the installation to finish. Then, you can find the icon of the NovaGuard agent on the screen, as shown in the following figure.



If computers in the test OU can successfully install the NovaGuard agent, link the group policy object to all computers in the domain. To do this, right-click the domain **aES197.com** and select **Link an Existing GPO…**, as shown in the

following figure.



NOTE

1. The group policy takes effect only if computers are in the linked OU. The group policy does not take effect if there are only domain users because it is for **Computer Configuration** rather than **User Configuration**. In this case, a computer automatically obtains the NovaGuard agent installation group policy after it starts up and joins the domain. For a group policy for **User Configuration**, a computer automatically obtains the group policy for NovaGuard agent installation after logging in to the computer using a domain user with the administrator role.

2. During the installation of the NovaGuard agent, necessary components are downloaded from the NovaGuard manager. To avoid excessive bandwidth usage due to bulk installation and ensure stability, limit the number of endpoints per bulk on which the NovaGuard agent is to be installed.

If the bandwidth is 100 Mbit/s (12.5 Mbit/s) and the maximum download bandwidth for each endpoint is 2 Mbit/s, limit the number of endpoints per bulk to 5, with a reserved bandwidth of 0.5 Mbit/s.

If the bandwidth is 1,000 Mbit/s (125 Mbit/s) and the maximum download bandwidth for each endpoint is 2 Mbit/s, limit the number of endpoints per bulk to 60, with a reserved bandwidth of 5 Mbit/s.

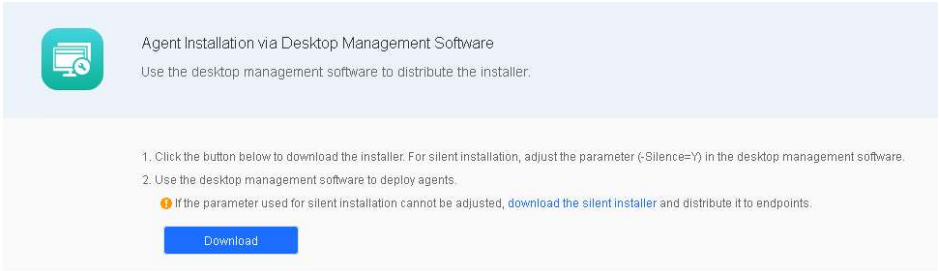
3. A computer with the NovaGuard agent installed will not undergo another installation when restarted.

2.3.2.5 Installation via Desktop Management Software

In scenarios where you have desktop management software that supports software distribution, you can distribute the NovaGuard agent via desktop management software for bulk installation.

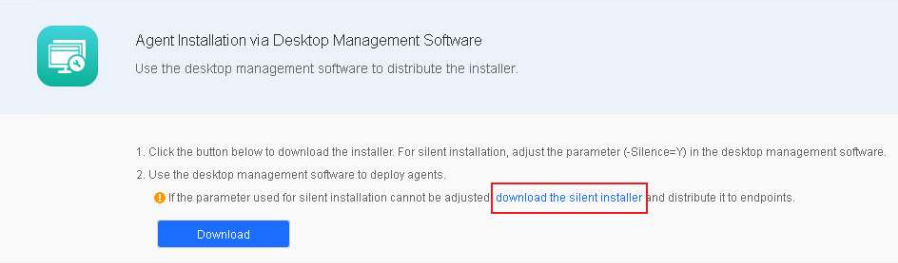
Scenario 1: Desktop management software for bulk installation supports the silence parameter.

In this scenario, you can download the standard NovaGuard agent installer and set the silence parameter (-Silence=Y) for bulk installation. Go to **System** > **Agent Deployment** > **Agent Download**, select **Windows**, click **Agent Installation via Desktop Management Software** in **Bulk Deployment**, and click **Download**, as shown in the following figure.



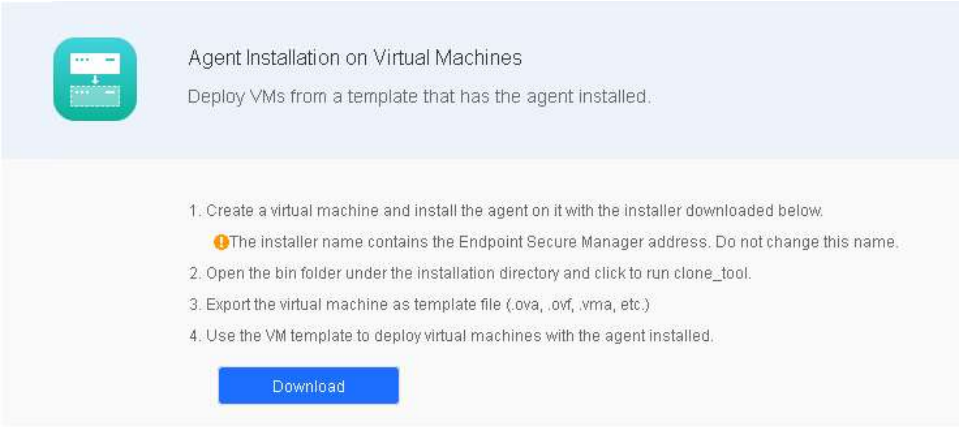
Scenario 2: Desktop management software for bulk installation does not support the silence parameter.

In this scenario, you must download the silent NovaGuard agent installer for Windows for bulk installation. Go to **System** > **Agent Deployment** > **Agent Download**, select **Windows**, click **Agent Installation via Desktop Management Software** in **Bulk Deployment**, and click **download the silent installer**, as shown in the following figure.

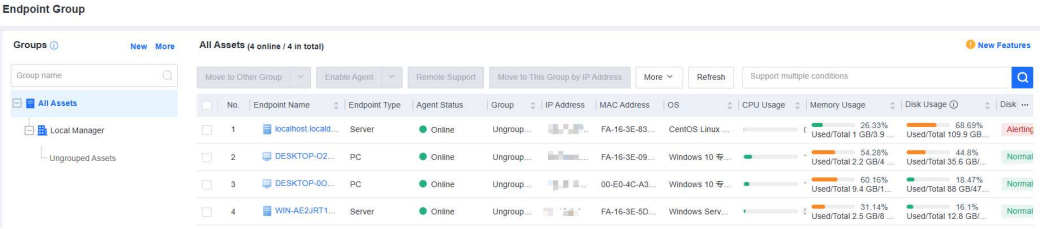


2.3.2.6 Installation on Virtual Machines

In virtualization environments, administrators can convert a virtual machine with NovaGuard agent installed into a template and create virtual machines in bulk. Go to **System** > **Agent Deployment** > **Agent Download**, select **Windows**, and click **Agent Installation on Virtual Machines** in **Bulk Deployment**, as shown in the following figure.



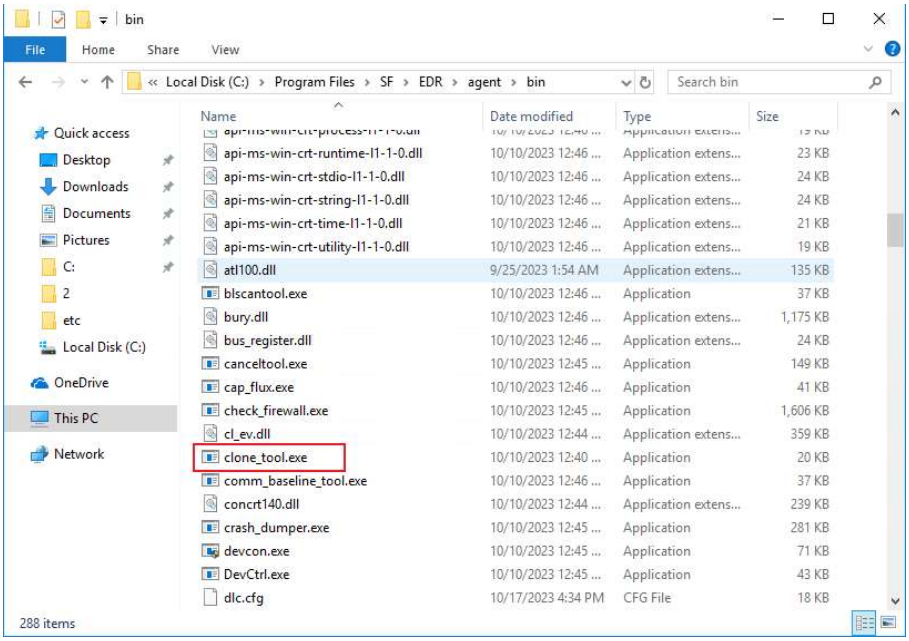
Step 1. Download the installer for standard installation following the instructions in Section 2.4.2.1. The endpoint will go online once the installation is complete.



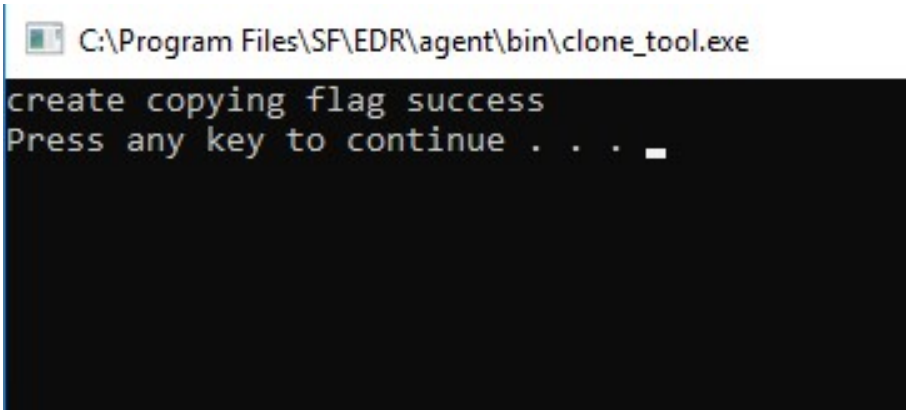
Step 2. Before exporting a virtual machine, right-click **clone_tool.exe** under the "**xxx/bin/"** NovaGuard agent installation directory and execute it as an administrator to ensure that the NovaGuard agent IDs of the created virtual

machines are unique.

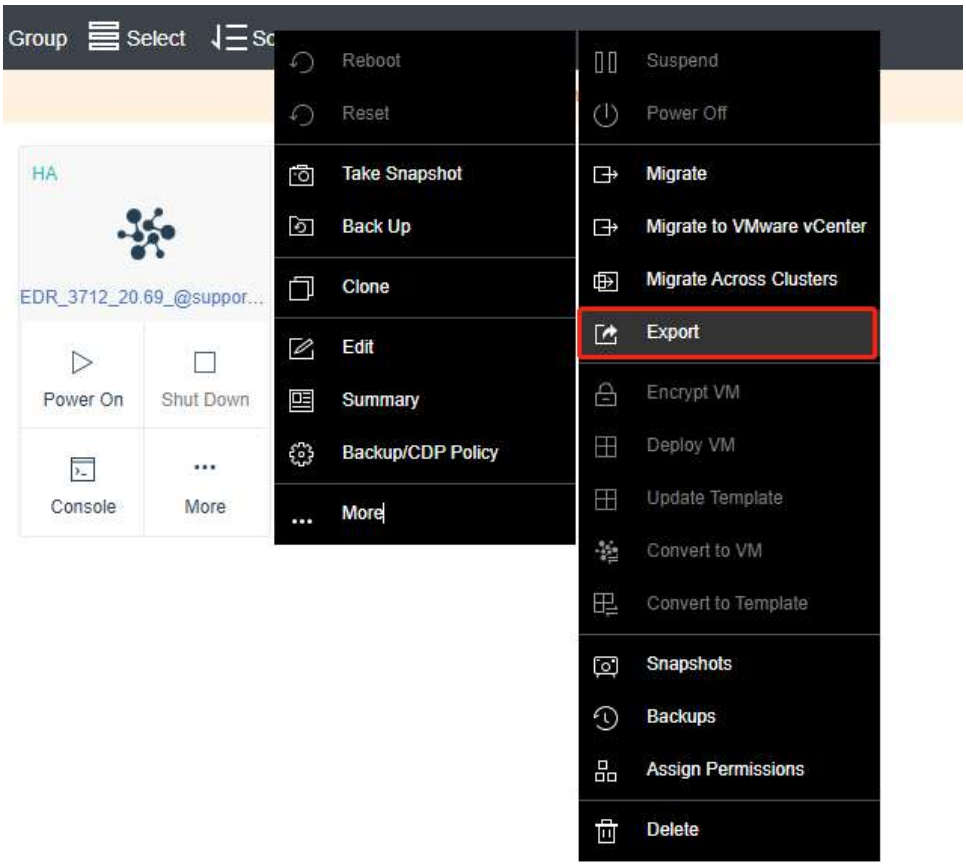
Find the tool, and it is in "**C:/Program Files/SF/EDR/agent/bin**" by default.



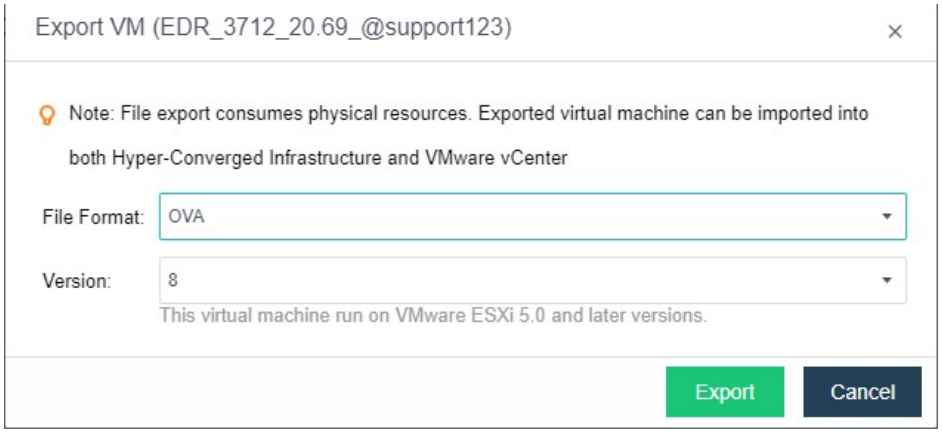
Right-click **clone_tool.exe** to execute it as an administrator and wait for the prompt "**create copying flag success**" to appear.



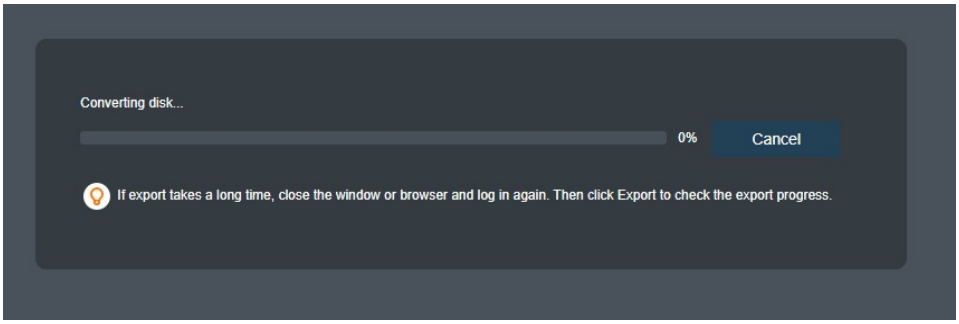
Step 3. Export the virtual machine. The following steps use ForeNova HCI as an example.



Step 4. Select a **File Format**. OVA is recommended.



Once the OVA file is exported, you can use it to create virtual machines with NovaGuard agent installed in bulk.

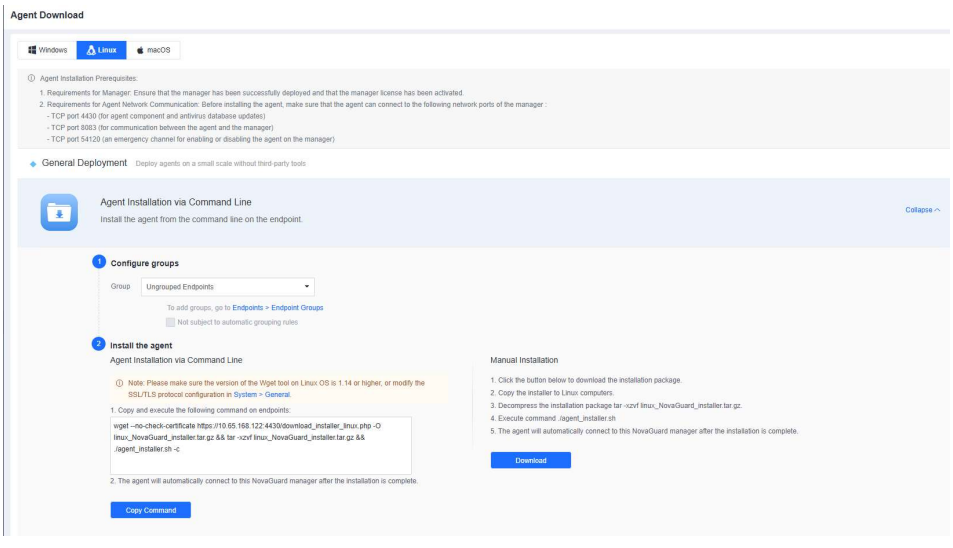


2.3.3 Deployment on Linux

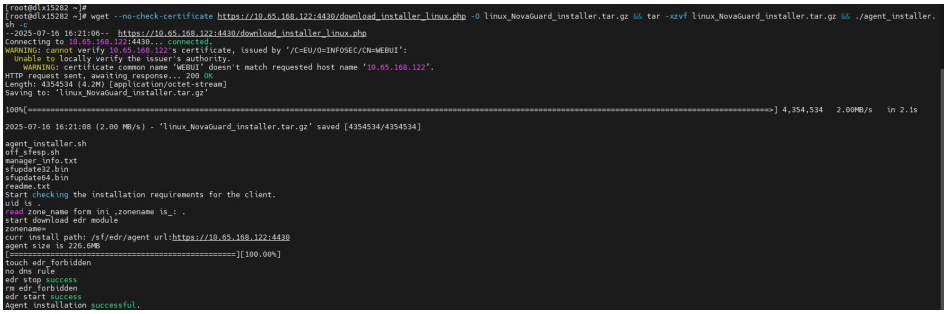
You can deploy NovaGuard agents on Linux on a small or large scale. The small-scale deployment methods include installation via the command line, manual installation, installation on physical machines (full offline installer), and redirection to the NovaGuard agent installer download page. Large-scale deployment methods include installation via the Linux bulk deployment tool and installation on virtual machines.

2.3.3.1 Installation via the Command Line

In small-scale deployment scenarios, you can obtain the installation command and run it on an endpoint for automatic deployment. Go to **System** > **Agent Deployment** > **Agent Download**, and select **Linux**, as shown in the following figure.



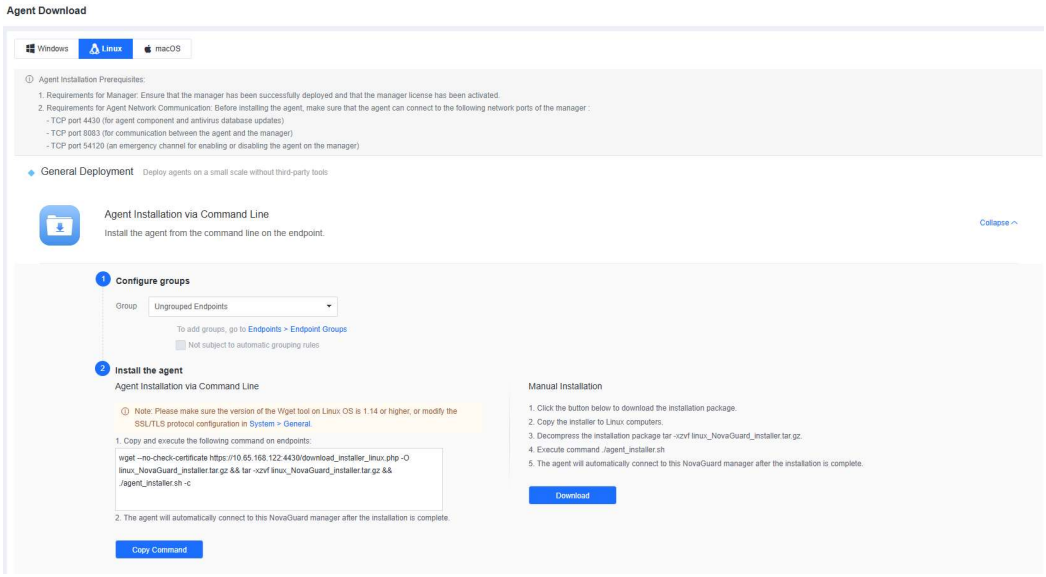
Click **Agent Installation via Command Line**, click **Copy Command**, and run the command on the endpoint, as shown in the following figure.



2.3.3.2 Manual Installation

Download the NovaGuard agent installer to your local device, upload the installer to the endpoint, and run the installation command.

Go to **System** > **Agent Deployment** > **Agent Download**, and select **Linux**, as shown in the following figure.

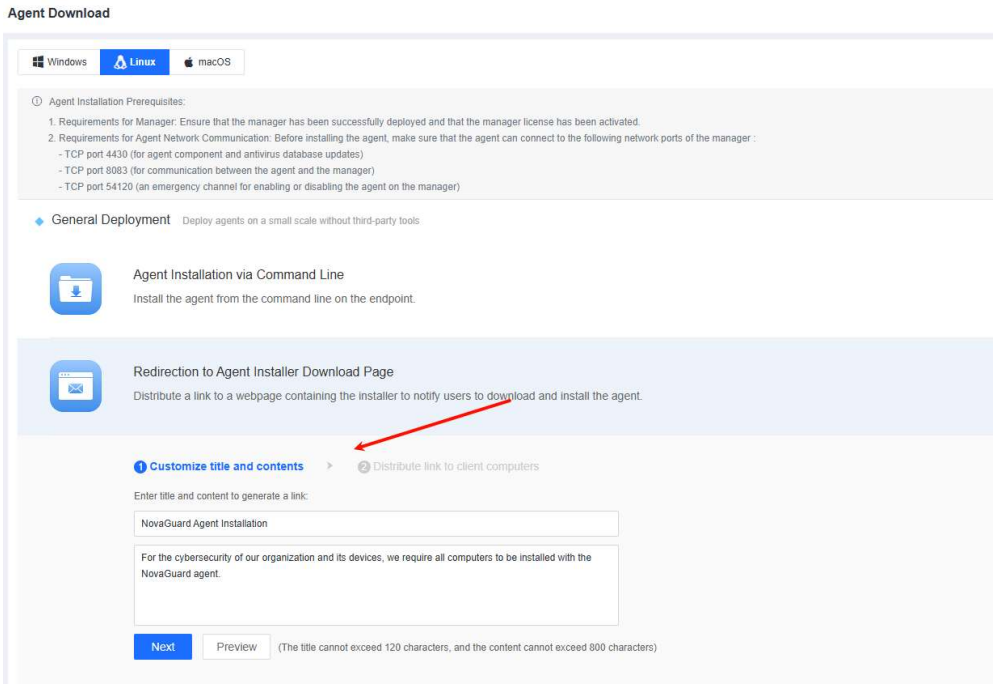


1. Click **Download** under **Manual Installation** to download the installer.
2. Copy the installer to the Linux endpoint.
3. Run **tar -xzvf linux_NovaGuard.tar.gz** to decompress the installer.
4. Run **./agent_installer.sh** to start the installation.
5. Wait for the installation to complete. Then, the NovaGuard agent on the endpoint will automatically connect to the NovaGuard manager.

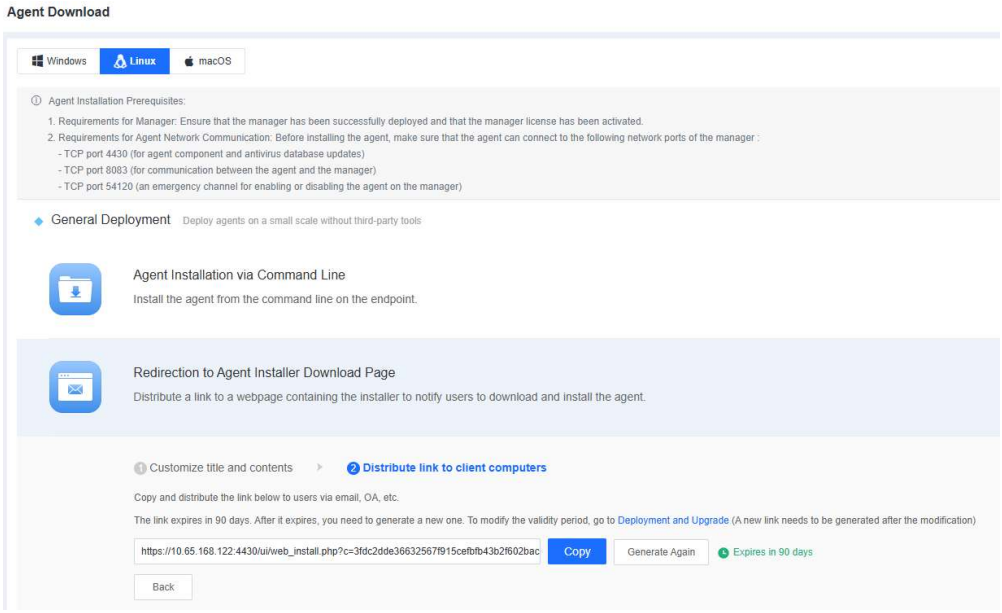
2.3.3.3 Redirection to the Agent Installer Download Page

Administrators can distribute a link to the installer download webpage to user endpoints via channels such as email and OA to remind users to download and install the NovaGuard agent.

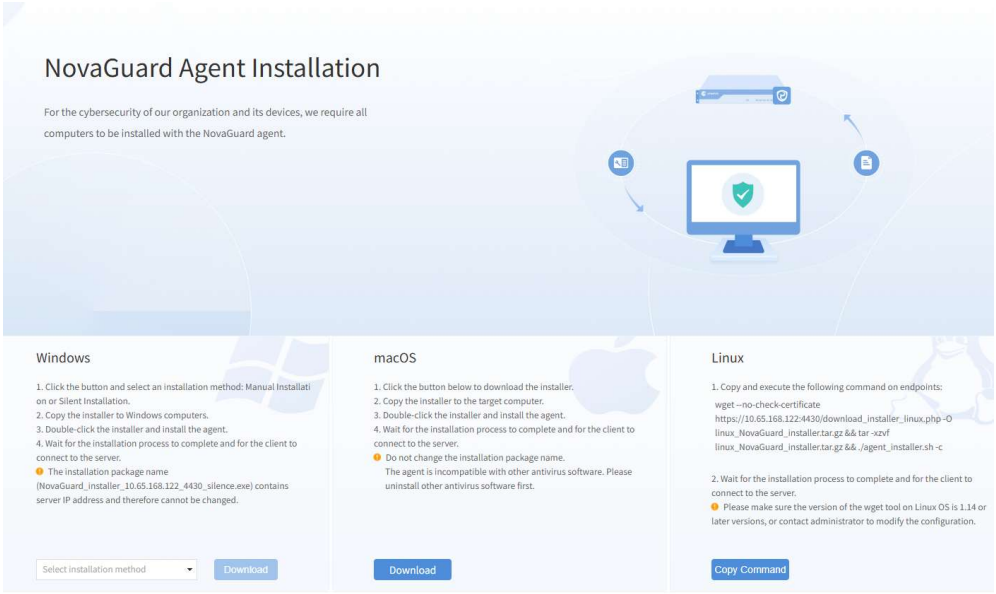
Go to **System** > **Agent Deployment** > **Agent Download**, select **Linux**, and then select **Redirection to Agent Installer Download Page** in **General Deployment**, as shown in the following figure.



Enter a title and the content on the **Customize title and contents** page and click **Next** to generate a link, as shown in the following figure.



Distribute the link to endpoints as an administrator via email, OA, or other channels for users to download and install the NovaGuard agent, as shown in the following figure.



2.3.3.4 Installation via the Linux Bulk Deployment Tool

1. Introduction to the tool

ForeNova provides a tool that connects to Linux servers in bulk using the SSH protocol for automatic installer download from the NovaGuard manager and bulk NovaGuard agent deployment on Linux.

2. **The operating environment for the tool**

   a) Windows

3. **Requirements:**

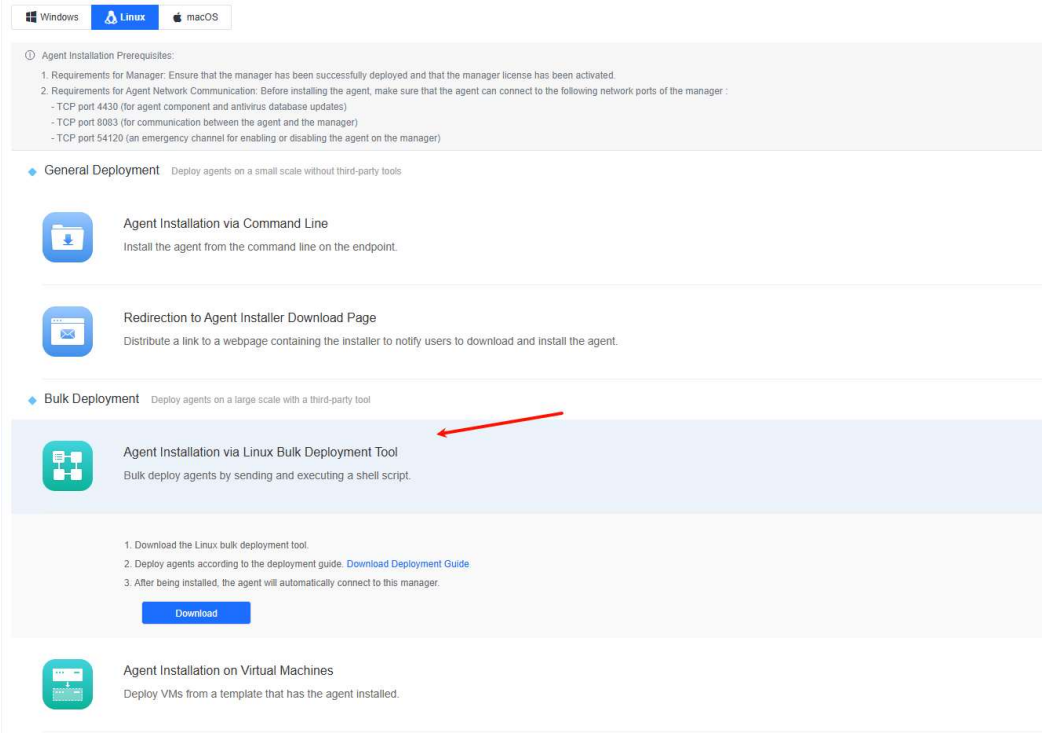
   a) Collect the root account usernames and passwords of all Linux servers in advance.

   b) The Windows PC that hosts the tool can connect to the Linux servers where the NovaGuard agent is to be installed via the SSH protocol.

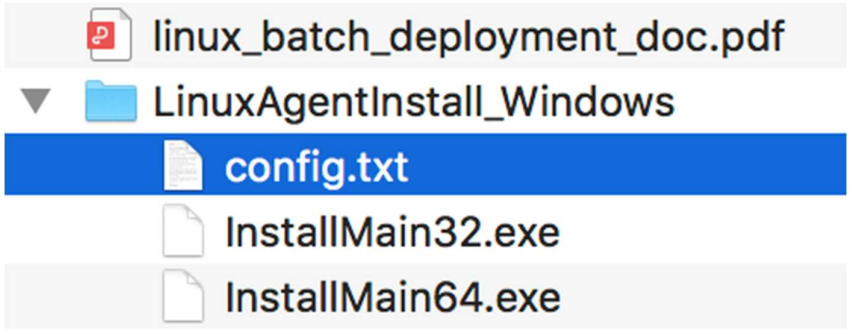
4. **Procedure:**

   a) Download the tool.

   Go to **System** > **Agent Deployment** > **Agent Download**, select **Linux**, click **Agent Installation via Linux Bulk Deployment Tool** in **Bulk Deployment**, and click **Download** and **Download Deployment Guide**, as shown in the following figure.

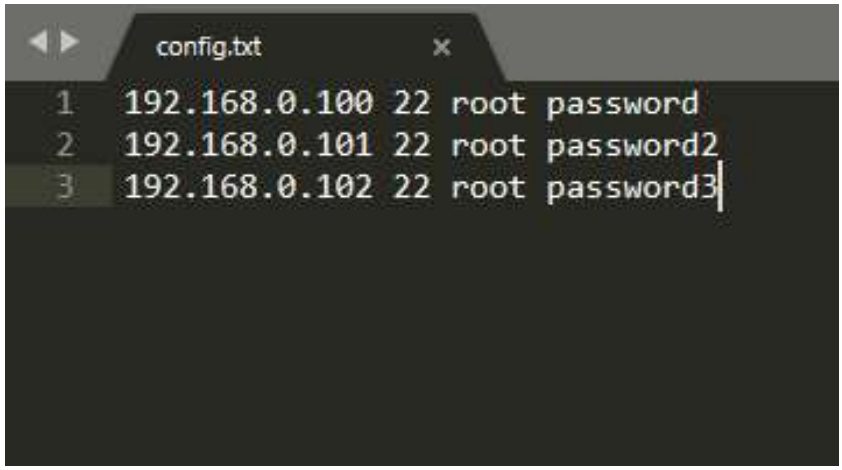


   b) As shown in the following figure, the tool consists of a configuration file named **config.txt** and two main programs named **InstallMain32.exe** and **InstallMain64.exe** that run on 32-bit Windows and 64-bit Windows.



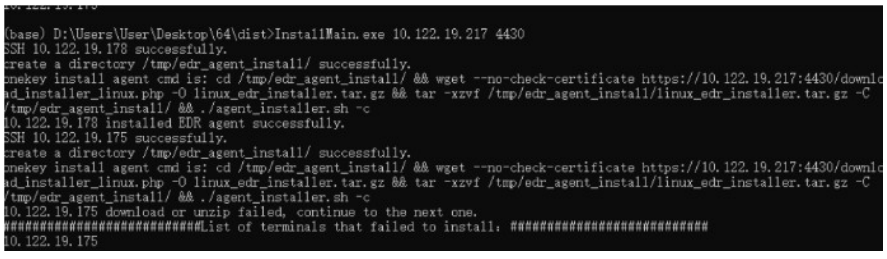
c) Edit the configuration file.

Add the collected root account usernames and passwords of the Linux servers where the NovaGuard agent is to be installed to **config.txt** in the format of "**Linux_IP SSH_port username password**", as shown in the following figure.



d) Run the tool.

Run **InstallMain64.exe** or **InstallMain32.exe**. For example, to run **InstallMain64.exe**, execute "**InstallMain64.exe [Manager IP]**", as shown in the following figure.



e) Verify the installation.

Wait for 10 to 30 minutes for the installation to finish. The installation

duration varies with the number of endpoints where the NovaGuard agent is being concurrently installed. Once the NovaGuard agent is installed successfully, you can find the online Linux servers on the **Endpoint** > **Endpoint Groups** page of the NovaGuard manager.

NOTE

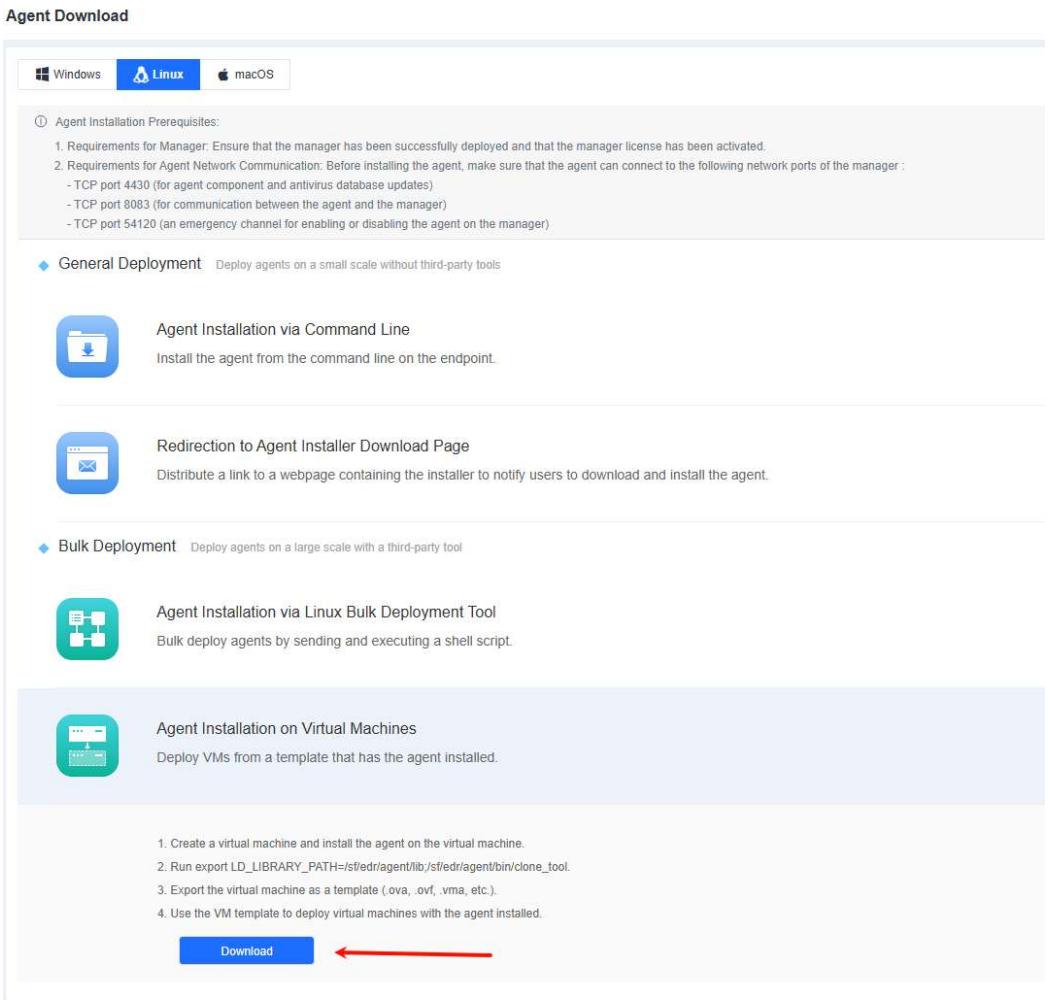
1. Put the configuration file and InstallMain64.exe in the same directory, and keep the configuration file name to "**config**.**txt**".

2. During the bulk installation via the deployment tool, Linux servers will download the NovaGuard agent installer from NovaGuard manager. Limit the number of endpoints to avoid excessive bandwidth usage due to bulk installation and ensure stability. If the bandwidth is 100 Mbit/s, limit the number of endpoints to 5 in a bulk installation. If the bandwidth is 1,000 Mbit/s, limit the number of endpoints to 60 in a bulk installation.

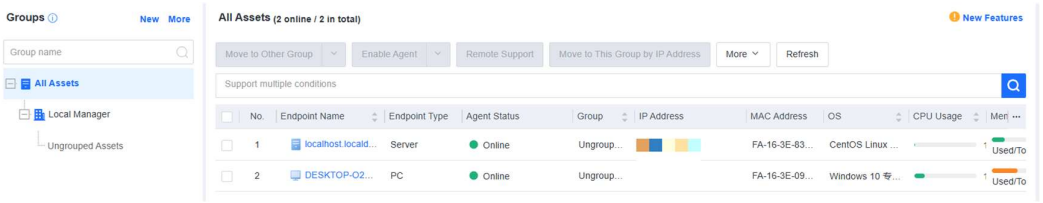
3. After the installation is complete, clear the content of config.txt and delete the file to avoid password leakage.

2.3.3.5 Installation on Virtual Machines

In virtualization environments, administrators can convert a virtual machine with NovaGuard agent installed into a template, from which virtual machines can be created in bulk. Go to **System** > **Agent Deployment** > **Agent Download**, select **Linux**, and click **Agent Installation on Virtual Machines** in **Bulk Deployment**, as shown in the following figure.



Step 1. Download the installer for standard installation following the instructions in Section 2.4.3.1. The endpoint will go online once the installation is complete.



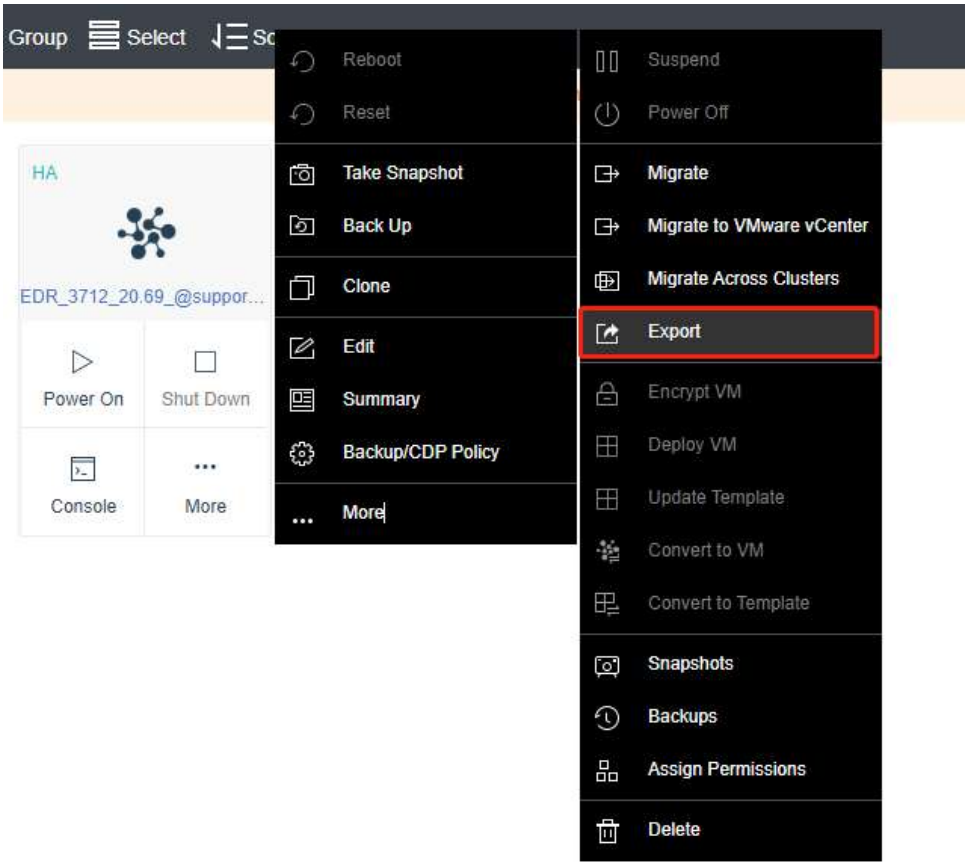
Step 2. Before exporting a virtual machine, run **clone_tool** under the "xxx/bin/" NovaGuard agent installation directory as the super administrator to ensure that the NovaGuard agent IDs of the created virtual machines are unique.

Run **export LD_LIBRARY_PATH=/sf/edr/agent/xs_agent/lib** and **cd /sf/edr/agent/bin/** to go to the installation directory. Then, run **./clone_tool** as the

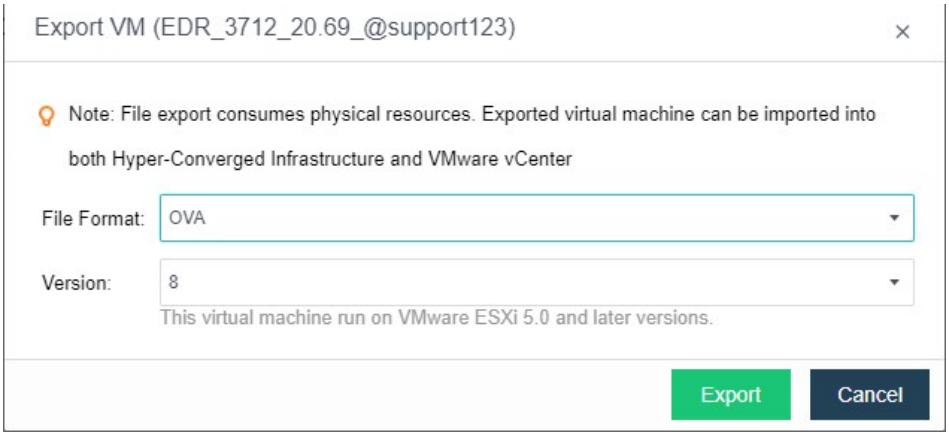
super administrator and wait for the prompt "**create copying flag success**" to appear.



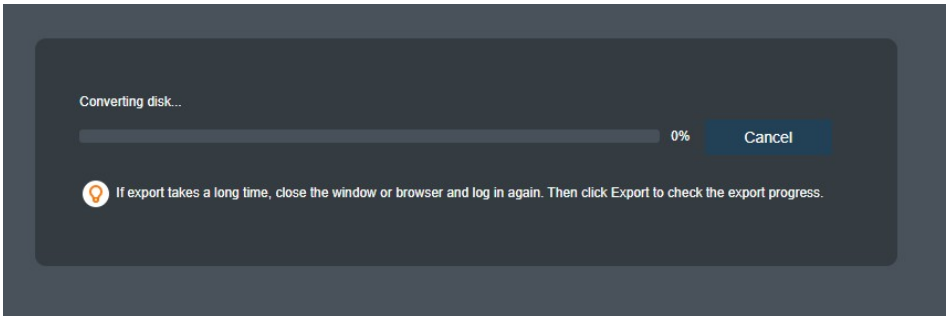
Step 3. Export the virtual machine. In this example, we will use the ForeNova HCI for demonstration.



Step 4. Select a file format. OVA is recommended.



Step 5. Once the OVA file is exported, you can use it to create virtual machines with NovaGuard agent installed.



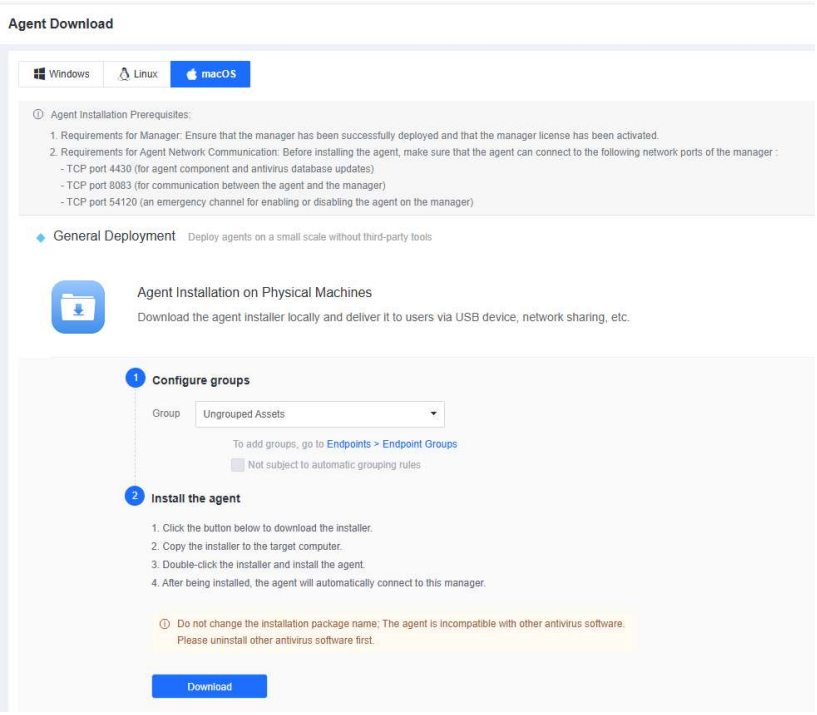
2.3.4 Deployment on macOS

You can install the NovaGuard agent on macOS in two ways: installation on physical machines and redirection to the NovaGuard agent installer download page.

2.3.4.1 Installation on Physical Machines

Administrators can download the NovaGuard agent installer locally and deliver it to users via portable devices and network sharing.

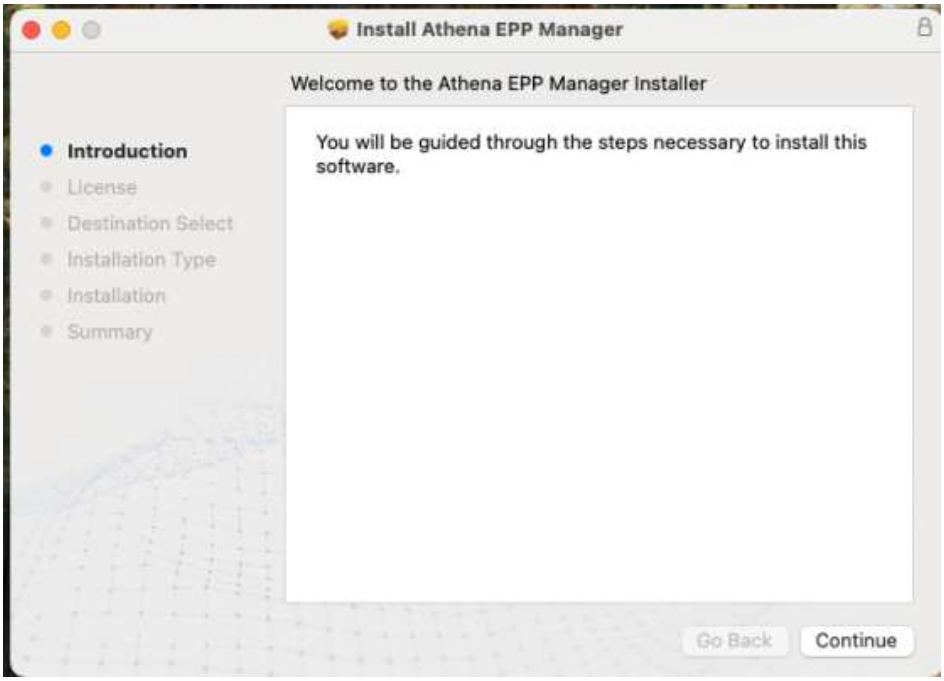
Go to **System** > **Agent Deployment** > **Agent Download**, select **Mac**, and click **Agent Installation on Physical Machines** > **Download**, as shown in the following figure.

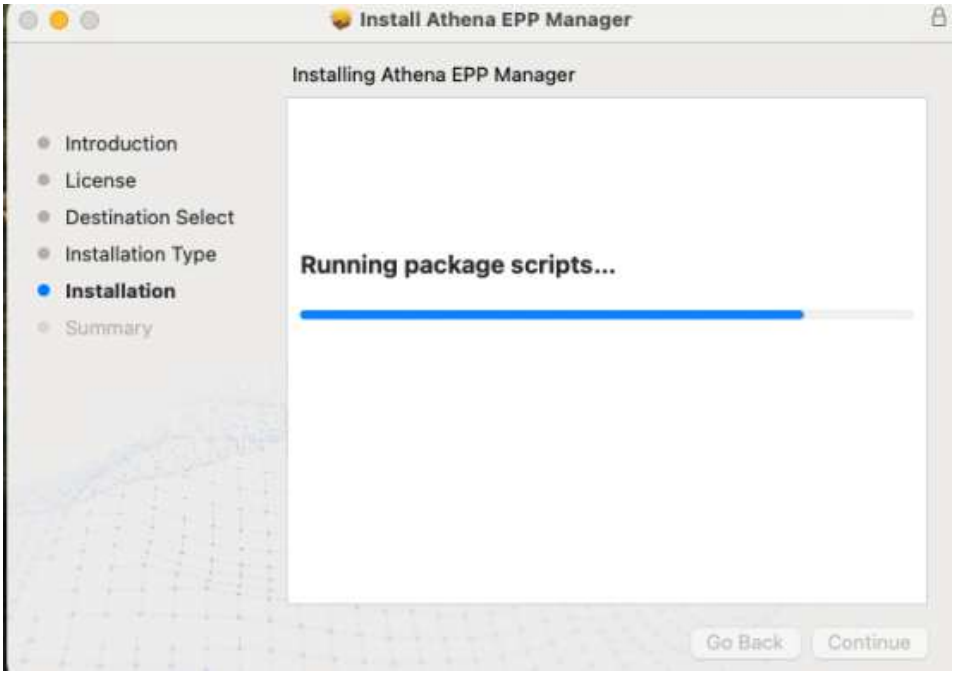


NOTE

The name of the installation package for macOS (**NovaGuard_[Manager IP]_4430.exe**) contains the NovaGuard manager IP address. Do not change the installer's name.

Double-click the installer and follow the wizard's prompts, as shown in the following figure.





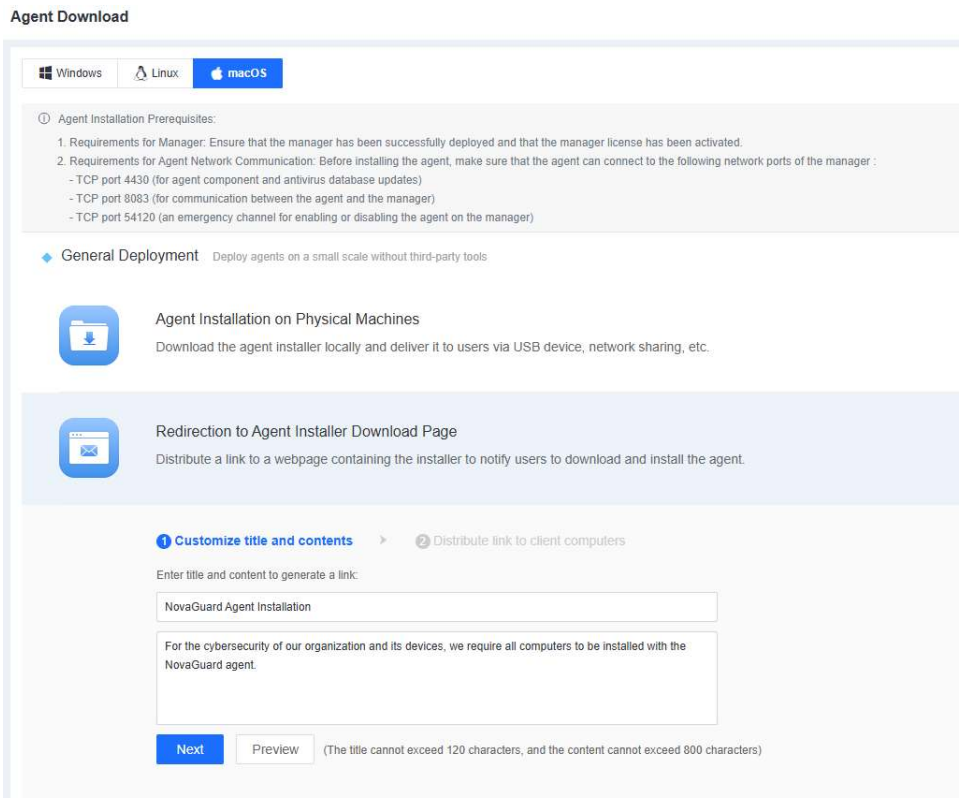
After the installation, you can find the icon of the NovaGuard agent in the macOS menu bar, as shown in the following figure.



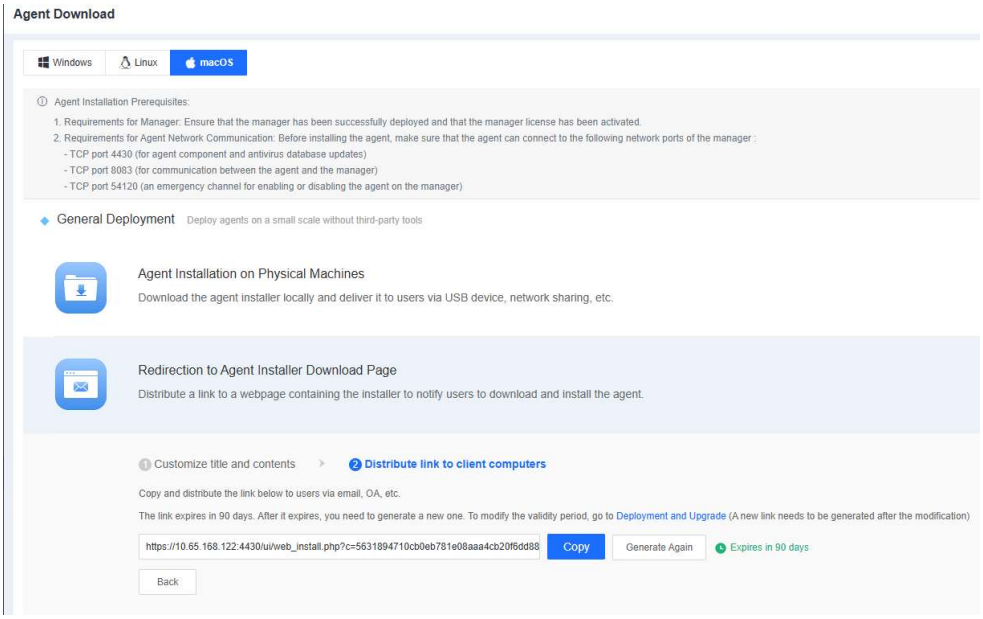
2.3.4.2 Redirection to the Agent Installer Download Page

Administrators can distribute a link to the installer download webpage to user endpoints via channels such as email and OA to the users to download and install the NovaGuard agent.

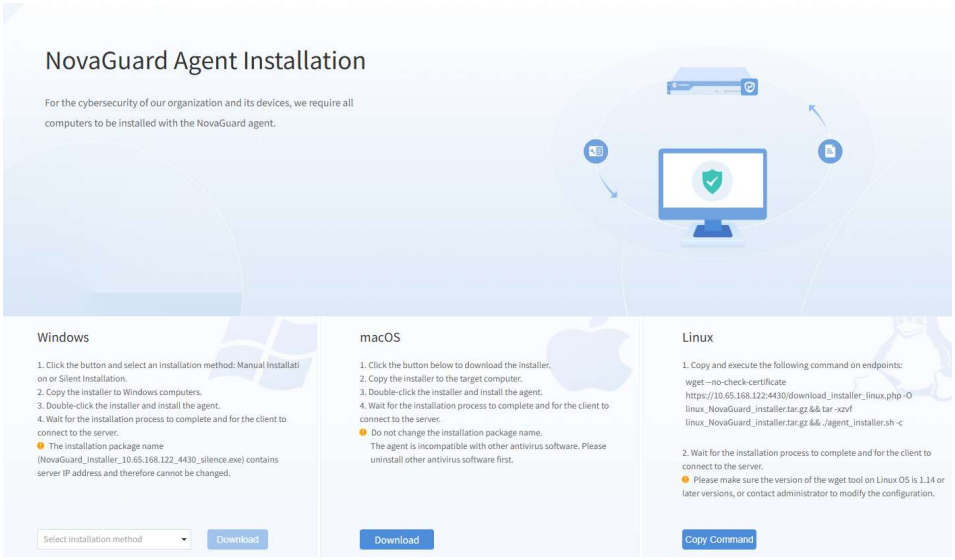
Go to **System** > **Agent Deployment** > **Agent Download**, select **Mac**, and click **Redirection to Agent Installer Download Page**, as shown in the following figure.



Enter a title and the content on the **Customize title and contents** page and click **Next** to generate a link, as shown in the following figure.



Distribute the link to endpoints as an administrator via email, OA, or other channels for users to download and install the NovaGuard agent, as shown in the following figure.



2.3.5 Pre-installation

Pre-installation refers to a process of installing an operating system and necessary computer components before delivering them to the customer. To reduce the workload, create an image from a computer with the operating

system and essential components and install it on other computers in bulk using that image. The procedure for pre-installing the NovaGuard agent is as follows:

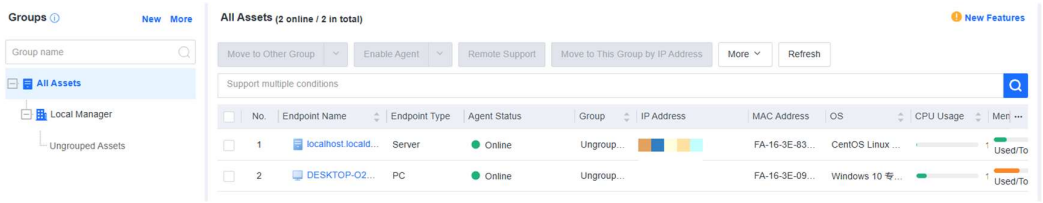
1. Confirm with the customer the IP address to be assigned to the NovaGuard manager. Please note that the IP address cannot be changed.
2. Select an installer compatible with the CPU architecture and operating system of the customer's computers, and replace the IP address in the installer name with the NovaGuard manager IP address, which the customer confirmed in Step 1.
3. Install the NovaGuard agent.
4. Prepare the template environment before exporting a virtual machine. Execute **clone_tool** under the "**xxx/bin/"** NovaGuard agent installation directory as an administrator to ensure that the NovaGuard agent IDs of the created virtual machines are unique. The execution method varies with the operating system of the computer. For details, see Sections 2.4.2.8 and 2.4.3.6 **Installation on Virtual Machines**.
5. Create an image for pre-installation, and pre-install the operating system and necessary components on other computers in bulk by using that image.



Strictly follow the pre-installation procedure. Otherwise, extra work may be required. For example, suppose the operating system and necessary components are pre-installed on computers without confirming the assigned IP address of the NovaGuard manager. In that case, the computers can connect to the NovaGuard manager only after the assigned IP address is specified on each of them.

2.3.6 Verification of Installation

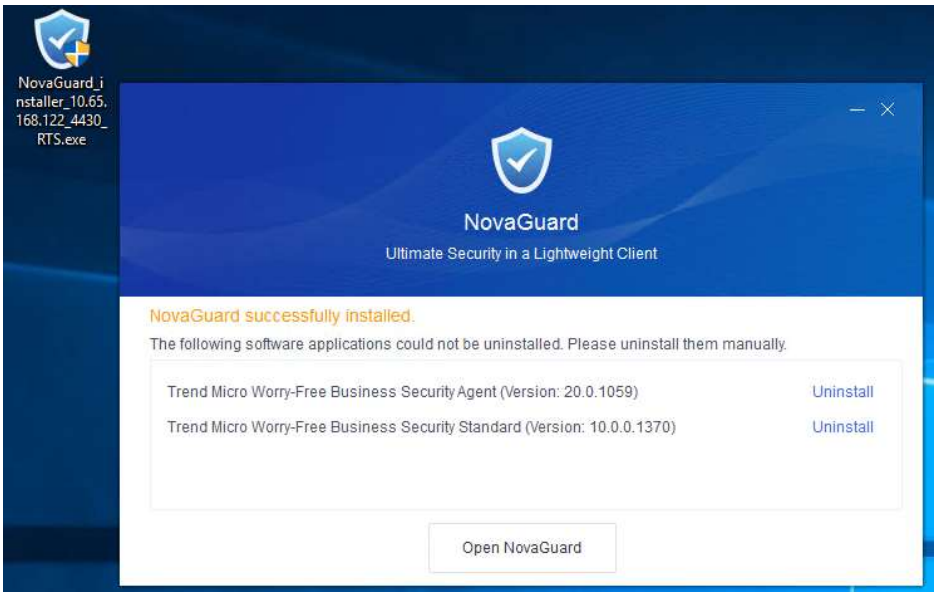
After the installation, the NovaGuard agent will automatically connect to the NovaGuard manager. You can find the online endpoints on the **Endpoint** > **Endpoint Groups** page of the NovaGuard manager, as shown in the following figure.



2.3.7 Uninstallation of Incompatible Third-Party Antivirus Software

When you install the NovaGuard agent on an endpoint, NovaGuard automatically detects and uninstalls third-party antivirus software that is incompatible with the NovaGuard agent on the endpoint during the agent installation process.

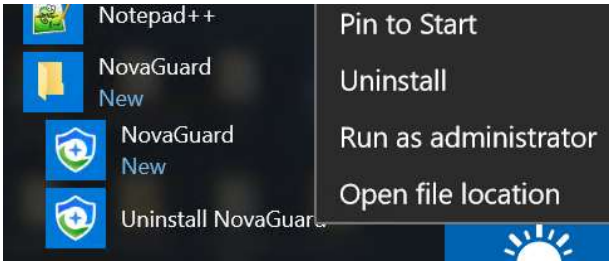
Modify the file name of the agent installation file and add the suffix **_RTS** at the end. It will uninstall the third-party EDR when the agent is installed. Otherwise, it will not uninstall the third-party EDR.



2.4 NovaGuard Agent Uninstallation

2.4.1 Uninstall from a Windows Endpoint

Open the **Start** menu of the Windows endpoint, find the NovaGuard agent, click **Uninstall NovaGuard agent**, right-click the NovaGuard agent, select **Uninstall**, and follow the uninstallation prompts, as shown in the following figure.

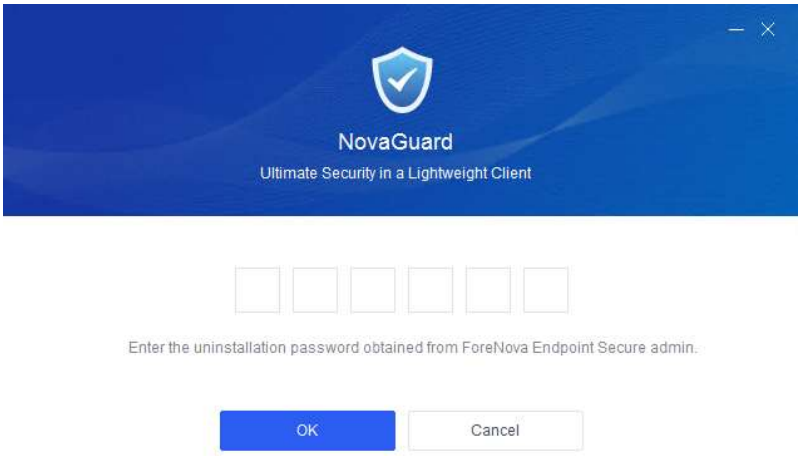


On the uninstallation page that appears, click **Uninstall**.



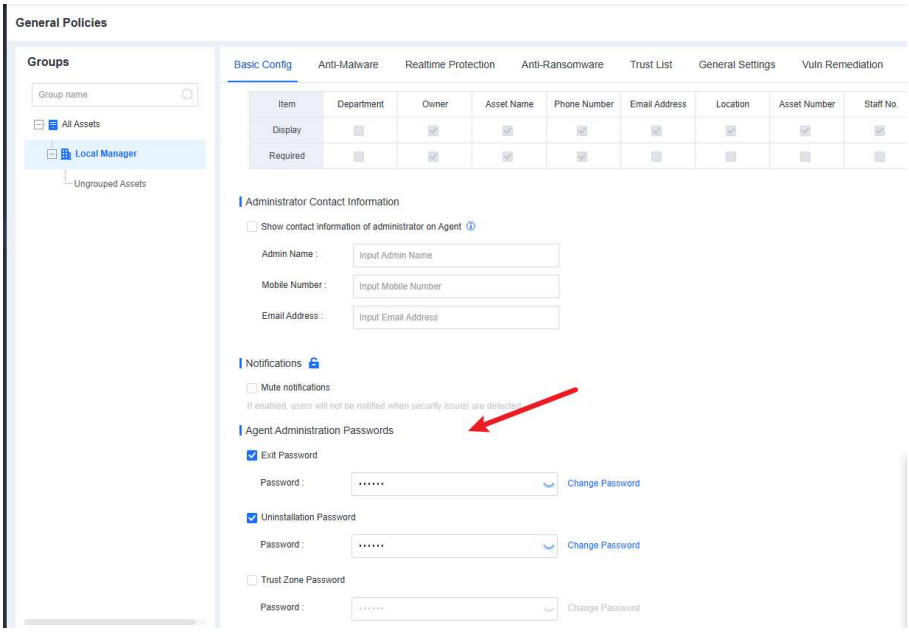


Wait for the following prompt page to appear.

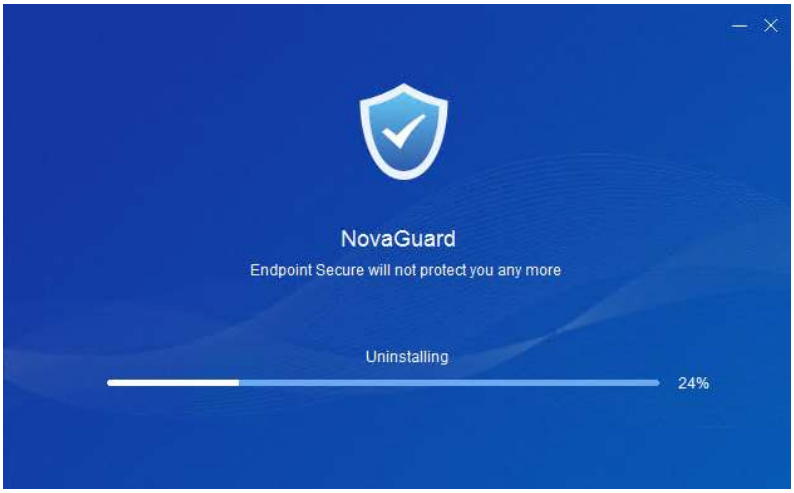


NOTE

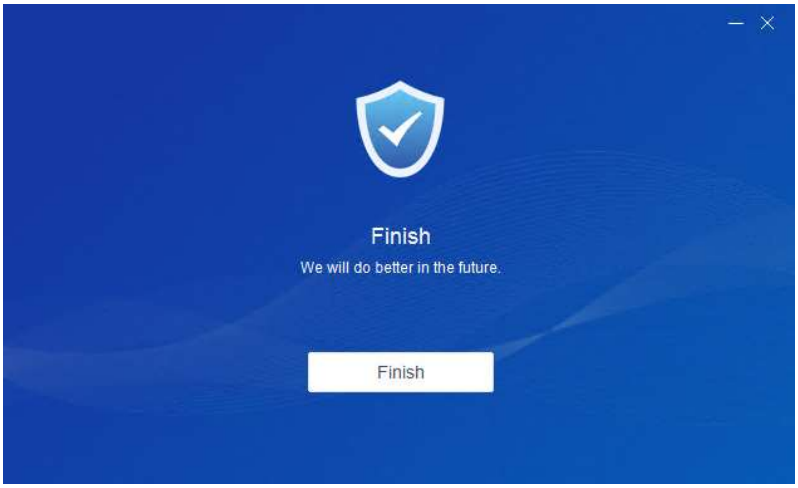
NovaGuard agent uninstallation requires the uninstallation password, which you can find in **Policies** > **General Policies** > **Basic Config** > **Agent Administration Passwords**.



Enter the uninstallation password, click **OK**, and wait for the uninstallation to complete.



The uninstallation is **complete** once the following prompt appears.



2.4.2 Uninstall from a Linux Endpoint

On the command line of the Linux endpoint, go to the NovaGuard agent directory "**/sf/edr/agent/bin**", and run the uninstallation command **eps_uninstall.sh**, as shown in the following figure.

```
[root@localhost ~]# /sf/edr/agent/bin/eps_uninstall.sh
start uninstall eps agent
mask 20edr_agent success.
stop edr_agent process for avoiding extra agent ipc msg
start stop eps_services
mask all service success.
touch edr_forbidden
clean dns rule ret is
clean_2 dns rule ret is
clean_3 dns rule ret is
/sf/edr/agent/bin/eps_services: line 119: /sys/kernel/debug/tracing/events/kprobes/Kl/enable: No such file or directory
which: no syslog-ng in (/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin)
recover iptables system log fail, continue ...
edr stop success
uninstall
no dns rule
which: no syslog-ng in (/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin)
recover iptables system log fail, continue ...
edr stop success
edr sevice stop success.
edr service stop success.
ipc_proxy start success
/sf/edr/agent/bin/eps_uninstall.sh: line 436: 18873 Terminated              $SCRIPTPATH/ipc_proxy
start clean rasp
lrasp_tool not exist
end clean rasp
start clean file
no dns rule
Removed symlink /etc/systemd/system/multi-user.target.wants/edr_agent.service.
iptables v1.4.21: Couldn't load target `SFIPS':No such file or directory

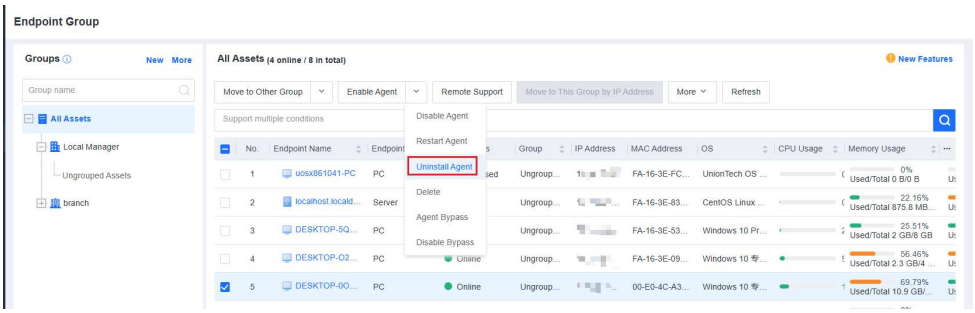
Try `iptables -h' or 'iptables --help' for more information.
iptables v1.4.21: Couldn't load target `SFIPS_OUT':No such file or directory

Try `iptables -h' or 'iptables --help' for more information.
iptables: No chain/target/match by that name.
iptables: No chain/target/match by that name.
iptables: No chain/target/match by that name.
iptables: No chain/target/match by that name.
kill edr/agent/bin/eps_services_ctrl pid( 16896) successfully
kill edr/agent/bin/abs_monitor pid( 10332) successfully
/sf/edr/agent/bin/eps_uninstall.sh: line 231: cd: /sf/edr/agent/bin/../: No such file or directory
edr agent uninstall success!!
[root@localhost ~]#
```

The uninstallation is complete once the prompt "**edr agent uninstall success!!**" appears.

2.4.3 Uninstallation on NovaGuard Manager

On the NovaGuard manager, go to **Endpoint** > **Endpoint Groups** and select the endpoint from which you want to uninstall the NovaGuard agent. Click **Uninstall Agent**, as shown in the following figure.

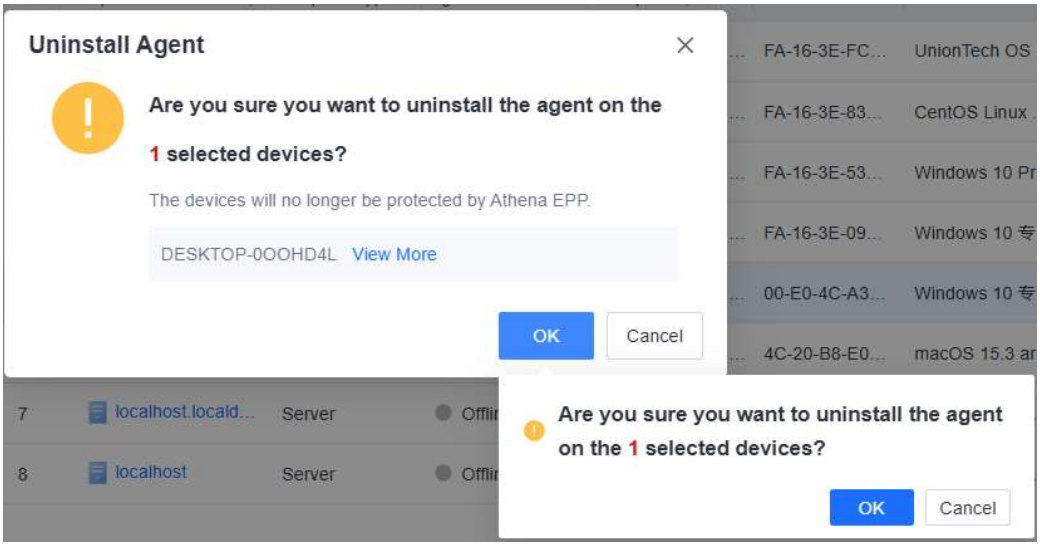


NOTE

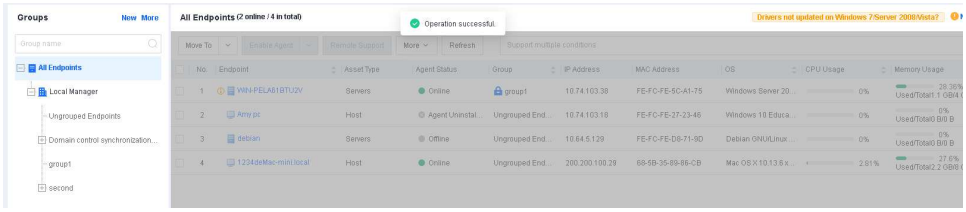
You can uninstall the NovaGuard agent in **Online** or **Disabled** status, and the endpoints must be able to receive the policies distributed from the console. The uninstallation will

automatically start silently in the background after the NovaGuard agent on the endpoint receives the uninstallation command.

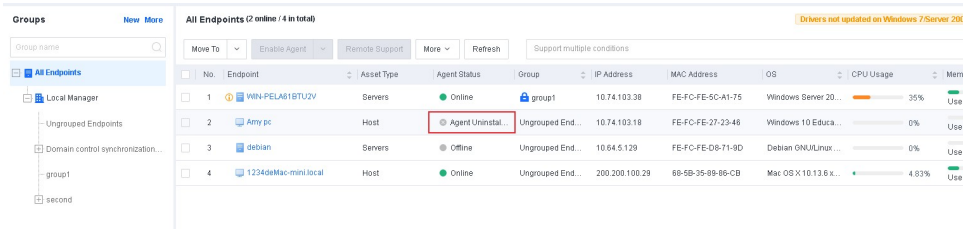
Click **OK** in the confirmation window.



Wait for the prompt "**Operation successful**" to appear on the NovaGuard manager.



The uninstallation is complete once the status of the endpoint becomes **Agent Uninstalled**.



2.5 Environments

2.5.1 NovaGuard manager Installation Environment

You can install the NovaGuard manager on your existing operating system. The requirements are as follows.

CPU Architecture	Operating System (64-bit)
x86-64	Ubuntu 20.04 and later
x86-64	CentOS 7 and later

Table 1: CPU and Operating System Requirements for NovaGuard manager Installation

Endpoints	CPU	Memory	Disk
1 - 2000	6 cores	8 GB	300 GB
2000 - 5000	8 cores	12 GB	500 GB
5000 - 10000	12 cores	16 GB	800 GB

Table 2: Hardware Requirements for Typical NovaGuard manager Installation

Endpoints	CPU	Memory	Disk
1~2500	8 cores	16 GB	500G
2500~5000	12 cores	16 GB	800G
5000~10000	16cores	20 GB	1TB

Table 3: Hardware Requirements for Integrated Installation of NovaGuard Manager and aTrust

2.5.2 NovaGuard agent Installation Environment

You can install the NovaGuard agent on operating systems such as Windows PC, Windows Server, Linux, and macOS. The supported operating systems are in a separate list. Please request by support@forenova.com

Hardware Specifications	Disk Space	Remarks
6 cores and 8GB RAM (recommended specifications)	5 GB	
4 cores and 4GB RAM (minimum specifications)	5 GB	The Gene Analytic Engine is not installed by default and needs to be installed manually.

Hardware Specifications

2.5.3 Network Connectivity Requirements

NovaGuard requires network connectivity between the NovaGuard agent and the NovaGuard manager and between the NovaGuard manager and the cloud server. The required ports and server addresses are as follows.
Please request this document by support@forenova.com

File Whitelist Setting

To avoid false positives during virus scans, collect trusted files such as virus-free business software and previously whitelisted files from other antivirus products, log in to the NovaGuard manager that you have deployed and activated, and add the trusted files in **Policies** > **Detection Policies** > **File Hashes** or **Policies** > **Exclusions**. Added trusted files will not be scanned.

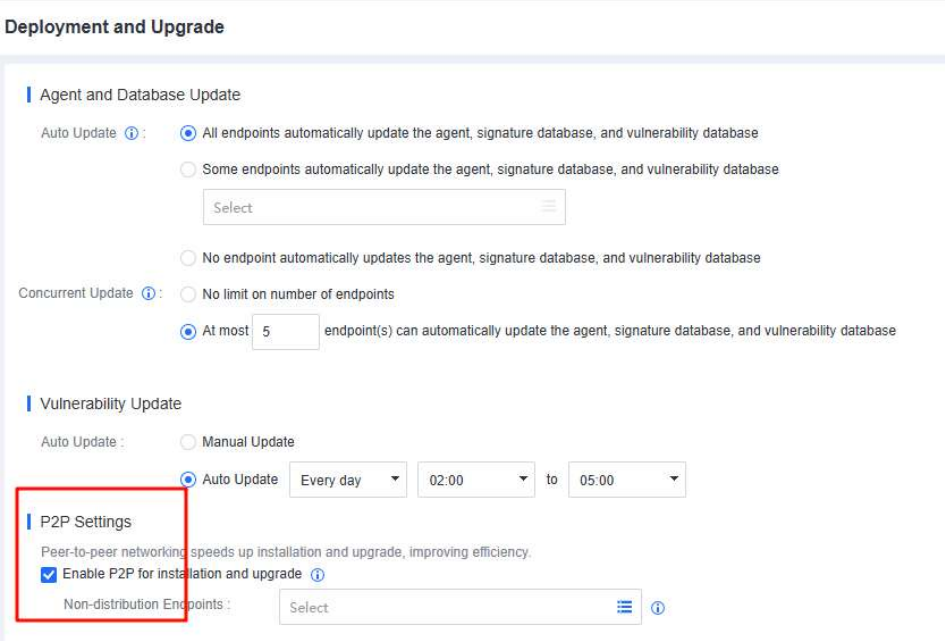
IOC Blacklist/ Whitelist	MD5 Hash	Action	Applicable Scope
Security tool	62e153936f09ae701770c5ce014f98ff	Alert	Security department group
IT O&M tool	37bb0bbc1255fdb1693aa45a70bedd91	Allow	IT department group
hacker.exe	6581c35e063322bc6c4f100c4aa48340	Alert and Fix	Security department group
Exclusion	**Excluded Path/Suffix**		**Applicable Scope**

The home folder	/home	Server group
Installation packages	.pkg	IT department group

3 Product Upgrade

The upgrade of NovaGuard involves the upgrade of the NovaGuard manager or NovaGuard agent to a new version and the update of the service packs, antivirus database, and vulnerability database.

We recommend that you go to **System** > **System** > **Deployment and Upgrade** and enable P2P upgrade, as shown in the following figure.



This feature avoids single-channel file download from the NovaGuard manager only, which causes slow installation and upgrade and excessive bandwidth usage.

NOTE

1. P2P deployment is not supported in scenarios where the NovaGuard manager is exposed to the Internet through port mapping.

2. P2P upgrade is supported for NovaGuard Windows agent installation, NovaGuard agent upgrade, and antivirus database update.

3.1 Upgrade to a New Version

3.1.1 Import an Upgrade Package

Pre-upgrade checks

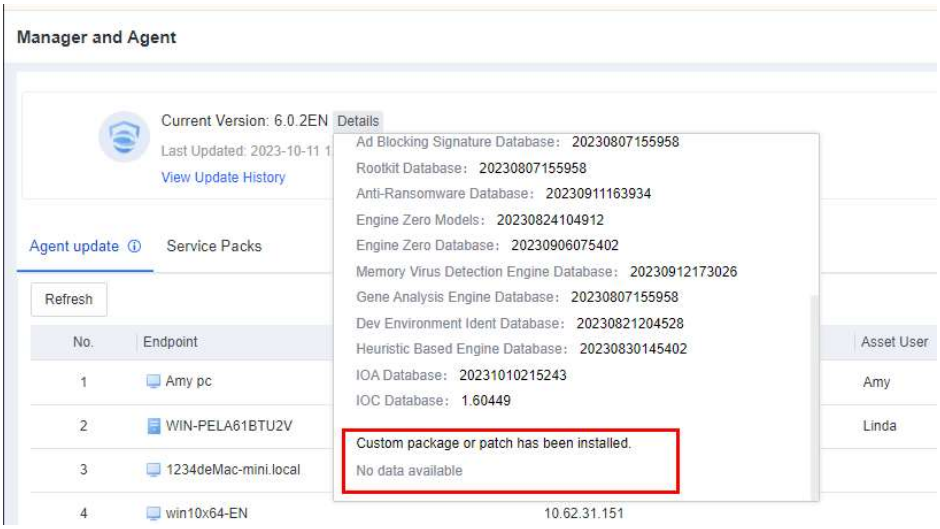
1. Check product licensing

Go to **System** > **Licensing** and check whether the license is valid, as shown in the following figure. If the license has expired, NovaGuard cannot be upgraded.



1. Check for custom packages and patches

You must contact technical support if custom packages or patches are installed. Go to **System > System Updates > Manager and Agent** to check whether custom packages and patches have been installed.



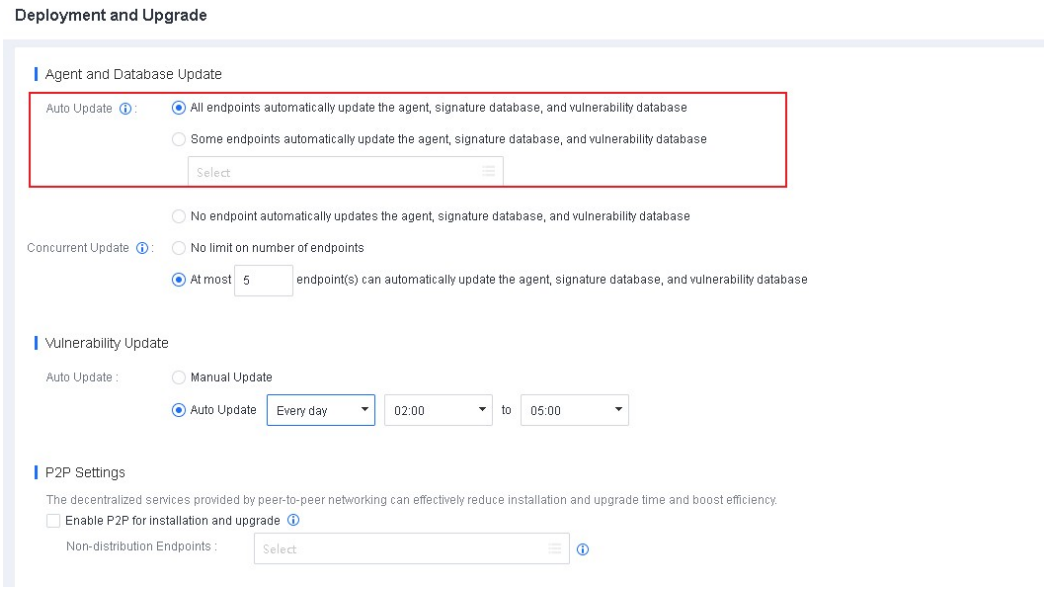
Precautions

After the NovaGuard manager is upgraded, the NovaGuard agent automatically downloads upgrade files from the NovaGuard manager. To ensure a stable and efficient NovaGuard agent upgrade, we recommend that you configure both auto upgrade and concurrent upgrade settings.

1. Auto update

On the **Deployment and Upgrade** page of the NovaGuard 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.

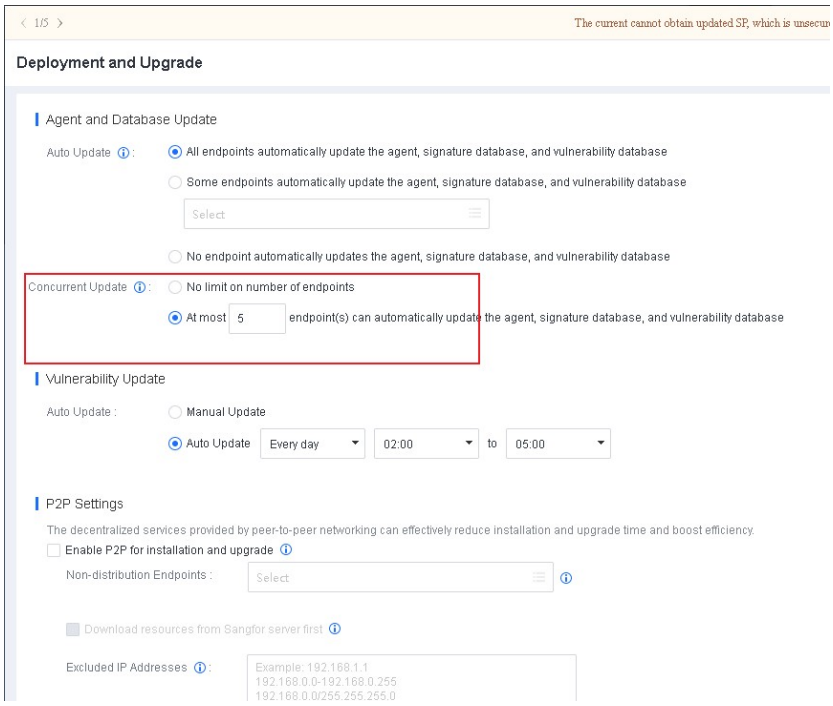
To configure the settings, go to **System** > **System** > **Deployment and Upgrade** > **Agent and Database Update** > **Auto Update**, as shown in the following figure.



2. Concurrent update

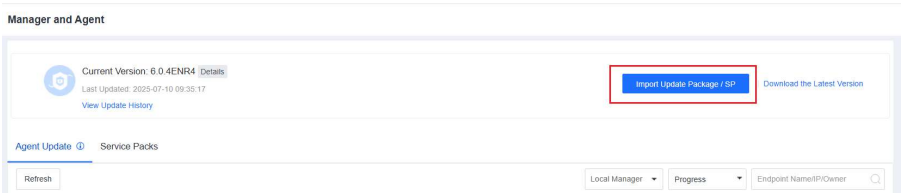
To avoid network congestion, you can specify the maximum number of endpoints that can download the NovaGuard agent installer at the same time. We recommend that you set the maximum number of concurrently updated endpoints to 5 or less if the network bandwidth is 100 Mbit/s and 30 or less if the network bandwidth is 1,000 Mbit/s.

To configure the settings, go to **System** > **System** > **Deployment and Upgrade** > **Agent and Database Update** > **Concurrent Update**, as shown in the following figure.



Procedure

1. Ask the ForeNova Support for the latest package
2. Log in to the NovaGuard manager. Go to **System** > **System Updates** > **Manager and Agent**, and click **Import Update Package / SP**, as shown in the following figure.

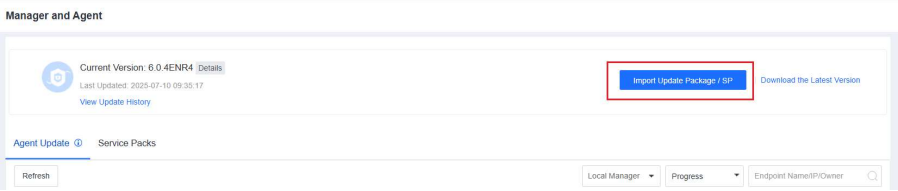


3. The upgrade process takes about 5 minutes to complete without restarting the server. After the upgrade, you need to log in to the NovaGuard manager again and check whether NovaGuard is upgraded to the new version.

3.2 Update Service Packs

When an NovaGuard service pack is released, the NovaGuard manager can update it online, or you can manually import the service pack. To view the

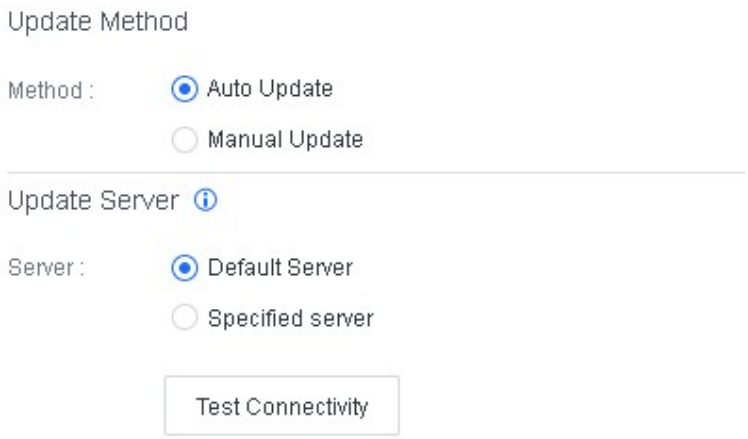
details of service pack update, go to **System** > **System Updates** > **Manager and Agent** > **Service Packs**.



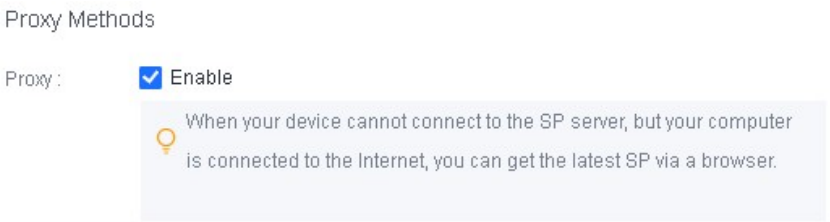
Configure service pack update settings

You can specify the method for updating service packs.

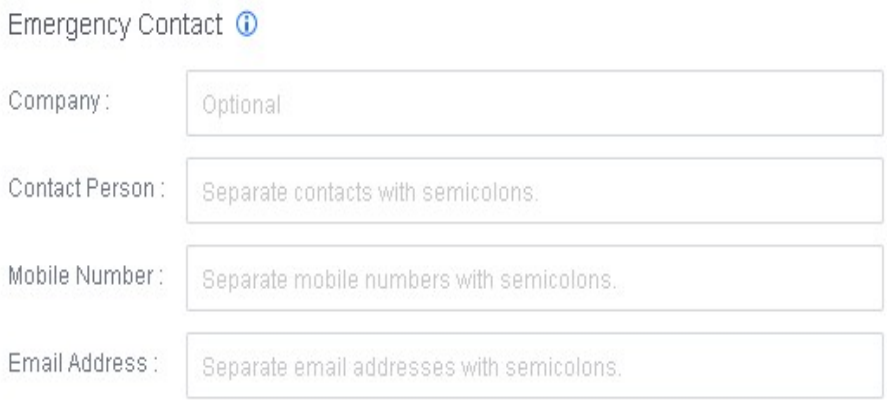
Go to **System** > **System Updates** > **Manager and Agent** > **Service Packs**. Click **Update Options** and specify the update method and upgrade server, as shown in the following figure.



If the NovaGuard manager cannot directly connect to the Internet, but the local computer has Internet access, you can enable a browser proxy, so that the NovaGuard manager obtains service pack updates through the proxy, as shown in the following figure.



We recommend that you provide an emergency contact, as shown in the following figure. If we have released an emergency pack, but you do not enable automatic upgrade, we can contact you at the earliest opportunity to prevent business interruptions.



3.3 Update the Signature Databases

3.3.1 Update the Antivirus Database

The antivirus database can be updated online and offline.

Online update

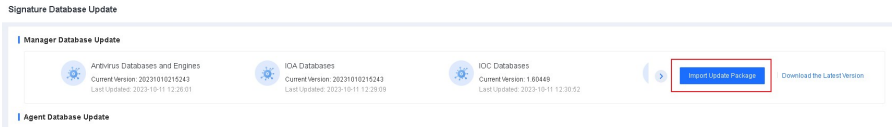
By default, if the NovaGuard manager is connected to the Internet, the antivirus database is automatically updated online.

Offline update

If the NovaGuard manager is disconnected from the Internet, you can manually update the antivirus database offline by performing the following steps:

1. Ask ForeNova support for offline packages.
2. Log in to the NovaGuard manager. Go to **System** > **System Updates** > **Signature Database Update**, and click **Import Update Package**. Then, select the antivirus database downloaded in Step 1. After the antivirus database and engine are imported to the NovaGuard manager, the NovaGuard agent will automatically update the antivirus database and

engine, as shown in the following figure.



3.3.2 Update the IOA or IOC Database

The IOA or IOC database can be updated online and offline.

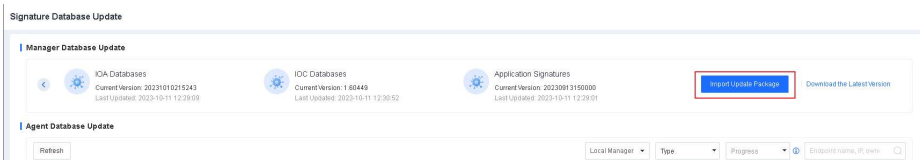
Online update

By default, if the NovaGuard manager is connected to the Internet, the database is automatically updated online.

Offline update

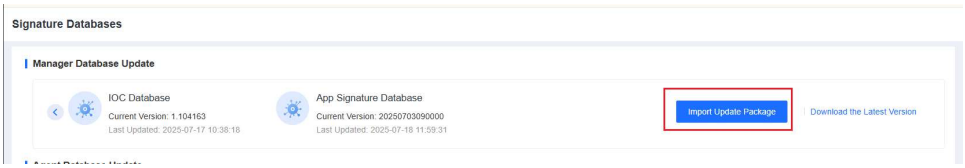
If the Manager is disconnected from the Internet, you can manually update the database offline by performing the following steps:

1. Ask ForeNova Support for offline packages
2. Log in to the NovaGuard manager. Go to **System** > **System Updates** > **Signature Database**, and click **Import Update Package**. Then, select the database downloaded in Step 1. After the IOA or IOC database is imported to the NovaGuard manager, the NovaGuard agent will automatically update the IOA or IOC database, as shown in the following figure.



3.3.3 Offline update Signature Database

The Signature Database can be updated offline.



3.4 Update the Vulnerability Database

The vulnerability database can be updated online and offline.

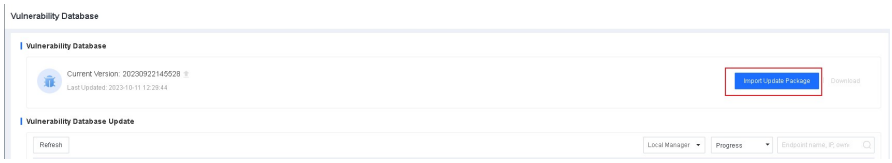
Online update

By default, if the NovaGuard manager is connected to the Internet, the vulnerability database and patch package are automatically updated online.

Offline update

If the NovaGuard manager is disconnected from the Internet, you can manually update the vulnerability database offline by performing the following steps:

1. Ask ForeNova Support for offline packages.
2. Log in to the NovaGuard manager. Go to **System** > **System Updates** > **Vulnerability Database**, and click **Import Update Package**. Then, select the database downloaded in Step 1. After the database is imported to the NovaGuard manager, the NovaGuard agent will automatically update the database, as shown in the following figure.



4 Getting Started

4.1 Login Page of NovaGuard manager

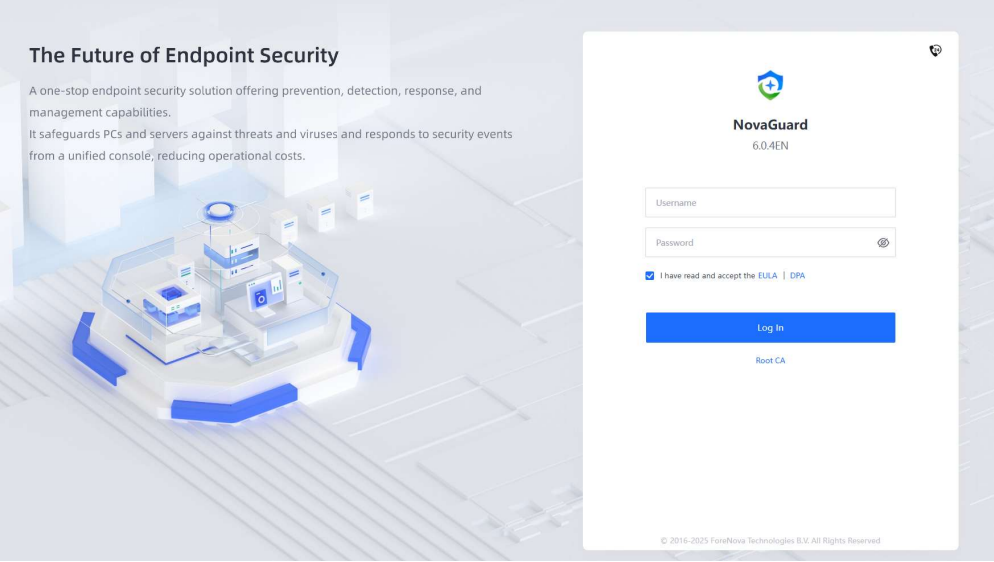
To ensure security, you must log in to the NovaGuard manager via the HTTPS port. Open a browser, enter "**https://[NovaGuard_IP]"** (the default IP address is 10.251.251.251), and press Enter.

NOTE

1. When the prompt "**The identity of this website or the integrity of this connection cannot be verified**." appears, click **Yes**.

2. For 6.0.4R2 and earlier versions, the default platform IP address is 10.251.251.251.

3. The browsers such as Internet Explorer 11 or later, Firefox, and Chrome are supported.



Enter the username, password, and verification code in the login boxes and click **Log In**.

NOTE

The default username and password are both **admin**.

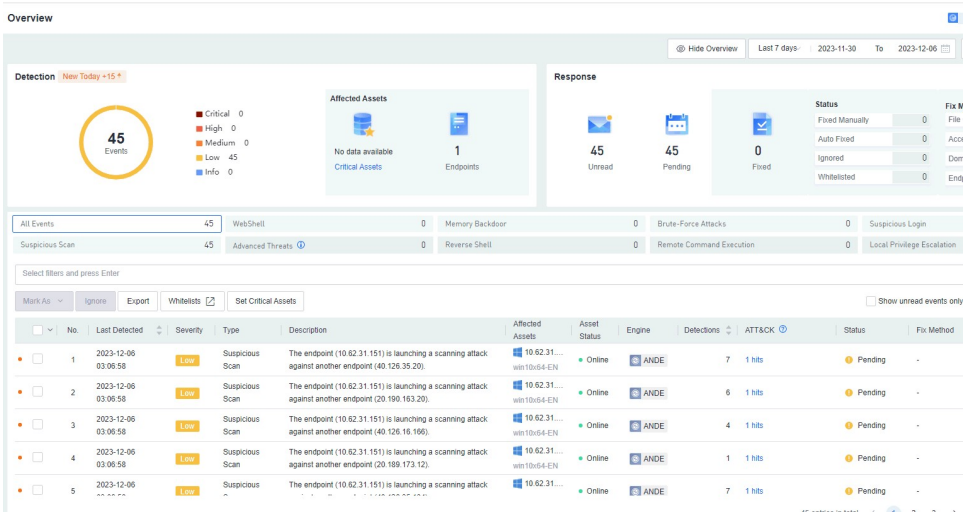
Follow the system prompt to change the default administrator password after the first time login to ensure platform security.

4.2 Detection and Response

4.2.1 Security Events

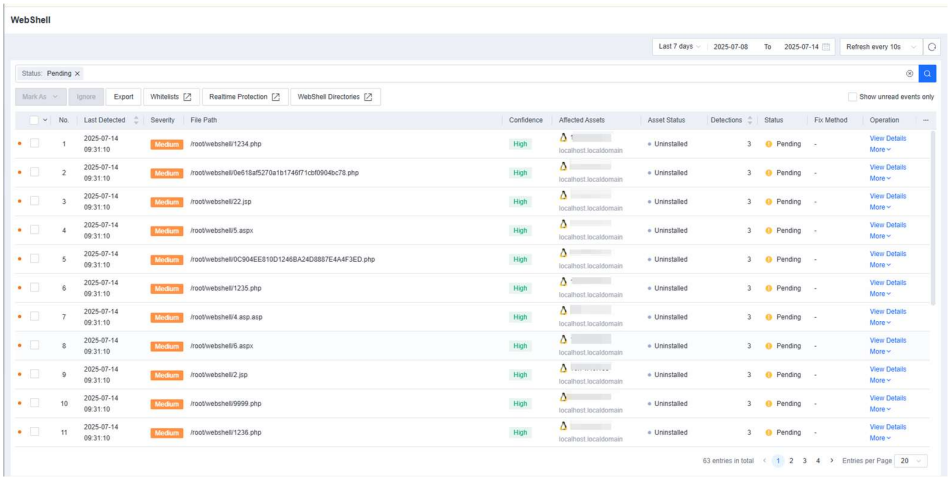
4.2.1.1 Overview

This page shows the summary of all recent security events detected (events detected in the last seven days are displayed by default; you can select a period). It provides an overview of events detected within the current network, including the total number of events, affected critical assets, and a breakdown of events such as web shell attacks and brute-force attacks.

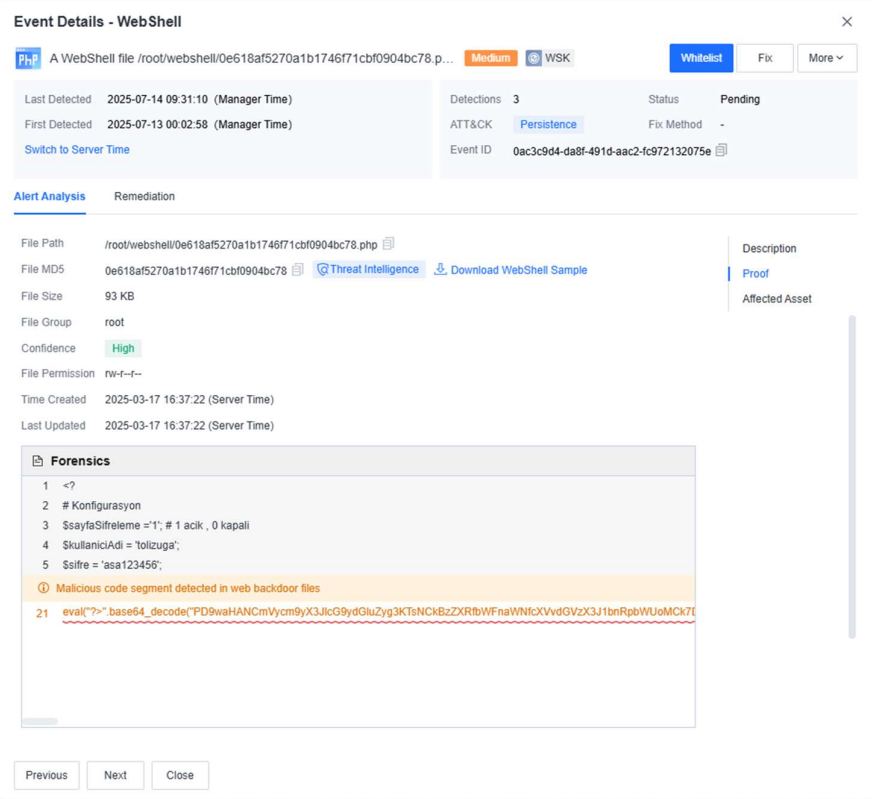


4.2.1.2 WebShell

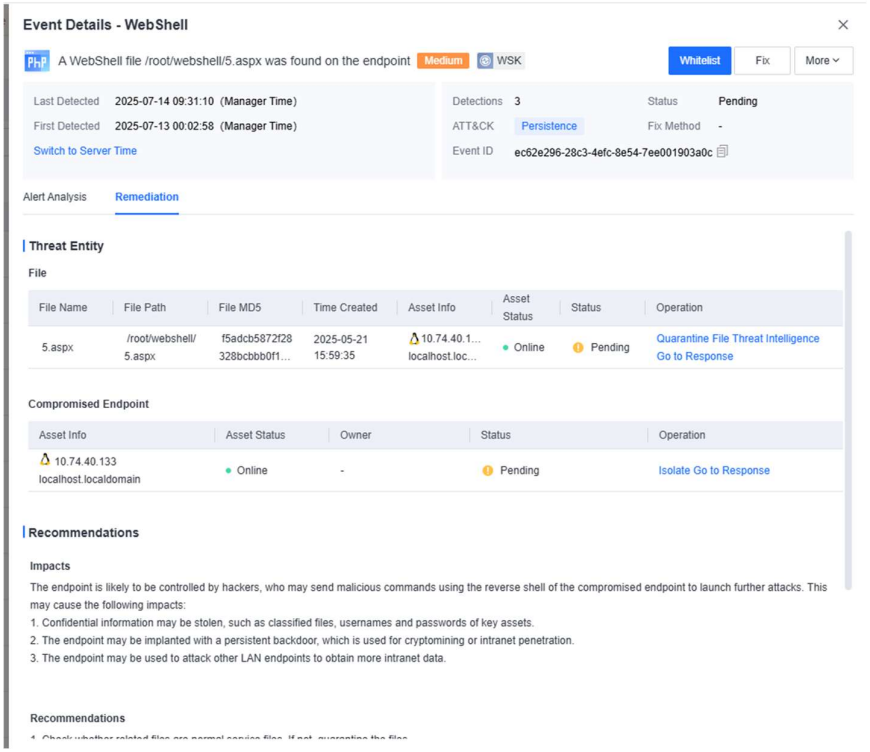
Scans and monitors endpoints in real time via the NovaGuard agent for web shells.



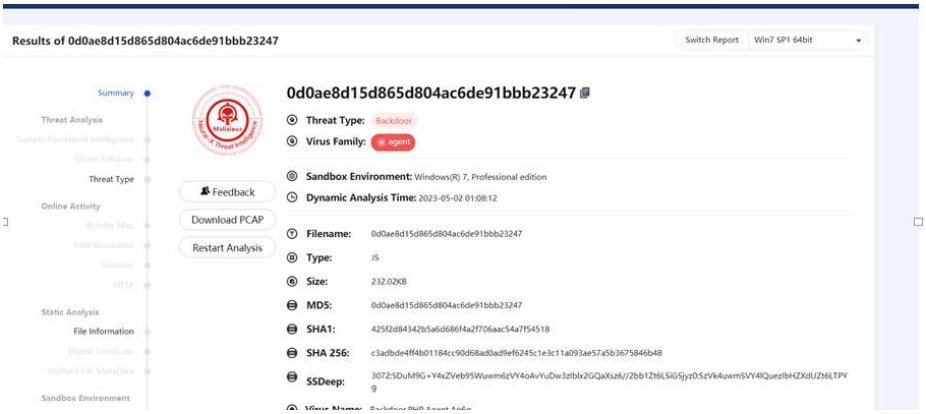
Click **View Details** to view the event details.



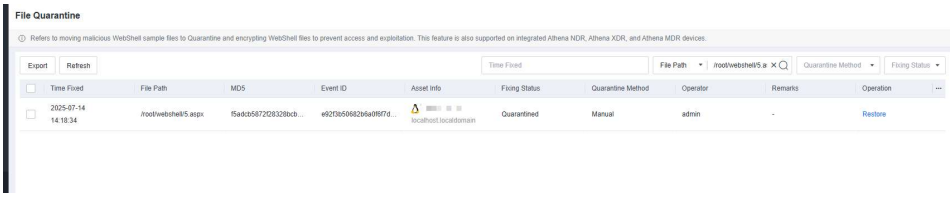
Click **Fix** to fix the threat entity or the compromised endpoint.



Click **Threat Intelligence** to visit ForeNova Threat Intelligence for web shell identification.



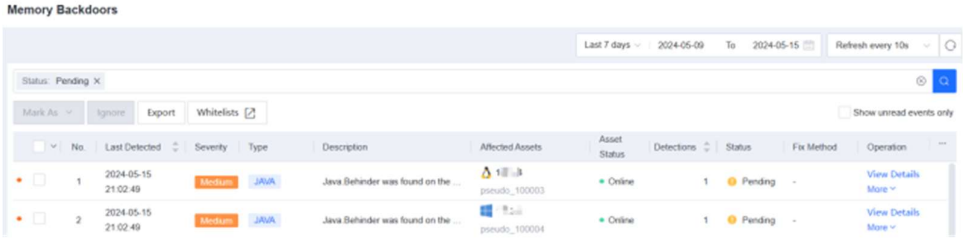
Click **Go to Response**. You will be redirected to the **Detection and Response** > **Response** page to view event logs.



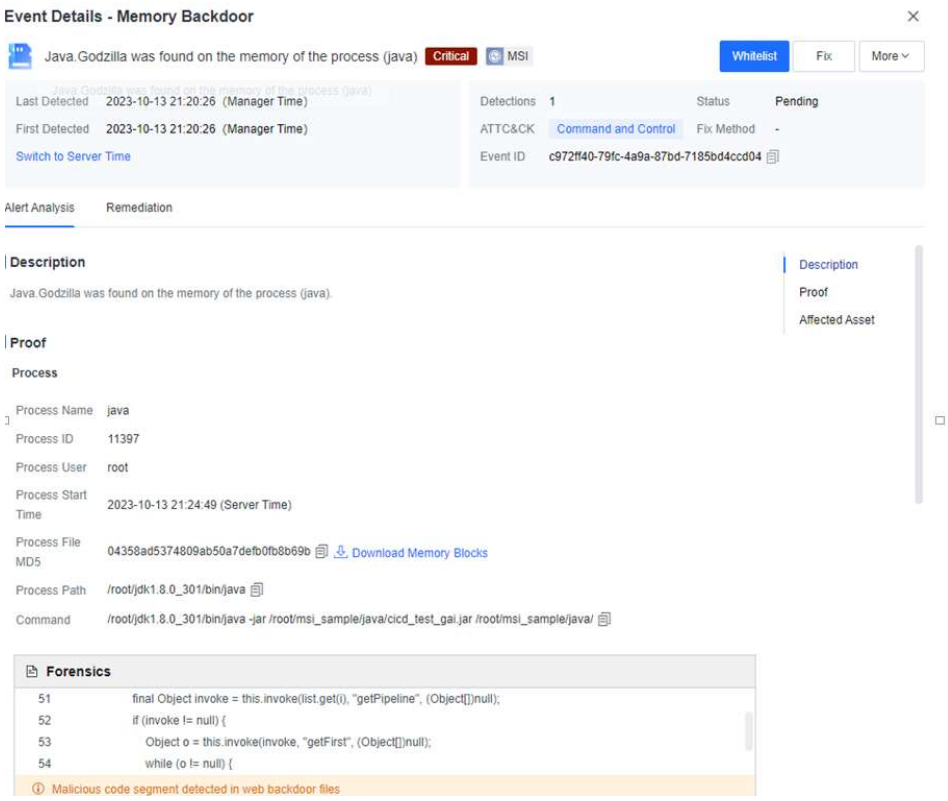
4.2.1.3 Memory Backdoors

Scans and monitors endpoints in real time for memory backdoors via the NovaGuard agent.

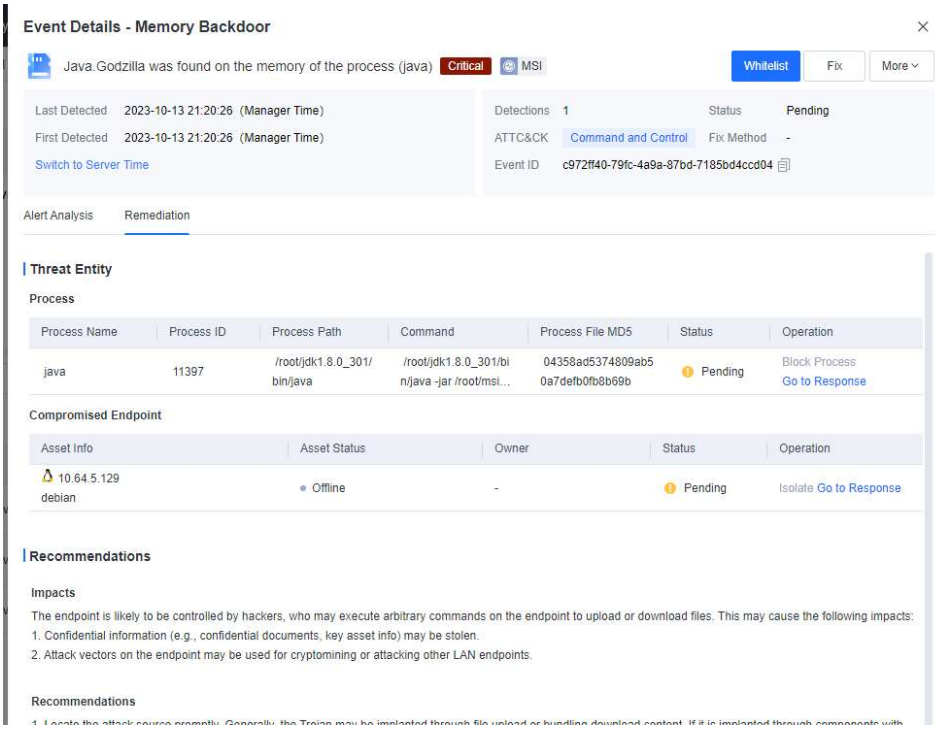
Memory backdoors are mainly detected on endpoints.



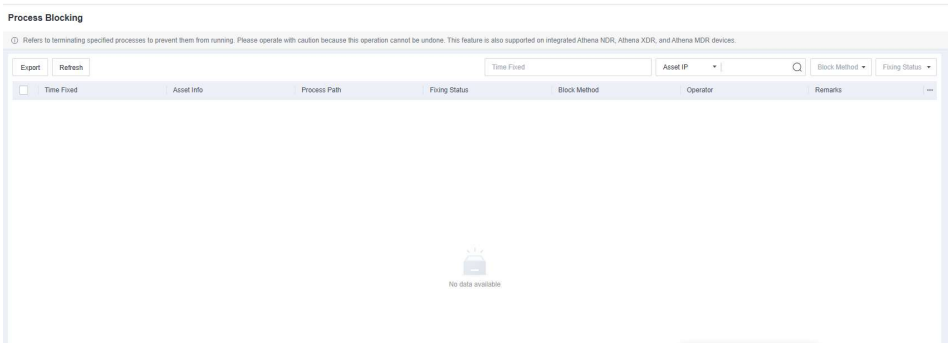
Click **View Details** to view the event details.



Click **Fix** to fix the threat entity or the compromised endpoint.

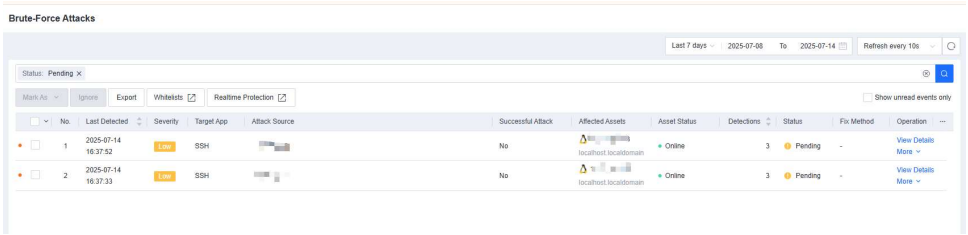


Click **Go to Response**. You will be redirected to the **Detection and Response** > **Response** page to view event logs.



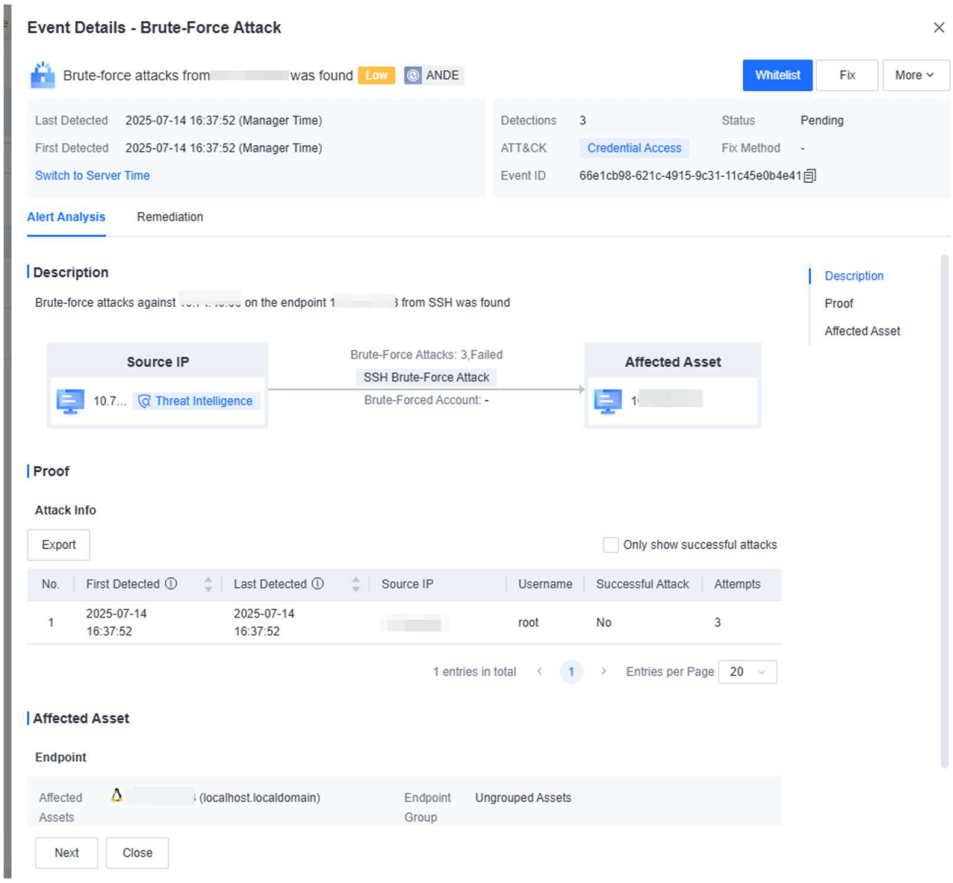
4.2.1.4 Brute-Force Attacks

NovaGuard can detect brute-force attacks against Remote Desktop Protocol (RDP), Server Message Block (SMB), Microsoft SQL Server, and SSH services.

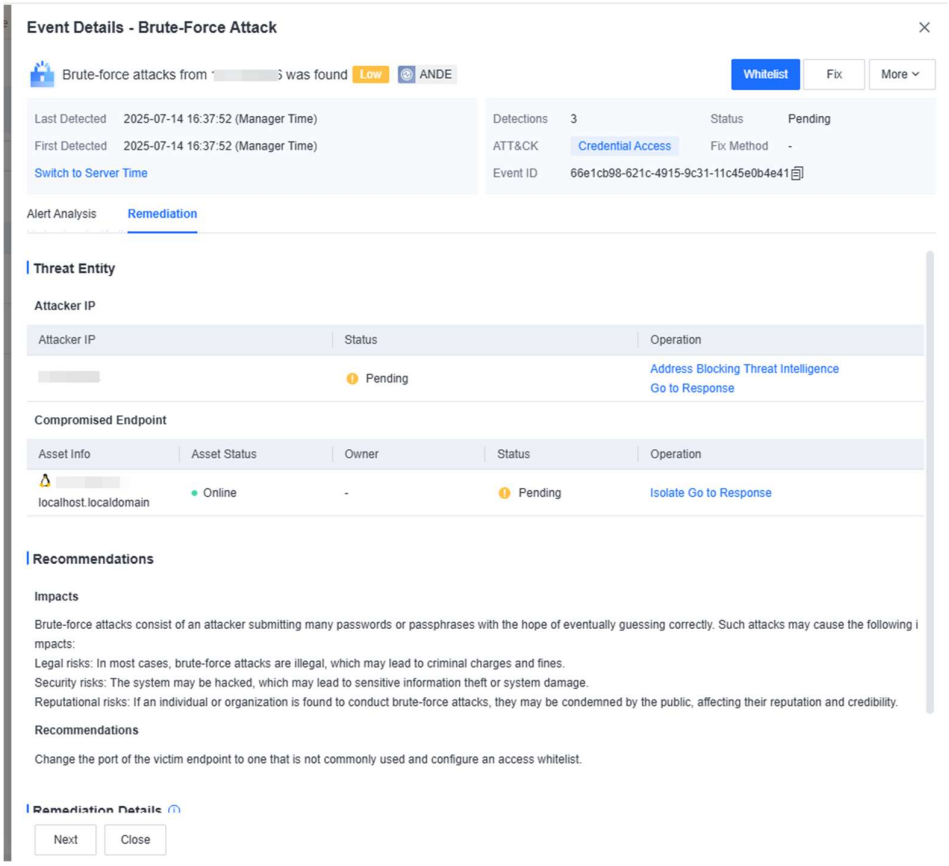


Click **View Details** to view the details of a brute-force attack event, including the source IP address, destination IP address, time when the attack was

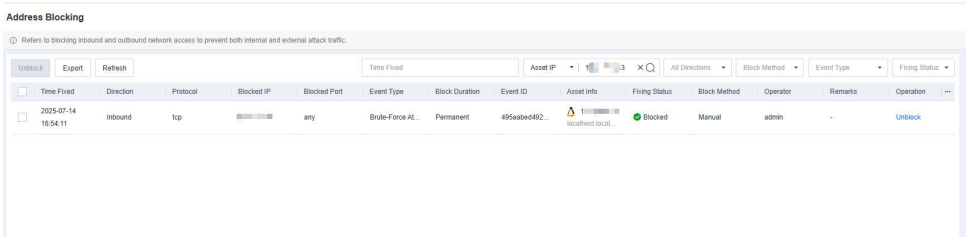
detected, number of attacks, and whether the attack is successful.



Click **Fix** to fix the threat entity or the compromised endpoint.



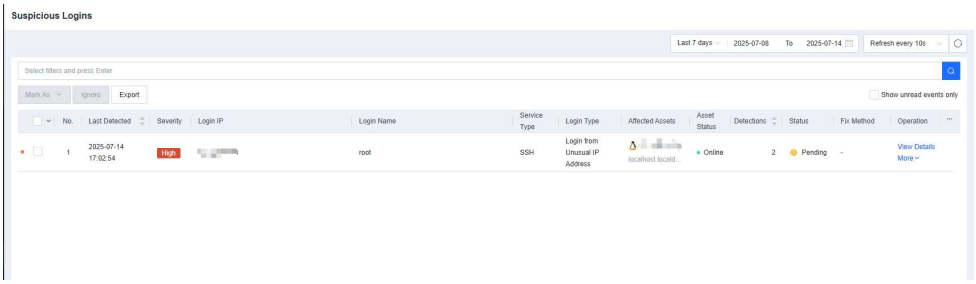
Click **Go to Response**. You will be redirected to the **Detection and Response** > **Response** page to view event logs.



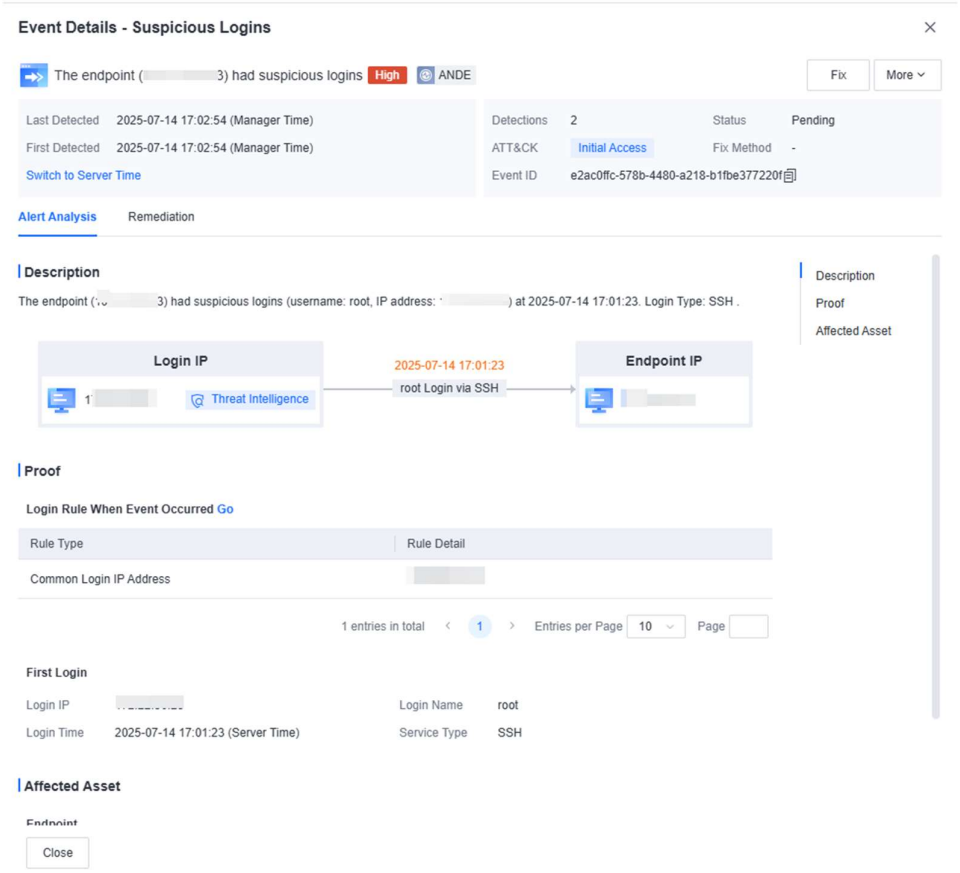
4.2.1.5 Suspicious Logins

NovaGuard can detect suspicious login from unusual times or uncommon IP addresses. It can also detect suspicious login events on Windows endpoints

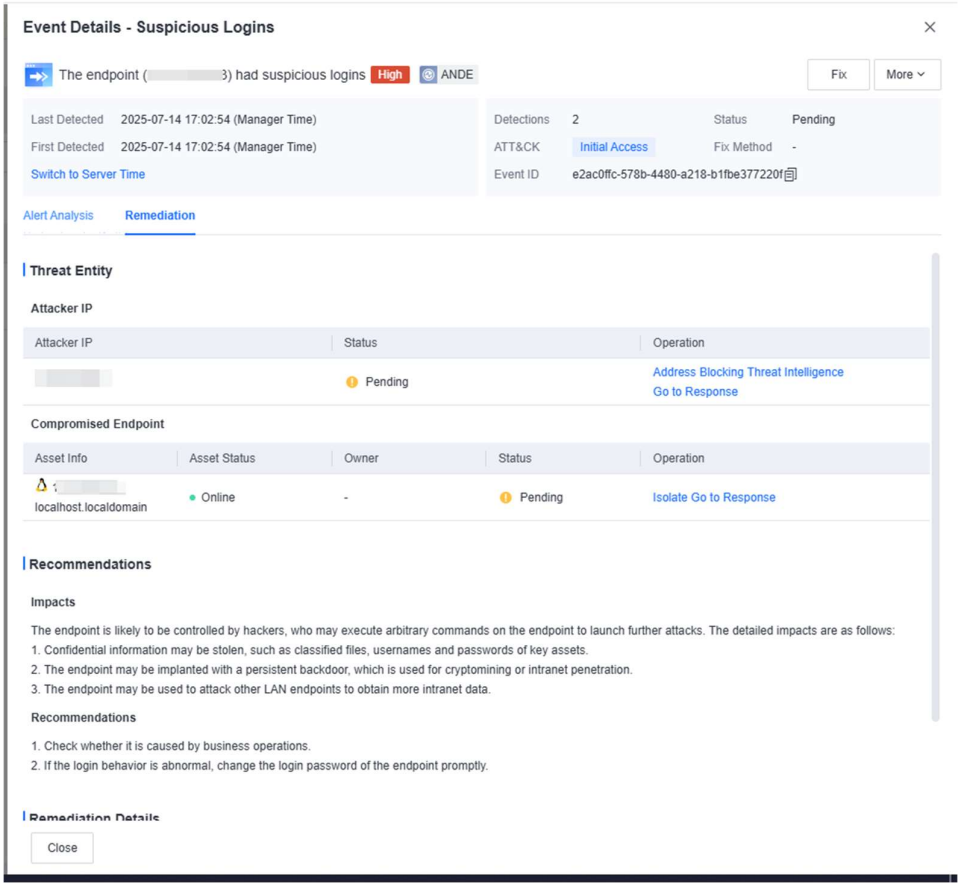
(including PCs) via RDP or SMB and those on Linux endpoints via SSH.



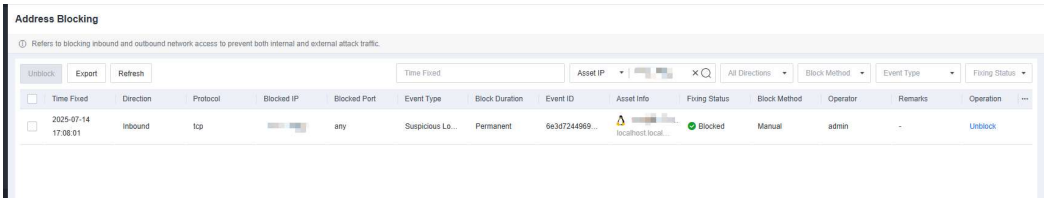
Click **View Details** to view the details of a suspicious login event, including the login IP address, protocol, login name, destination IP address, login time, number of occurrences, and recommendations.



Click **Fix** to fix the threat entity or the compromised endpoint.



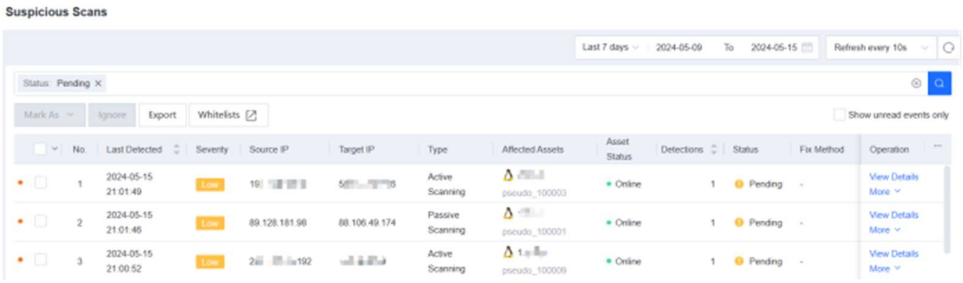
Click **Go to Response**. You will be redirected to the **Detection and Response** > **Response** page to view event logs.



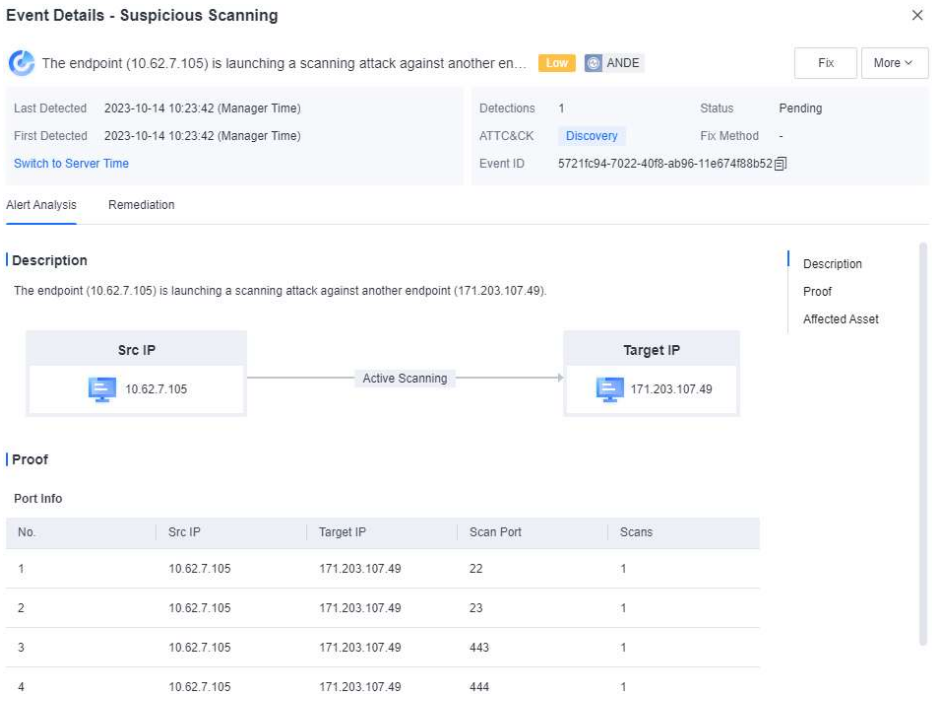
4.2.1.6 Suspicious Scans

The NovaGuard agent can actively and passively detect the port scanning activity. The agent-installed endpoint can actively detect the port-scanning activity and detect the port-scanning activity from other endpoints toward the agent-installed endpoint.

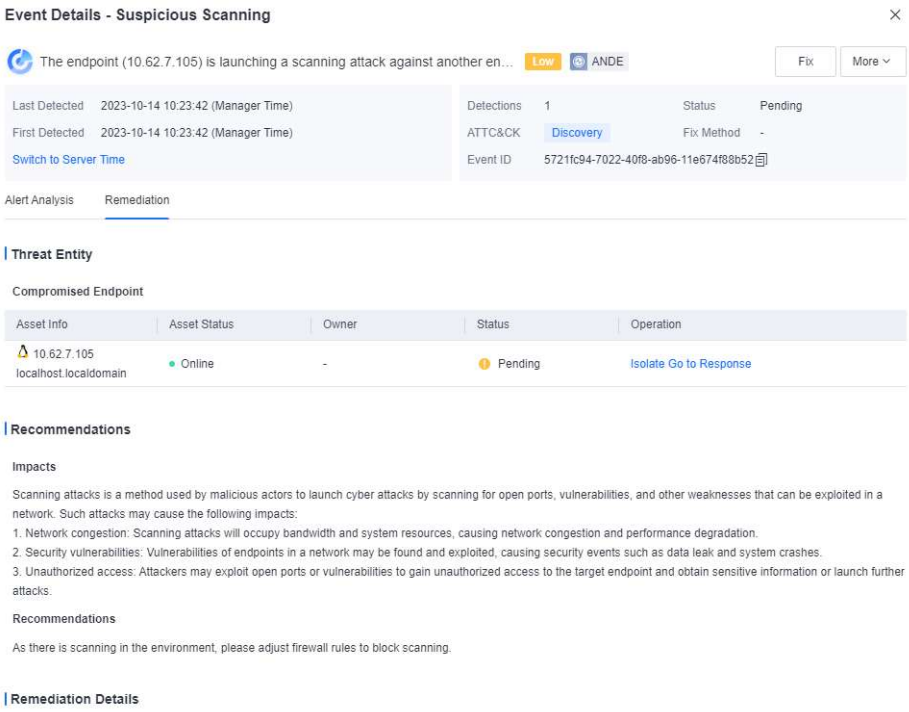
Suspicious scans will be reported automatically once detected without requiring manual configuration.



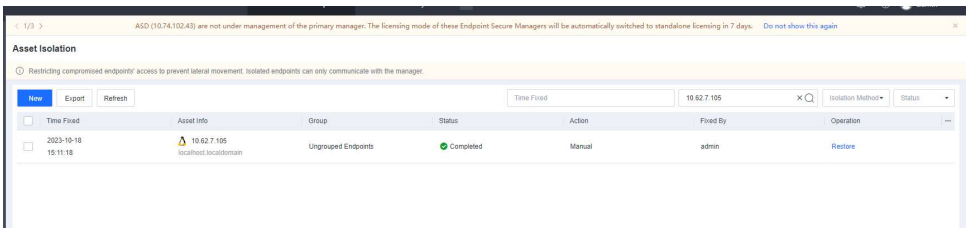
Click **View Details** to view the details of a suspicious scan event, including the source IP address, target endpoint and port, time when the scan was detected, number of occurrences, and recommendations.



Click **Fix** to fix the compromised endpoint.



Click **Go to Response**. You will be redirected to the **Detection and Response** > **Response** page to view event logs.



4.2.1.7 Advanced Threats

Scenario

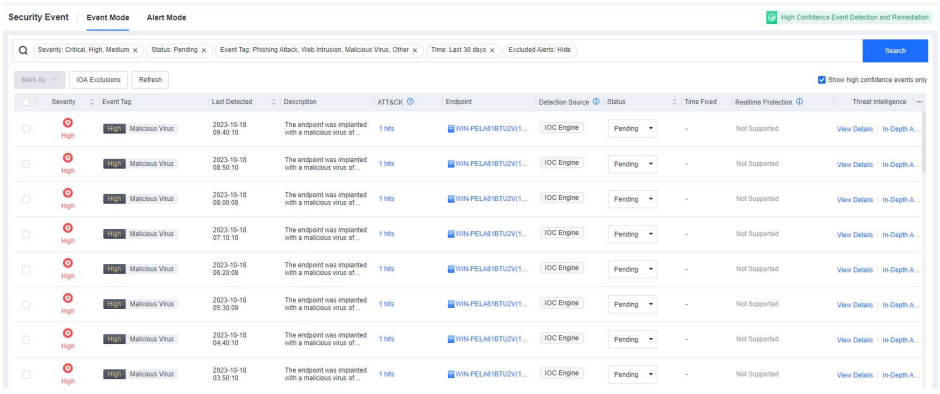
In response to emerging threats and attack-defense scenarios, such as ransomware attacks and phishing emails exploiting office networks to breach internal systems, NovaGuard can, by leveraging Indicator of Attack (IOA) rules, detect abnormal behaviors such as ransomware and phishing (for details, see MITRE ATT&CK framework, which outlines adversary tactics and techniques such as fault injection, credential stealing, and permission escalation). NovaGuard swiftly generates security alerts when detecting threats or attacks

and blocks high-risk activities. Furthermore, NovaGuard traces the process chain responsible for initiating an attack, consolidates all related abnormal behaviors into a precise security event, and helps identify the source of the attack and any startup items created in the operating system for comprehensive removal.

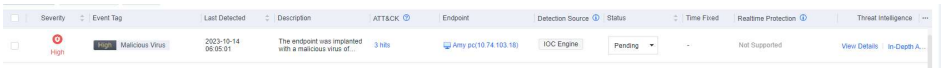
Example:

The following is an example of detecting and handling cryptomining, which illustrates the features of Advanced Threats.

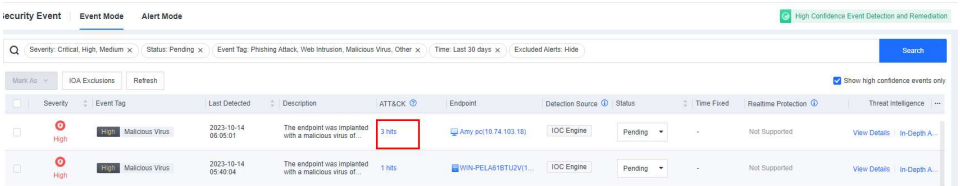
During routine O&M, the security administrator observes some suspicious activities flagged by the Advanced Threats service of NovaGuard. These activities include cryptomining attacks, account activations, and creating suspicious files, as shown in the following figure.



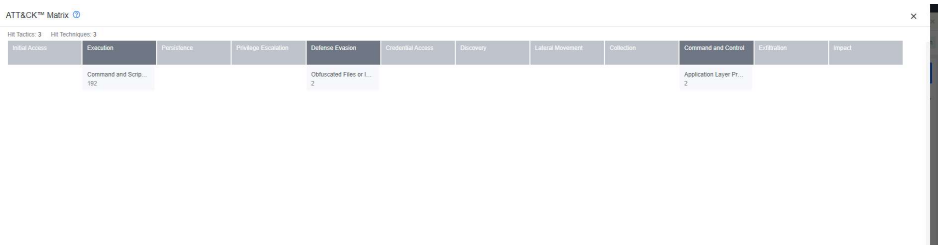
On the **Event Mode** tab, the administrator finds a security event of critical severity, as shown in the following figure. NovaGuard has consolidated various suspicious activities into a complete attack event.



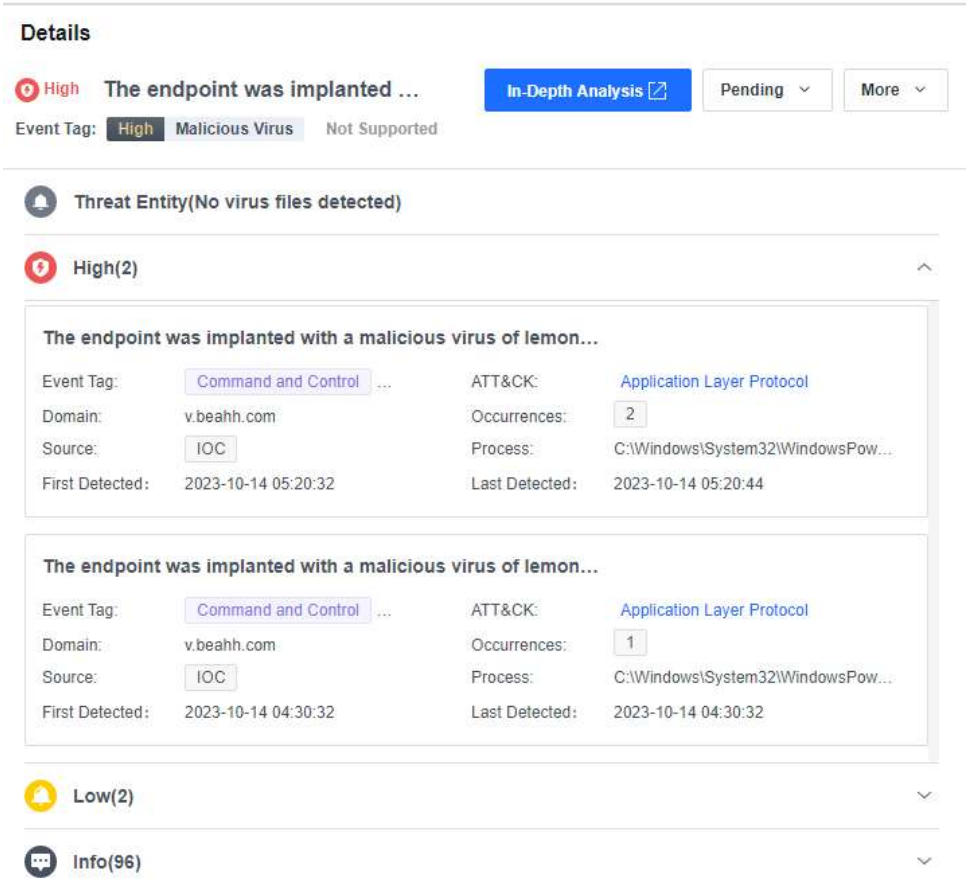
On the **Event Mode** tab, the administrator finds multiple hits within the ATT&CK matrix, as shown in the following figure.



The attack hits multiple tactics within the ATT&CK matrix, including execution, persistence, defense evasion, credential access, discovery, command and control, and impact.



After clicking **View Details**, the administrator can check the involved threat entities and alerts.

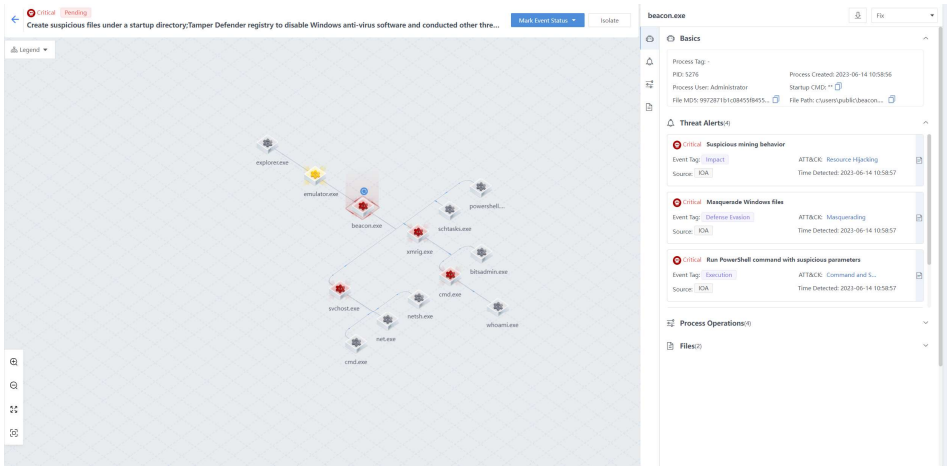


After clicking **In-Depth Analysis**, the administrator can trace the complete attack chain.



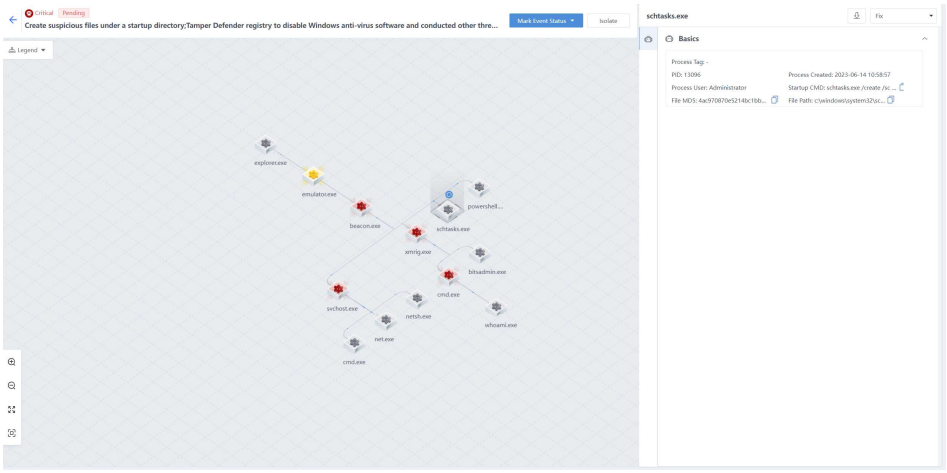
1. Attack entry

The attacker accessed the testing machine through a remote desktop login and released the attack sample emulator.exe. After the sample is executed, the beacon.exe file and a process are automatically created.



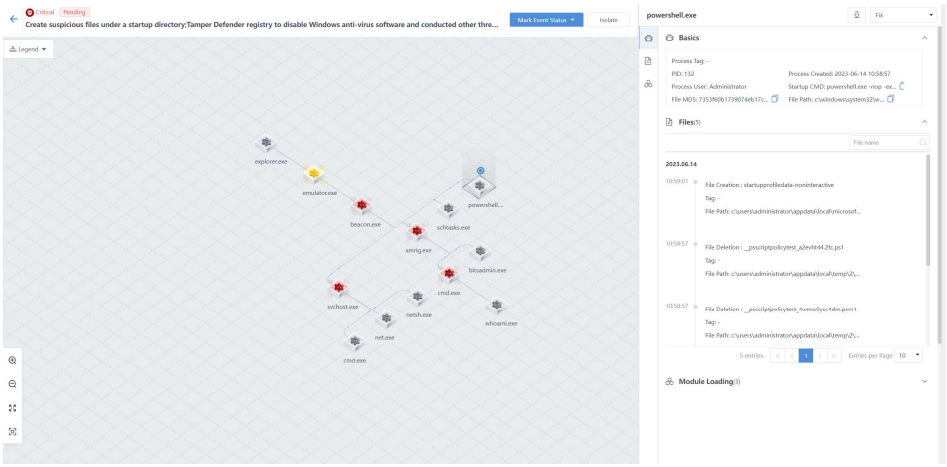
2. Create suspicious task plans to carry out persistent attacks

The beacon.exe creates the schtasts.exe process and creates suspicious task plans through the schtasts.exe process to carry out persistent attacks.



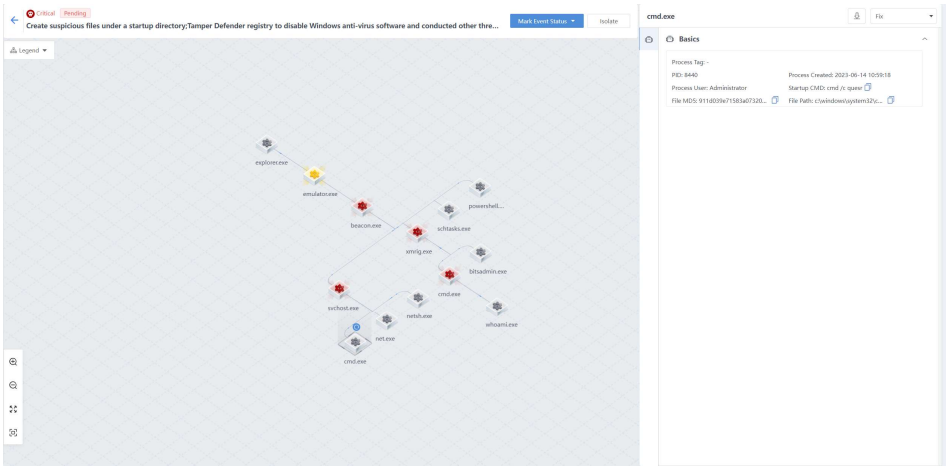
3. Execute confusing PowerShell commands to bypass security protection and carry out the attack

The beacon.exe creates a powershell.exe process to bypass security protection and carry out the attack by executing confusing PowerShell commands.



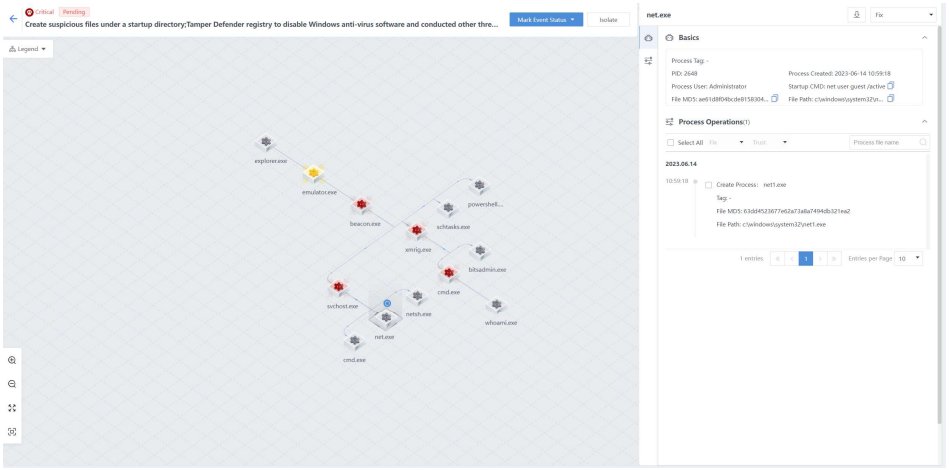
4. Detect host users to collect information

The beacon.exe creates the svchost.exe process and calls the command **cmd /c quser** to detect host user information to achieve information collection.



5. Activate a host guest user to achieve a persistent attack

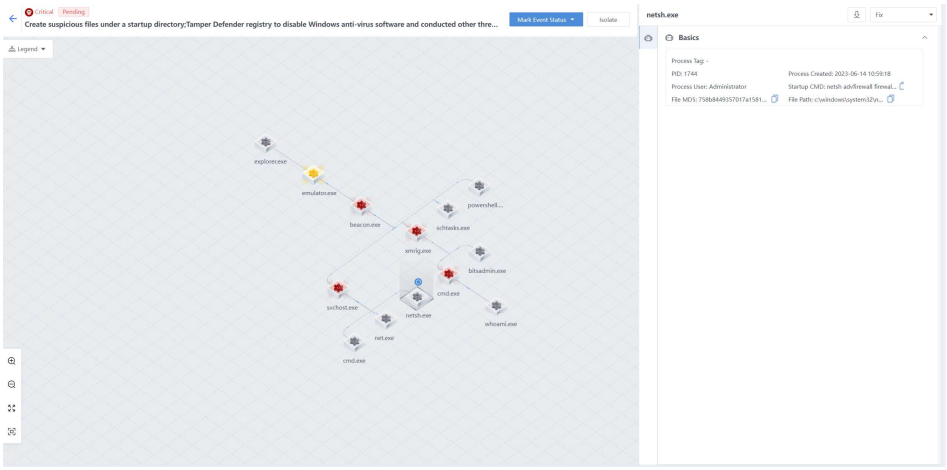
The beacon.exe creates the svchost.exe process and calls the command net user guest guest /active to activate the host guest user to carry out a persistent attack.



6. Create a suspicious firewall bypass list via netsh

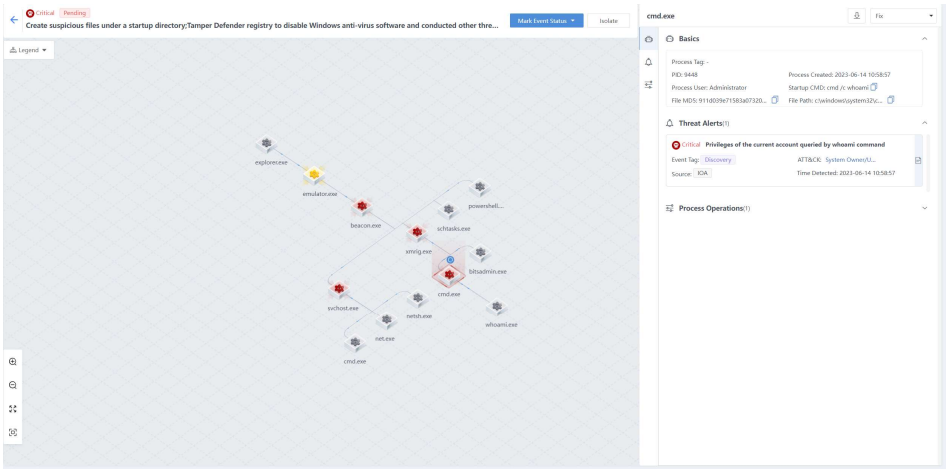
The beacon.exe creates the svchost.exe process and calls the netsh command to add firewall whitelist rules and establish suspicious connections in an

attempt to bypass firewall security protection.



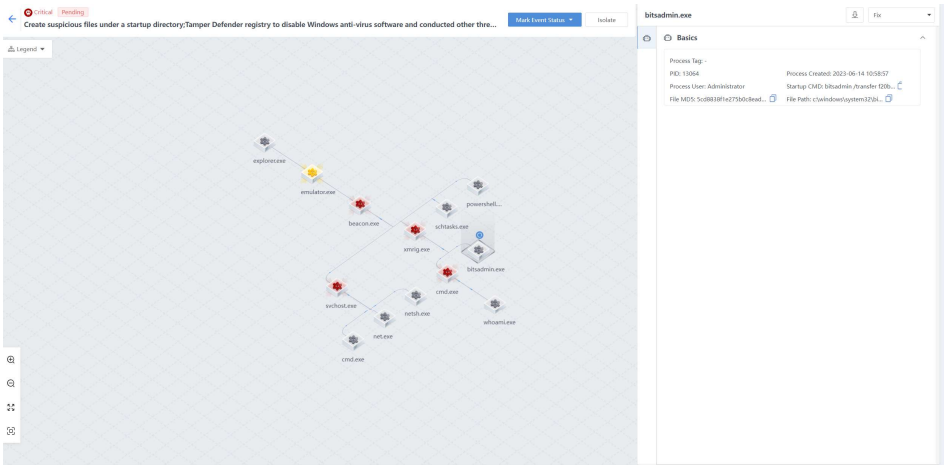
7. Check the permissions of the current user and gather sensitive information

The beacon.exe creates the xmrig.exe file and a process, calls the cmd /c whoami command to check the current user's permissions, and gathers sensitive information.



8. Download a mining virus for mining

beacon.exe creates xmrig.exe files and processes, and calls bitsadmin.exe to download a mining virus for mining.



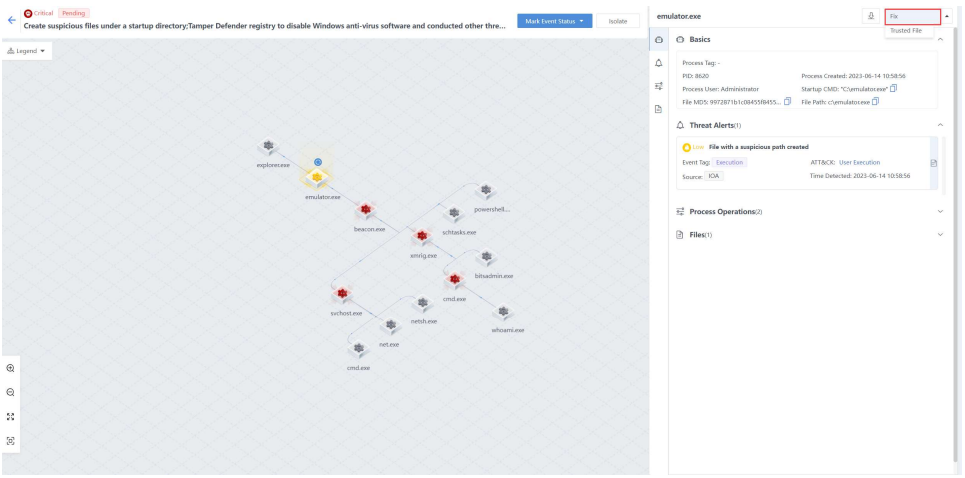
9. Handling of attacks

Through the traceability analysis of the above process attack chain, the conclusions are as follows:

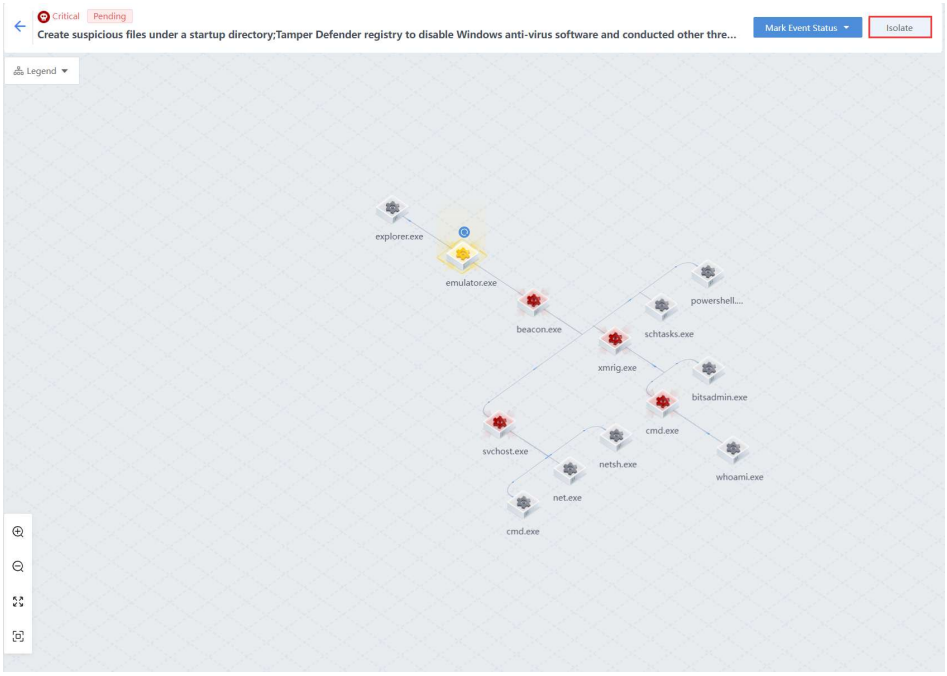
The testing machine is infected with a mining virus. The attack sample emulator.exe created the malicious files beacon.exe and xmrig.exe, and launched multiple processes to complete attacks such as execution, persistence, defense evasion, credential access, detection, and command and control.

The handling method is as follows:

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



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



- Perform a full investigation, kill the endpoint with the threat detected, and remove the remaining items.

a) The attacker obtained permissions and injected the virus via RDP access/brute-force attacks. Therefore, the following security enhancements are recommended:

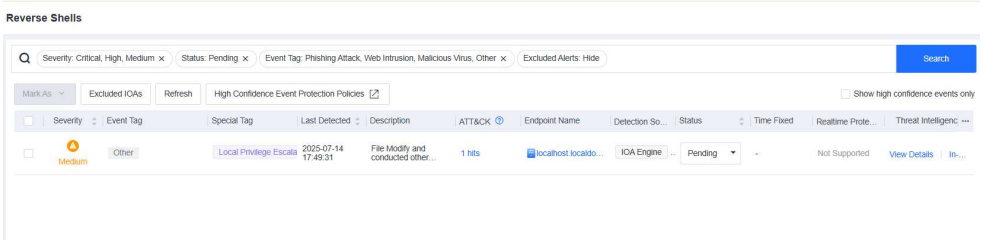
i. Disable unnecessary remote ports.

ii. Enable RDP secondary authentication and brute-force attack protection on NovaGuard.

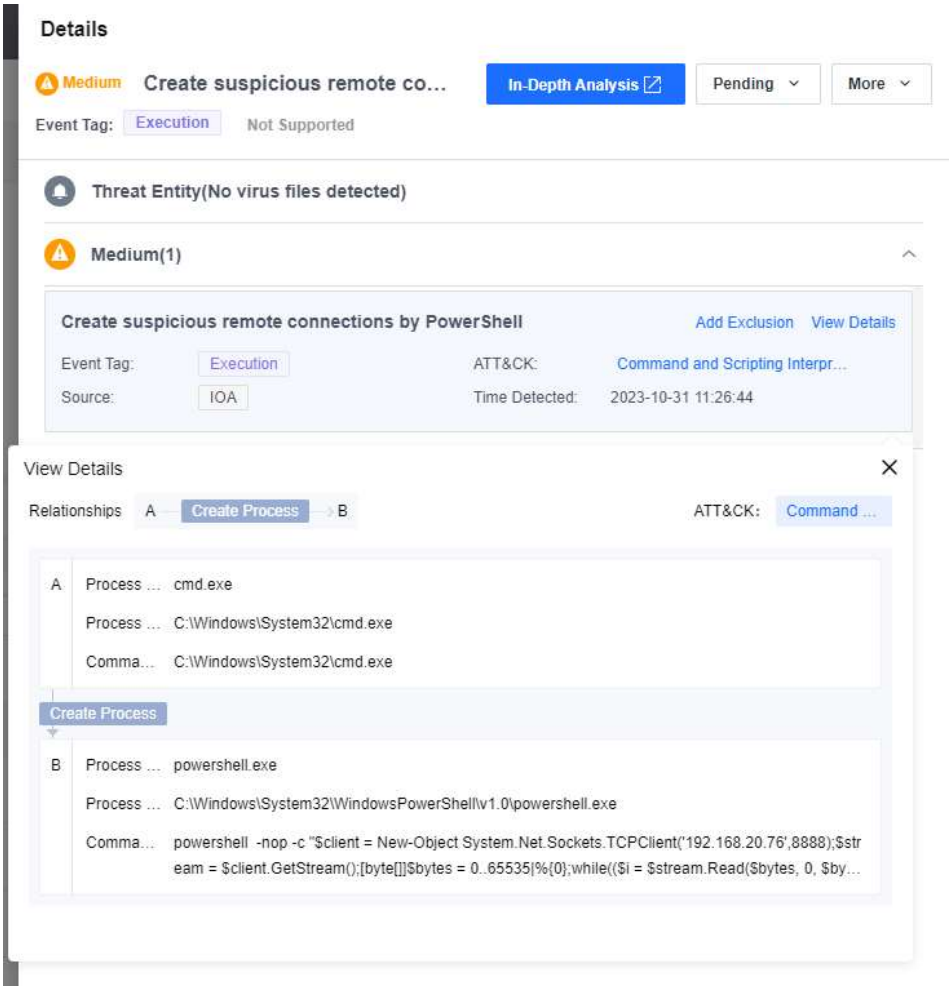
iii. Install system security patches in time.

4.2.1.8 Reverse Shells

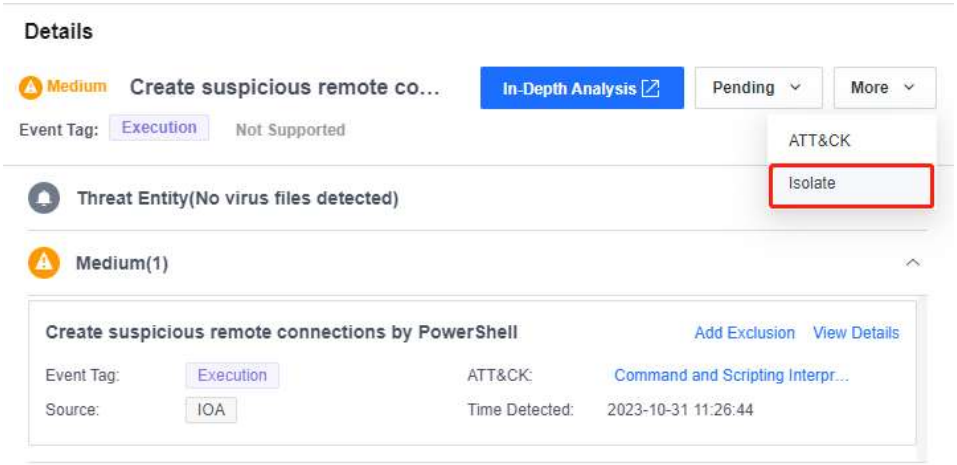
A reverse shell is a malicious activity in which the victim's host actively connects to applications on the attacker's server.



Click **View Details** to view the event details.

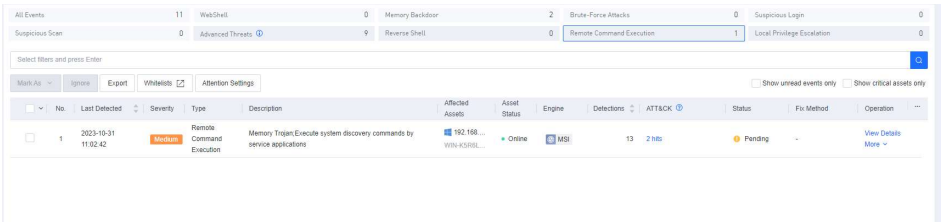


Click **More** > **Isolate** to isolate the endpoint.

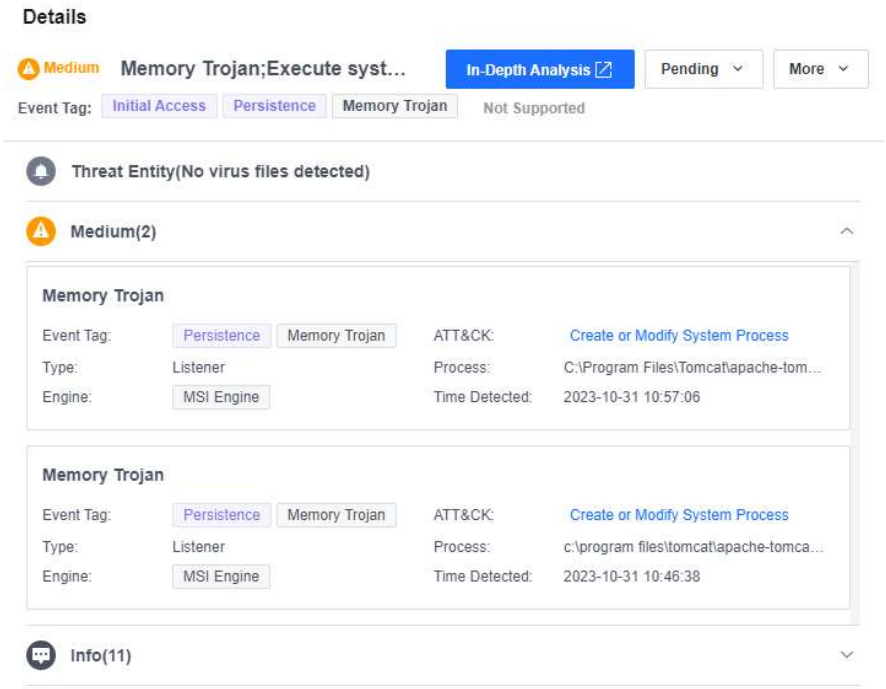


4.2.1.9 Remote Command Execution

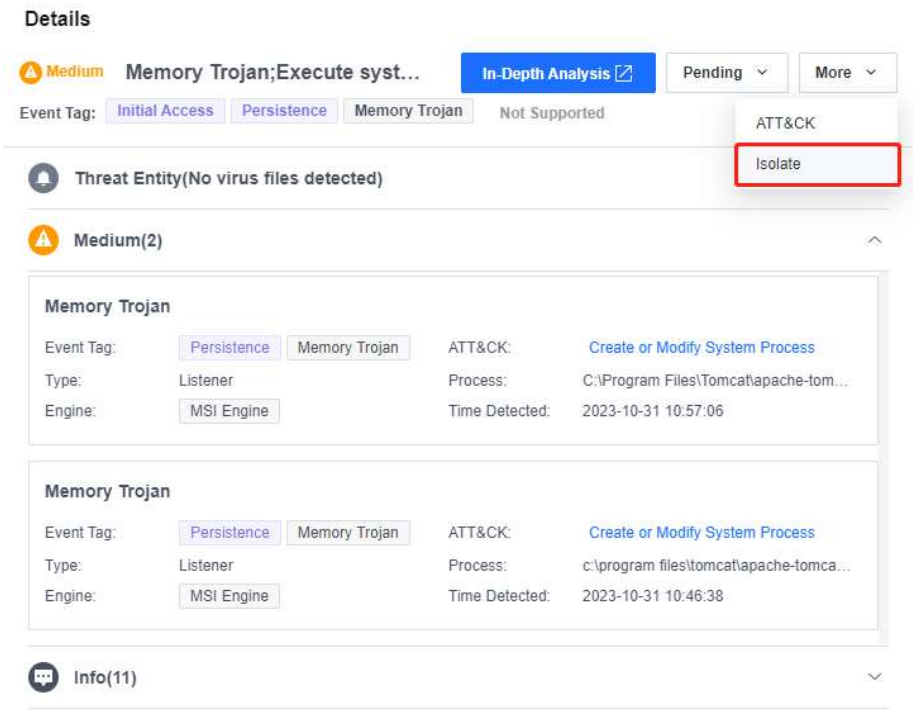
Remote Command Execution breaches business systems via Remote Command Execution vulnerabilities, enabling attackers to inject commands or code directly into backend servers.



Click **View Details** to view the event details.

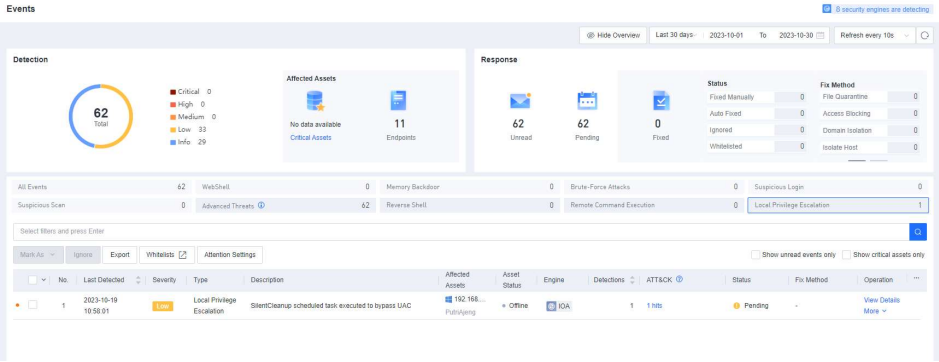


Click **More** > **Isolate** to isolate the endpoint.

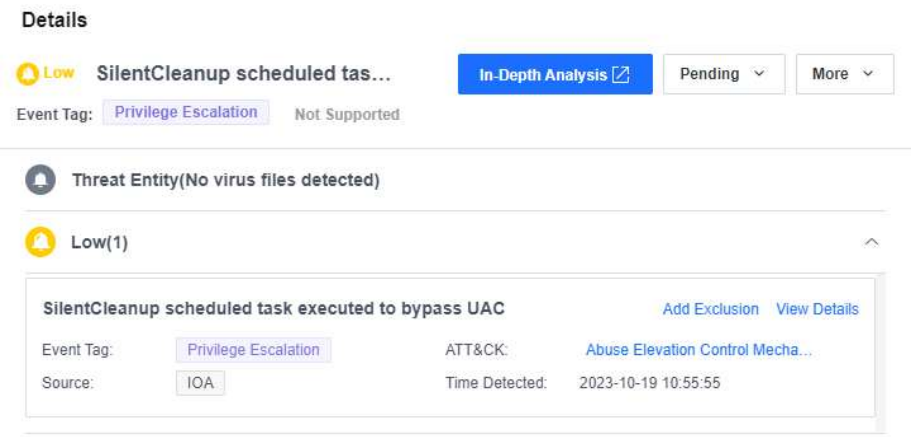


4.2.1.10 Local Privilege Escalation

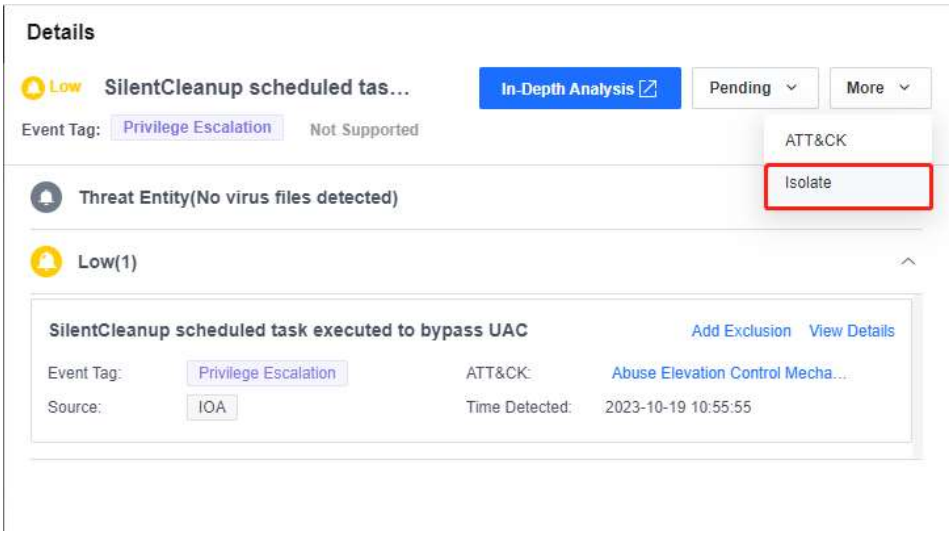
Local privilege escalation is an activity that involves elevating users' privilege with every low or restricted privilege to high or even root-level privilege.



Click **View Details** to view the event details.

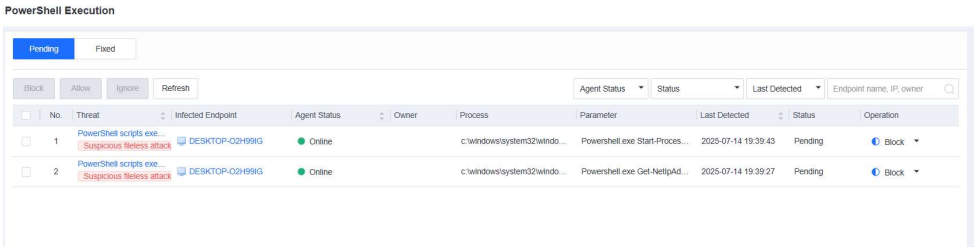


Click **More** > **Isolate** to isolate the endpoint.

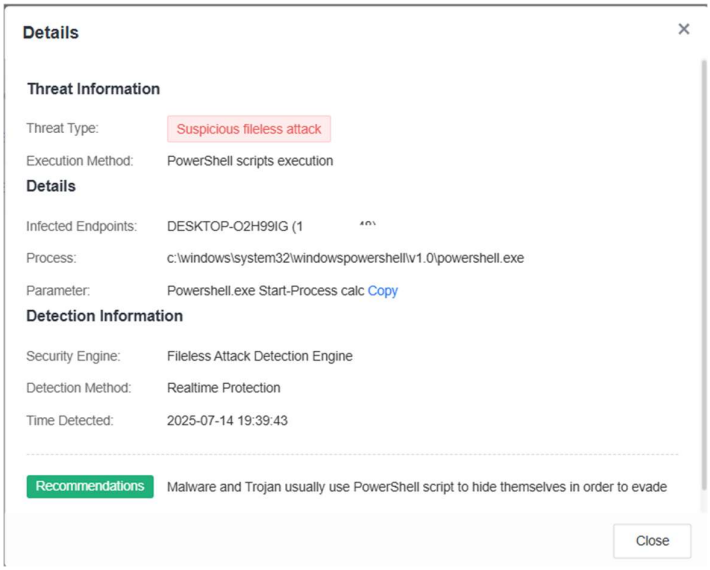


4.2.1.11 PowerShell Execution

PowerShell threats employ unusual attacking techniques that are difficult to detect, aiming to infect endpoints with viruses and cause damage.



Click the name of a threat to view the details of the relevant event, including the infected endpoints, process, parameters, and time detected.



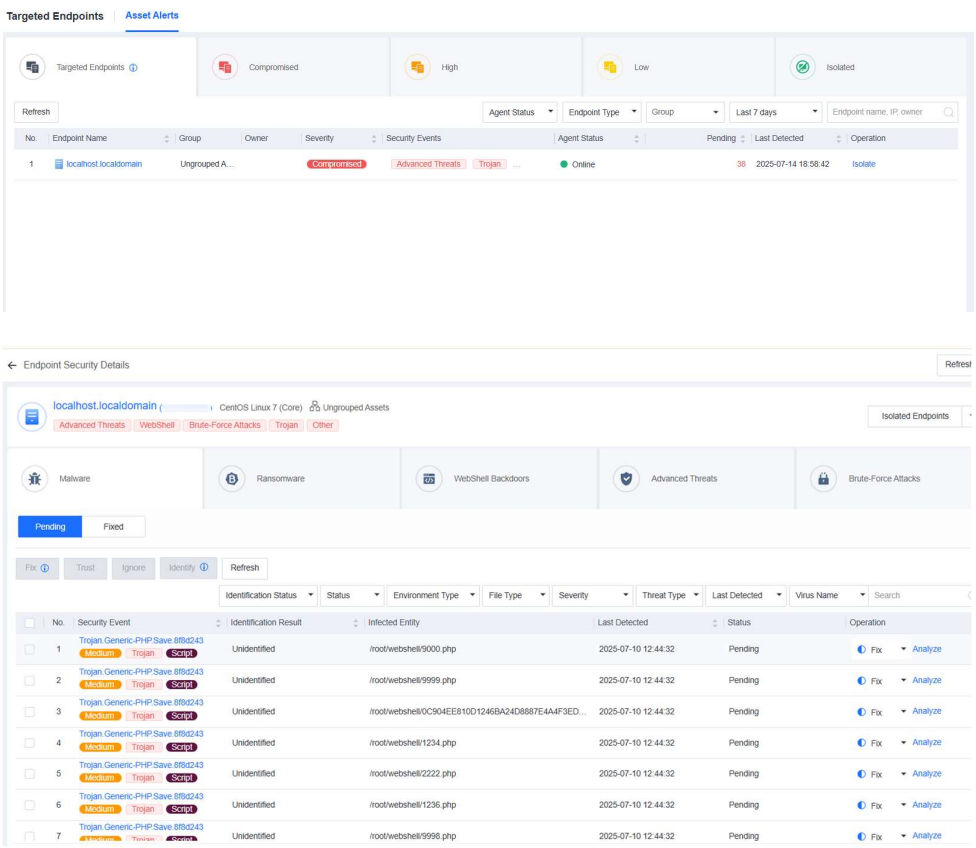
Click **Block** to block the current process.



Select **Also block execution of process with same commands on the endpoint** to prevent subsequent execution of processes with the same PowerShell parameters.

4.2.2 Target Endpoints

Go to **Detection and Response** > **Target Endpoints** and click **Asset Alerts** to view all risky endpoints. Click the name of an endpoint to enter the **Endpoint Security Details** page, where you can fix the relevant security events and isolate the endpoint, as shown in the figures below.

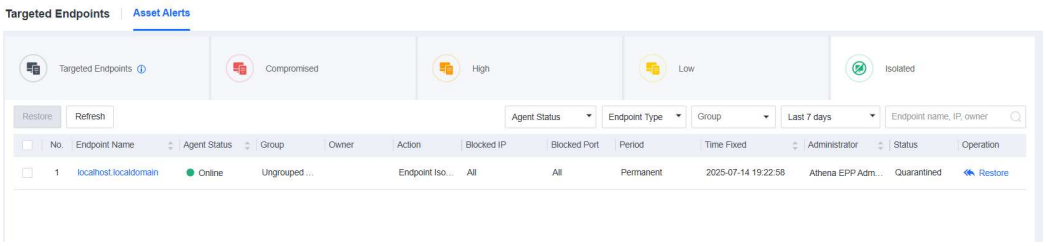


Risky endpoints are classified into the following three levels by severity:

- **Compromised**: Endpoints involved in critical threats and high-severity viruses, threats, WebShell backdoors.
- **High**: Endpoints involved in medium-severity viruses, threats, and brute-force attacks.
- **Low**: Endpoints involved in low-severity viruses, WebShell backdoors, and suspicious PowerShell executions.

You can filter endpoints by endpoint status, endpoint type, group, last detection time, endpoint name, or IP address as an administrator. For example, to fix security events for online endpoints only, you can filter endpoints by selecting **Online** for **Endpoint Status**.

You can isolate a detected risky endpoint. An isolated endpoint is restricted from accessing any network, ensuring no impact on business assets. You can also restore an isolated endpoint, as shown in the following figure.



4.2.3 Threat Hunting

Suppose you have known or obtained new threat intelligence from external sources. In that case, you can search for relevant information using simple combined conditions, such as IP address, domain name, and behavior. This allows you to initiate threat hunting across all endpoints in your network and identify endpoints and processes with potential threats, thus helping you detect new threats or possible risks in the network.

4.2.3.1 Search with a Single Condition

Search with a single condition includes search by domain name, network connection, executable file hash value, or file name.

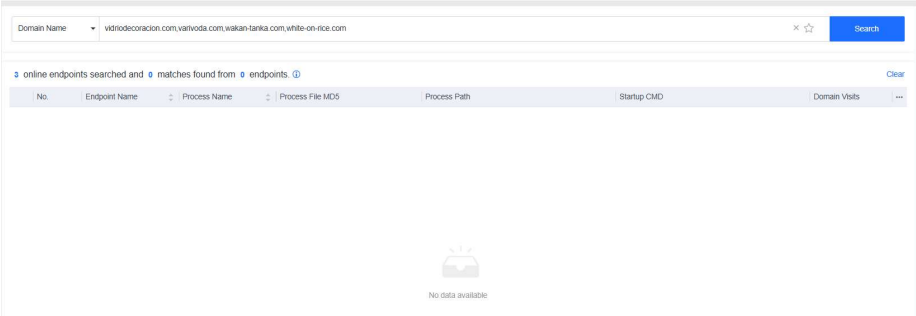
1. Search by **Domain Name**:

Enter one or more domain names separated by commas (,) to search for devices and activities communicating with the specified domain names. Fuzzy search using the wildcard (*) is supported.

Example: Use the domain names related to the Emotet virus to query potentially infected endpoints and the processes communicating with the Emotet domain names.

Search statement: vidriodecoracion.com,varivoda.com,wakan-tanka.com,white-on-rice.com

The query result is shown below.



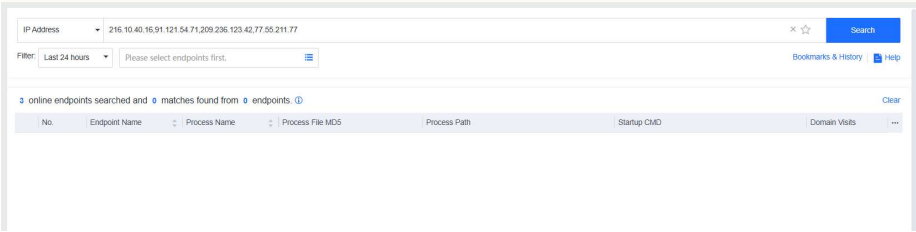
2. Search by **IP Address:**

Enter one or more IP addresses separated by commas (,) to search for endpoints with the network connection to/from the specified IP addresses and the corresponding processes.

Example: Use the IP addresses related to the Emotet virus to query potentially infected endpoints and the processes communicating with the IP addresses.

Search statement: 216.10.40.16,91.121.54.71,209.236.123.42,77.55.211.77

The query result is shown below.



3. Search by executable file **hash** value:

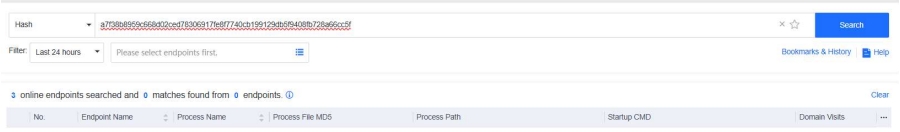
Enter one or more MD5 or SHA256 values of suspicious files separated by commas (,) to search process operation and module loading activities for endpoints matching the specified hash values and the corresponding processes.

Example: Use the SHA256 value of the file related to the Emotet virus to query potentially infected endpoints.

Search Statement:

a7f38b8959c668d02ced78306917fe8f7740cb199129db5f9408fb728a66cc5f

The query result is shown below.



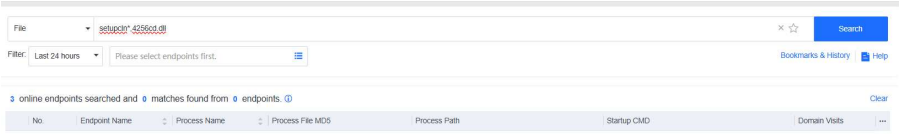
4. Search by **File** name

Enter one or more suspicious file names separated by commas (,) to search for related endpoints and events. Fuzzy search using the wildcard (*) is supported.

Example: Use malicious Emotet file names to query potentially infected endpoints.

Search Statement: setupcln*,4256cd.dll

The query result is shown below.



4.2.3.2 Search with Group Conditions

Multiple search conditions:

A search statement consists of the following elements: **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*"

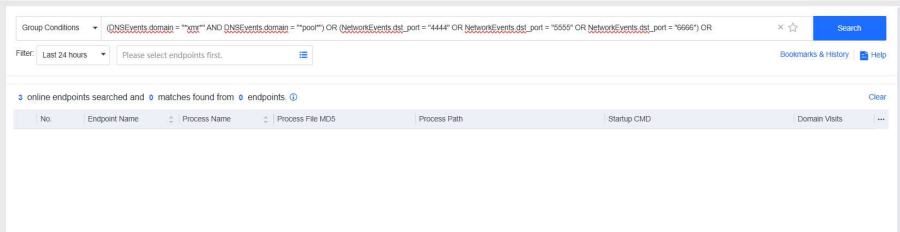
Example: Mining virus detection

Search Statement: (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.



Objects and fields

You can include the following objects in a set of conditions: Domain Name Access, Connection, Process Operation, File Operation, Loaded Module, and DeviceInformation. For details, see the following description:

Domain name 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	1d35014d937e02ee090a0cfc903ee6e6b1b65...
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

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	1d35014d937e02ee090a0cfc903ee6e6b1b65...
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	93d48bf194d87b190dc1fb9b8837011a58dc...
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	1d35014d937e02ee090a0cfc903ee6e6b1b65...
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	0ba37d0db6d5d74e9b1d8ebc540c1acd4a47...
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	1d35014d937e02ee090a0cfc903ee6e6b1b65...
process_commandline	Startup CMD	C:\Windows\system32\services.exe
process_user	Process User	NT AUTHORITY\SYSTEM

Loaded Module 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	92981d598dc950c191b0320955dd777fbac7...
process_id	Process ID	4305
process_name	Process Name	PING.EXE
process_md5	Process File MD5	f926bedd777fa0f4f71dd2d28155862a
process_SHA256	SHA256	1d35014d937e02ee090a0cfc903ee6e6b1b65...
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

Values

The value of a field must be enclosed with a pair of quotation marks (" "). Wildcards are supported: You can use a wildcard to represent one or more characters in a value. You can use an asterisk (*) to substitute zero, one, or multiple characters. The wildcard * can only be used together with the comparison operators "=" (equal) and "!=" (not equal).

Example: You can use mon* to represent the word "mongodb" or "mondodb".

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**, and **NOT**.

1. **AND**: AND means that both fields must be matched.

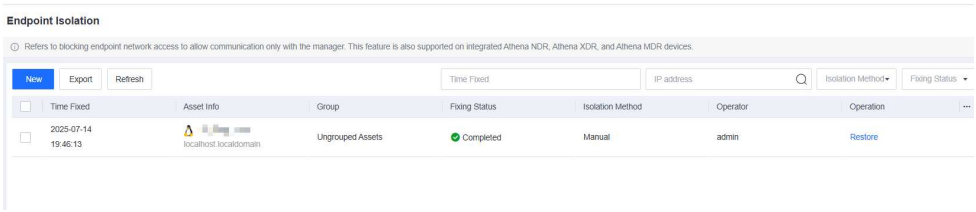
2. **OR**: OR means that at least one field must be matched.

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

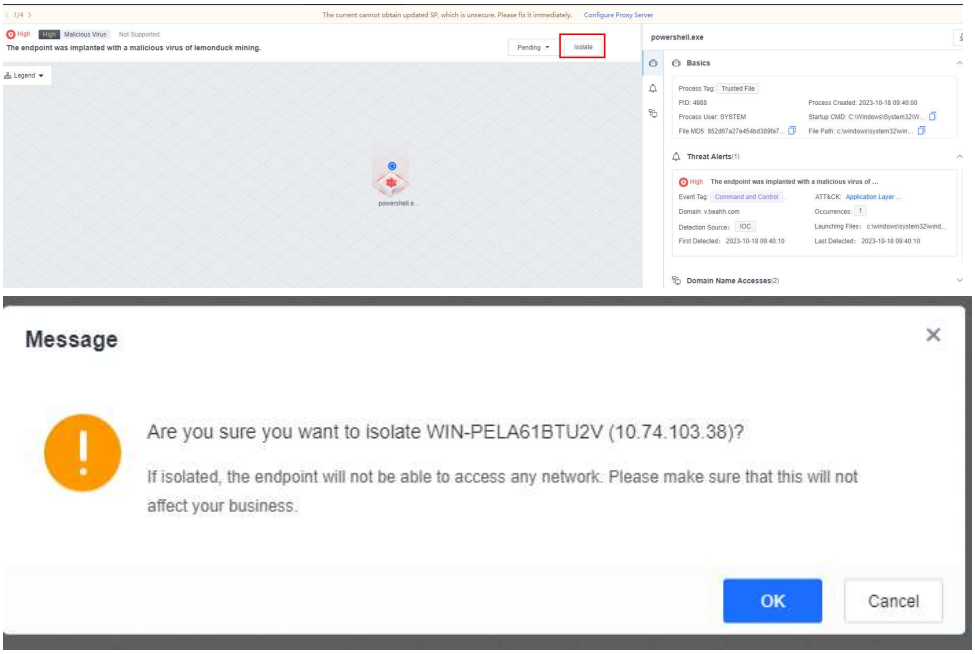
4.2.4 Response

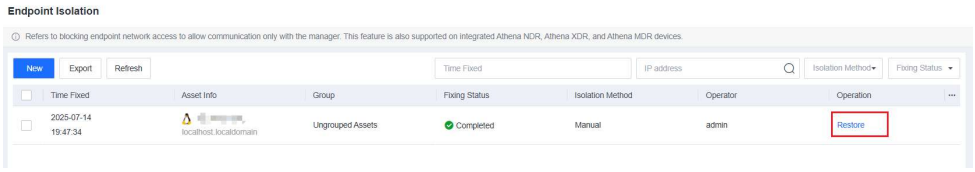
4.2.4.1 Endpoint Isolation

When NovaGuard detects a security event, it may classify the relevant endpoint as compromised or at high risk after identification. In this case, you can isolate the endpoint. An isolated endpoint can only communicate with the NovaGuard manager. All other inbound and outbound traffic for the endpoint is denied.

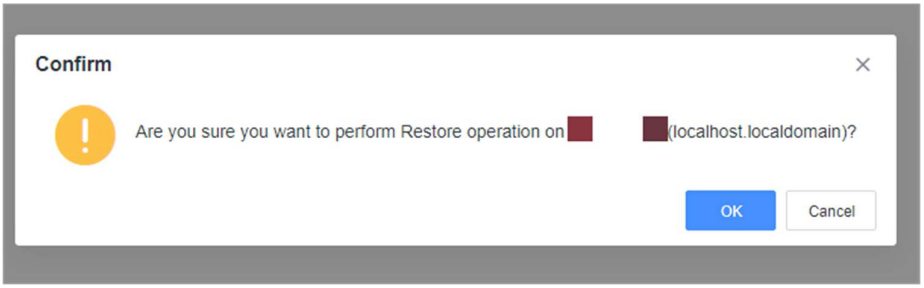


The following figures show an example of privilege escalation in advanced threats. To isolate the endpoint, click **Isolate**.

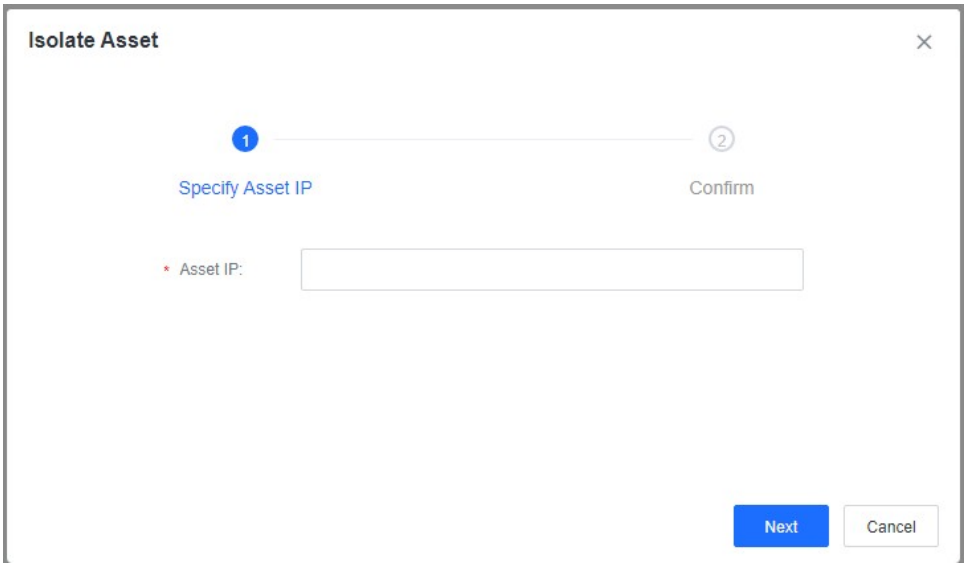




To cancel the isolation, click **Restore**.

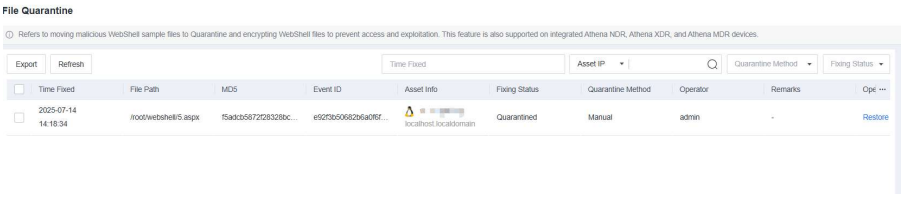


Administrators can also isolate an endpoint with NovaGuard agent installed as an administrator by clicking **New** and entering the IP address.



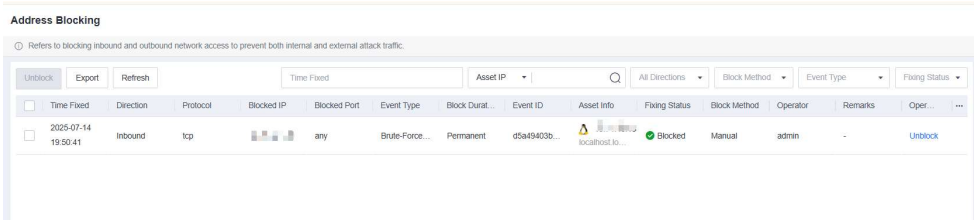
4.2.4.2 File Quarantine

This page displays logs of quarantined web shell files and file quarantine tasks issued when NovaGuard integrates with other platforms.



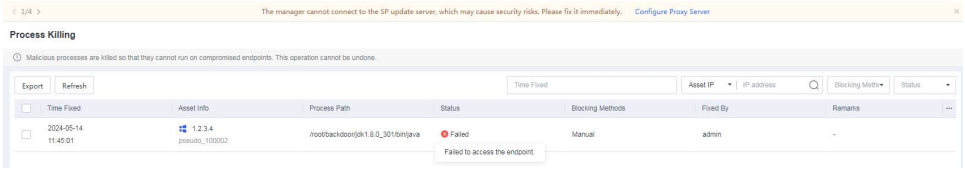
4.2.4.3 Access Blocking

You can configure an access control list (ACL) for a compromised endpoint to block access from attackers' IP addresses.



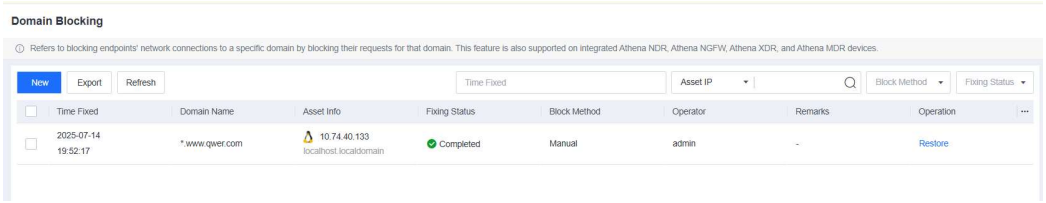
4.2.4.4 Process Killing

When NovaGuard detects a security event, it may classify the relevant endpoint as compromised or at high risk after identification. In this case, you can kill the processes running on the endpoint.



4.2.4.5 Domain Blocking

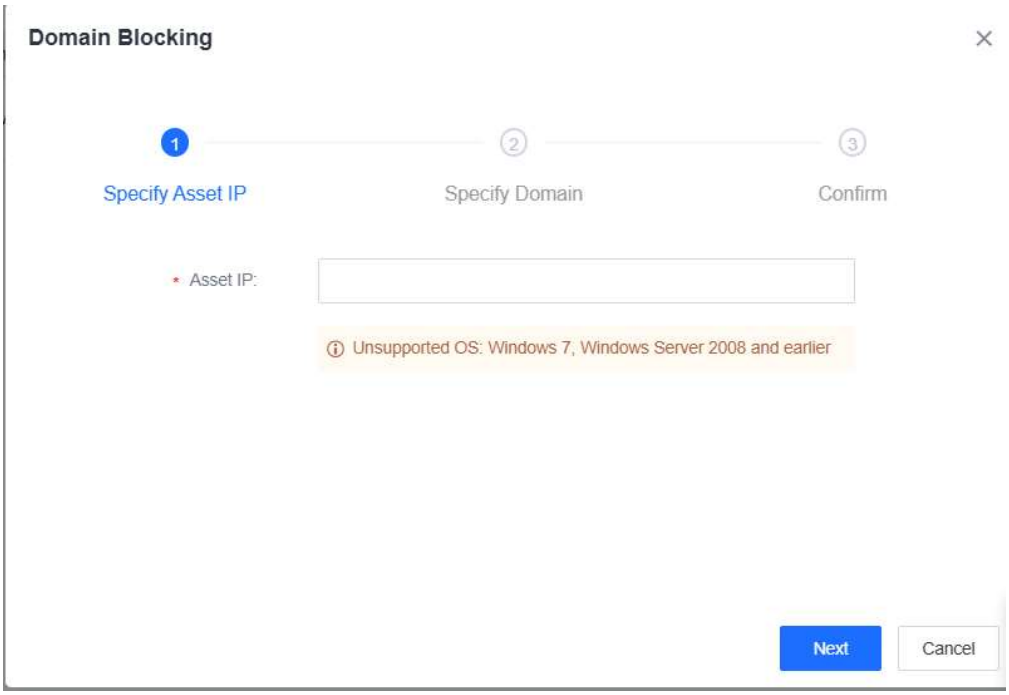
When NovaGuard detects a security event, it may classify the relevant endpoint as compromised or at high risk after identification. In this case, you can isolate the relevant domain name.



Click **New**, enter the IP address of the endpoint where the NovaGuard agent is installed, and specify the domain name or IP address to be isolated.

NOTE

This feature is unavailable for Linux operating systems, Windows Server 2008, or Windows Server 2003.

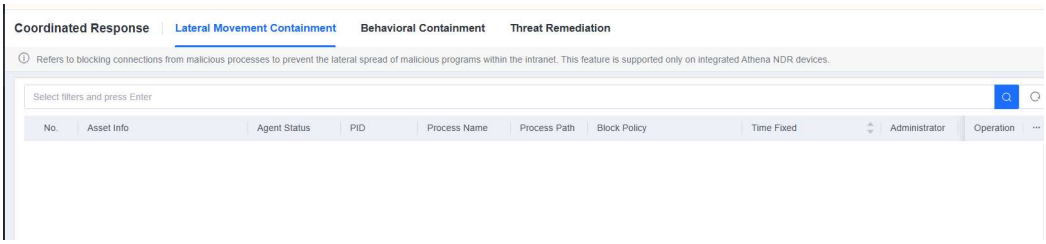


4.2.4.6 Coordinated Response

4.2.4.6.1 Lateral Movement Containment

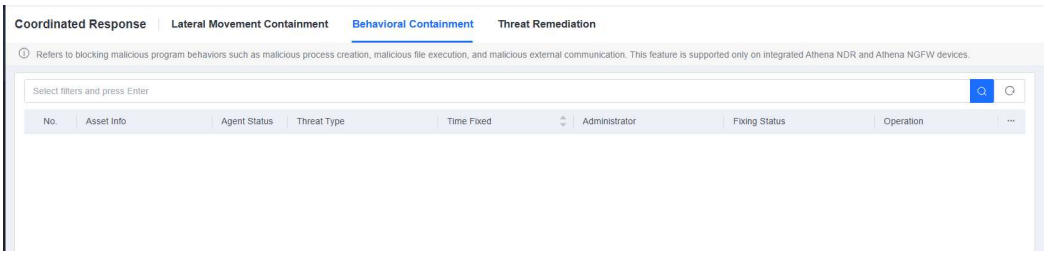
This page displays the logs of network port-blocking tasks issued when NovaGuard integrates with Network Secure and NovaCommand. You can

cancel the blocking on NovaGuard as an administrator.



4.2.4.6.2 Behavioral Containment

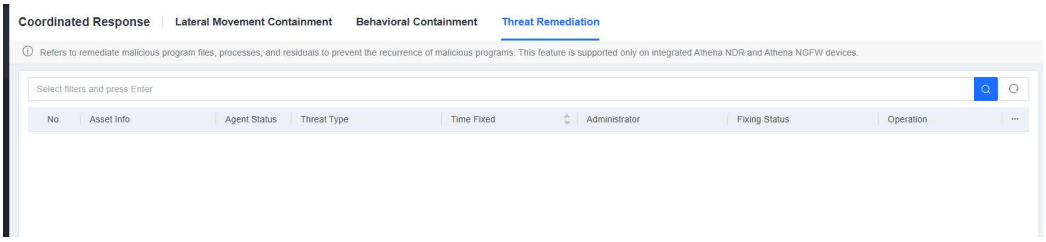
This page displays the logs of domain names and process-blocking tasks issued when NovaGuard integrates with Network Secure and NovaCommand. You can view the logs on NovaGuard as an administrator.



4.2.4.6.3 Threat Remediation

This page displays the logs of malicious file removal and rollback tasks issued when NovaGuard integrates with Network Secure and NovaCommand. You can view the logs on NovaGuard as an administrator.

For threats that have been removed, you can click **Remediation Details** to view the details. Meanwhile, the administrator can click **Roll Back** on NovaGuard to initiate a rollback.



4.3 Risk Assessment

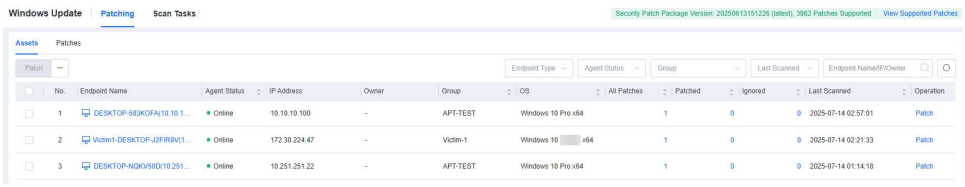
4.3.1 Windows Update

On the **Windows Update** page, you can view the frequently reported Windows vulnerabilities from the perspectives of assets and patches. In addition, you can select endpoints or patches and handle them as an administrator.

4.3.1.1 Patching

4.3.1.1.1 Assets

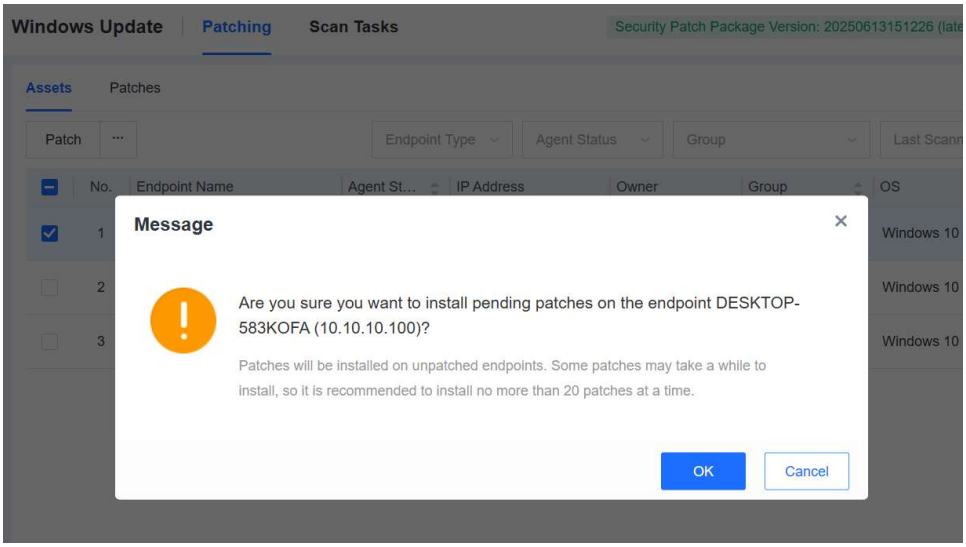
On the **Assets** tab, you can view the Windows patching statistics of endpoints, including the total number of patches, the number of installed patches, etc.



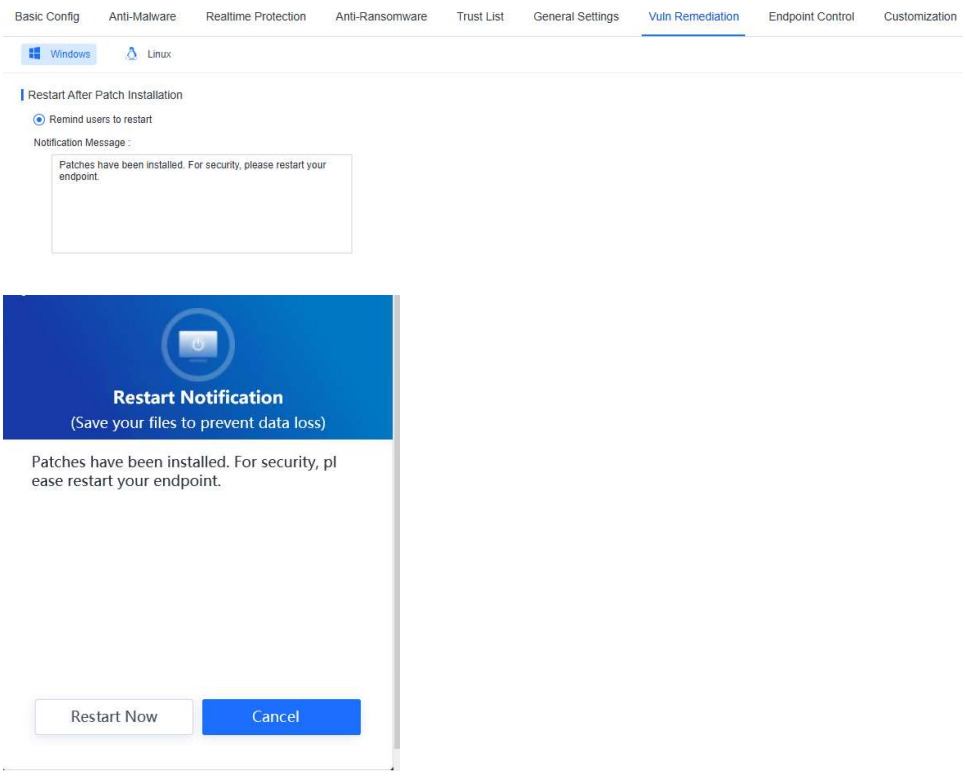
Select an endpoint and click **Patch** in the upper-left corner. Then, the corresponding patches will be pushed to the endpoint.

NOTE

Patches will be installed only on endpoints that are unpatched or failed to be patched. Some patches may take a long time to install. Therefore, we recommend that you install no more than 20 patches at a time.

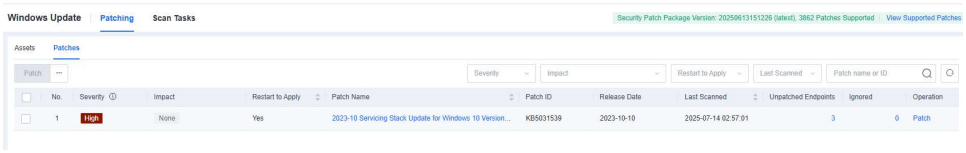


You can go to **Policies** > **General Policies** > **Vuln Remediation** and select **Remind users to restart** under **Restart After Patch Installation** as an administrator. This way, after the patches are successfully installed on the endpoint, a notification message will appear to prompt the endpoint user to restart the endpoint. The notification message can be customized as needed.



4.3.1.1.2 Patches

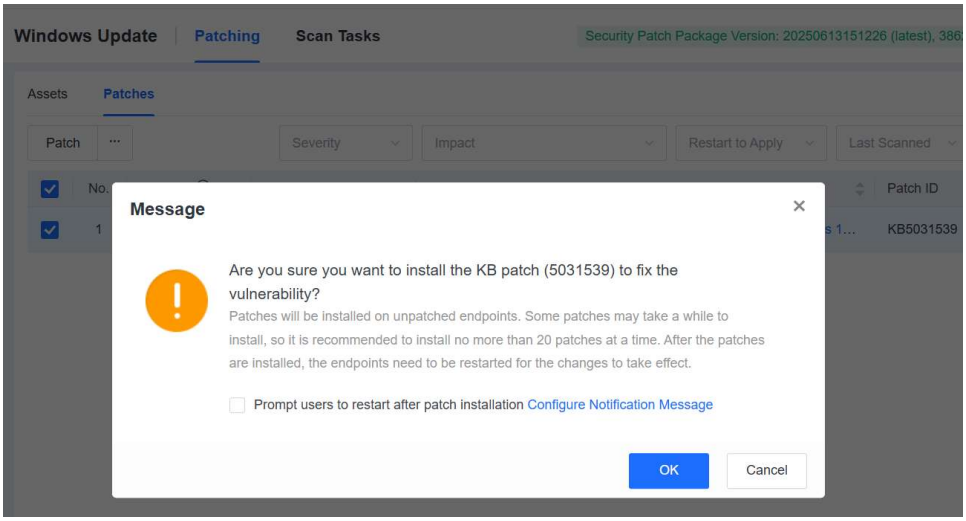
On the **Patches** tab, you can view the number of unpatched endpoints for a specific Windows patch, severity, impact type, whether an endpoint restart is needed to apply the patch, release date, etc.



Select a patch and click **Patch** in the upper-left corner. Then, the patch will be pushed to the corresponding endpoints.

NOTE

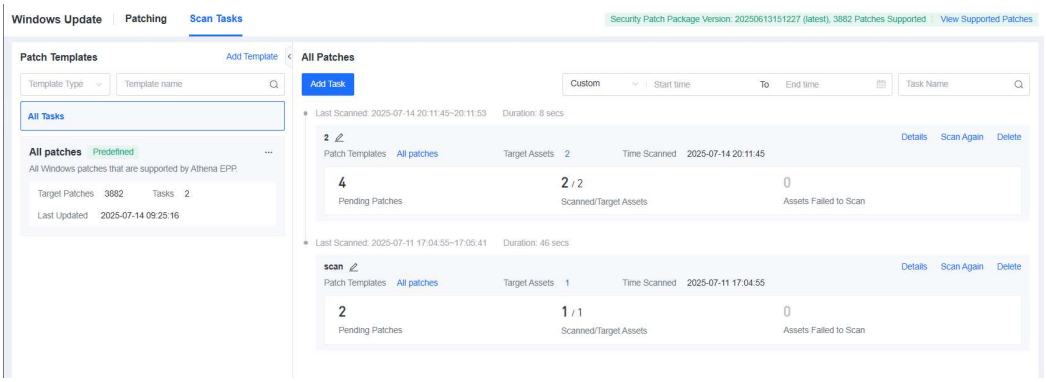
Patches will be installed only on endpoints that are unpatched or failed to be patched. Some patches may take a long time to install. Therefore, we recommend that you install no more than 20 patches at a time.



If **Remind users to restart** is selected, the corresponding endpoint users will receive a notification message prompting them to restart the endpoints after patch installation. The notification message is the same as the notification message that is prompted after patch installation when **Patch** on the **Assets** tab is clicked.

4.3.1.2 Scan Tasks

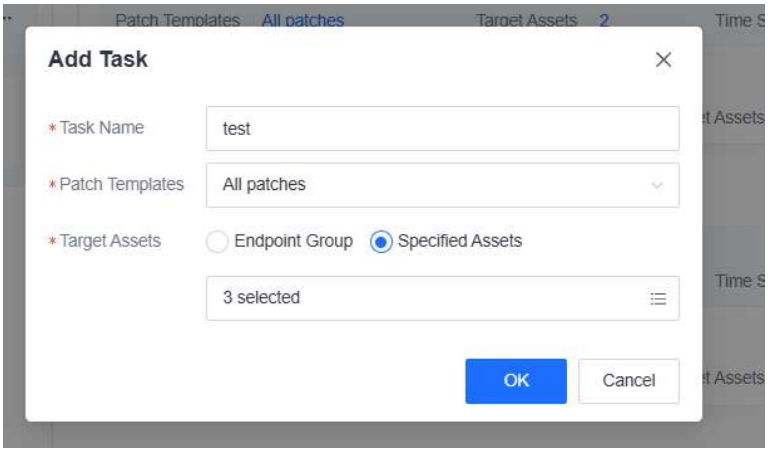
On the **Scan Tasks** tab, you can view the patch template statistics, such as the number of patches included in the predefined patch library, the time when the patch library was last updated, and other key information. In addition, you can create scan tasks for specific endpoint groups or endpoints to scan the vulnerabilities on the endpoints groups or endpoints.



Steps

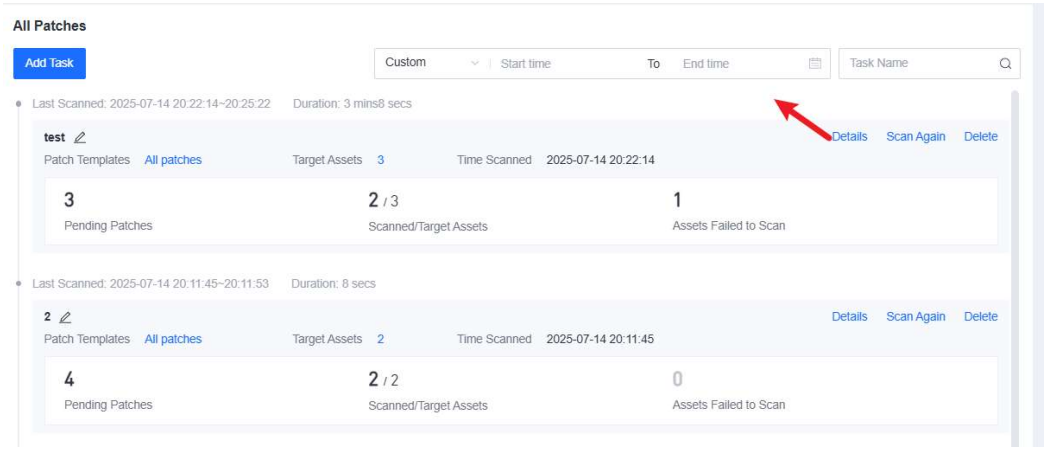
Step 1. Click **Add Task** to create a scan task. In the **Add Task** dialog box, configure the following parameters:

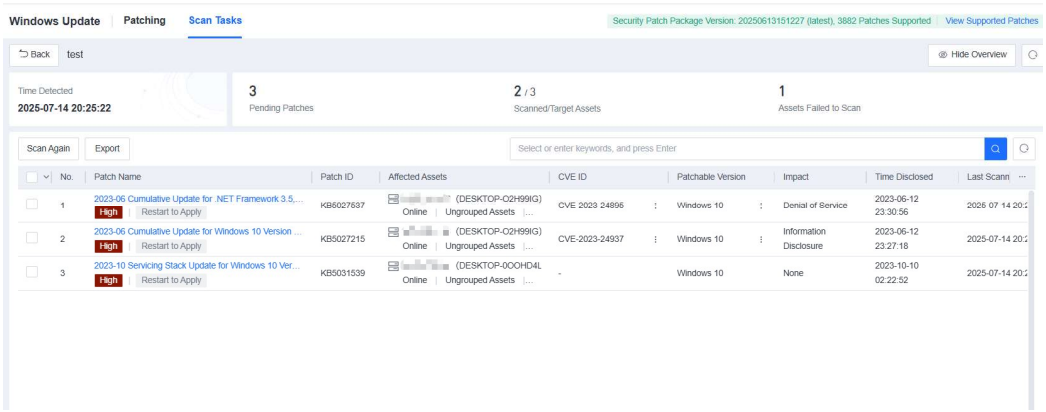
- **Task Name**: Specify the name of the scan task.
- **Patch Templates**: Select a patch template.
- **Target Assets**: Select the endpoint group or endpoint to which this scan task will apply.



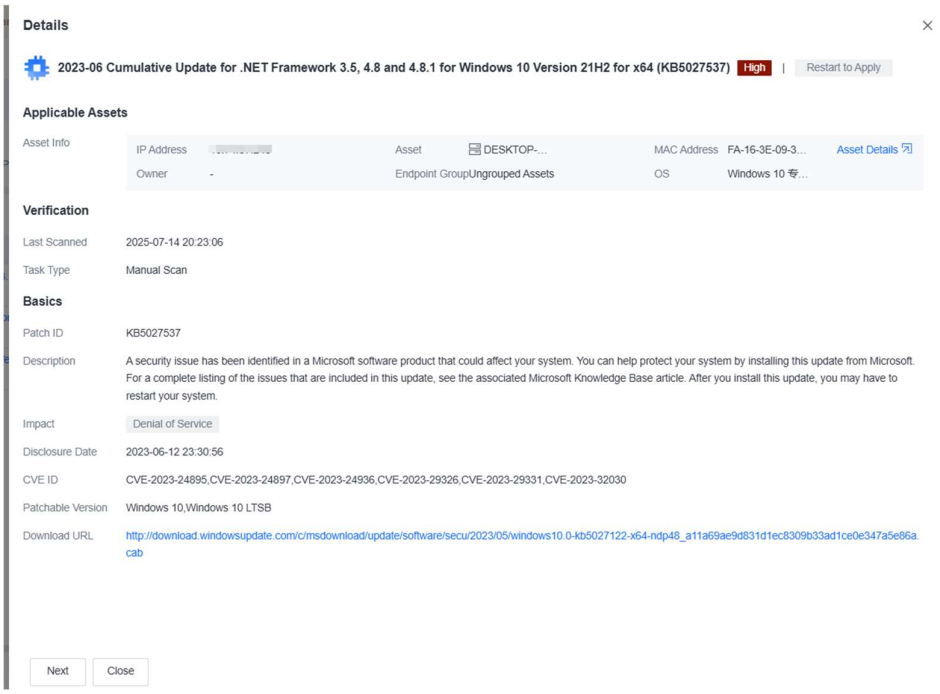
Then, click **OK**. The scan task is created and automatically executed.

Step 2. After the scan task is completed, click **Details** to view the scan result.





Step 3. Click the name of a patch to view the corresponding details, including the asset information, last scan time, patch ID, impact, disclosure date, patchable version, patch download URL, etc.

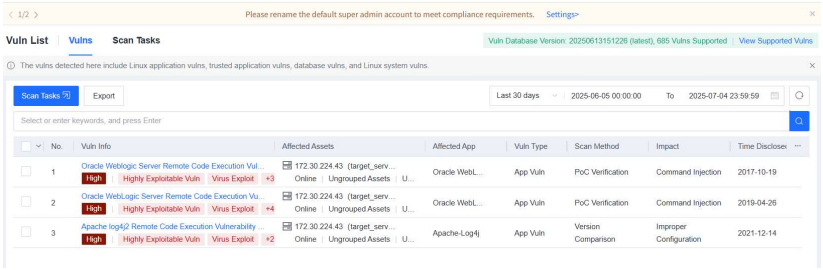


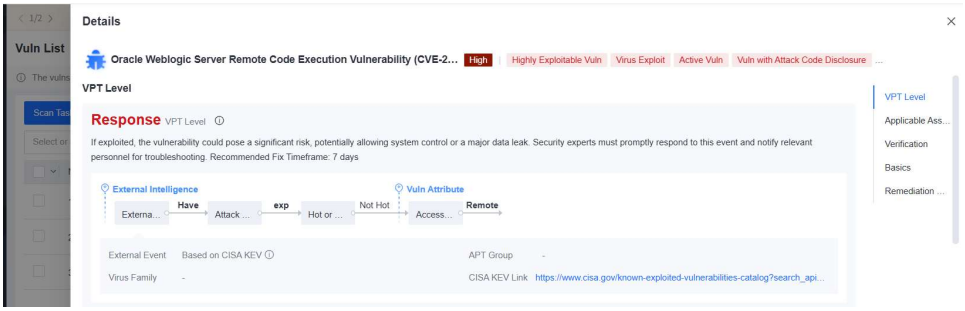
4.3.2 Vulnerabilities

4.3.2.1 Vuln List

4.3.2.1.1 Vulns

On the **Vulns** tab, you can view the detected vulnerabilities, including Linux application vulnerabilities, database vulnerabilities, and Linux system vulnerabilities.

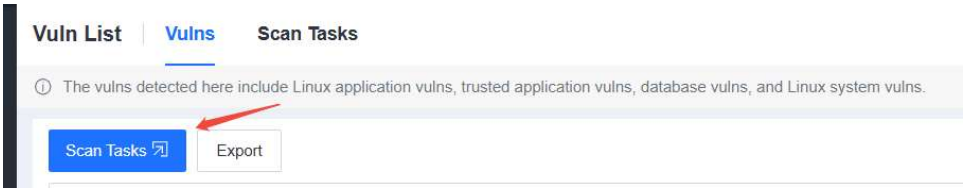



Details
Vuln List
Oracle Weblogic Server Remote Code Execution Vulnerability (CVE-2...
High
Highly Exploitable Vuln
Virus Exploit
Active Vuln
Vuln with Attack Code Disclosure
VPT Level
Response
VPT Level
If exploited, the vulnerability could pose a significant risk, potentially allowing system control or a major data leak. Security experts must promptly respond to this event and notify relevant personnel for troubleshooting. Recommended Fix Timeframe: 7 days
External Intelligence
Have
exp
Not Hot
Vuln Attribute
Remote
Externa...
Attack ...
Hot or ...
Access...
External Event
Based on CISA KEV
Virus Family
APT Group
CISA KEV Link
https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search_api...
VPT Level
Applicable Ass...
Verification
Basics
Remediation ...

4.3.2.1.2 Scan Tasks

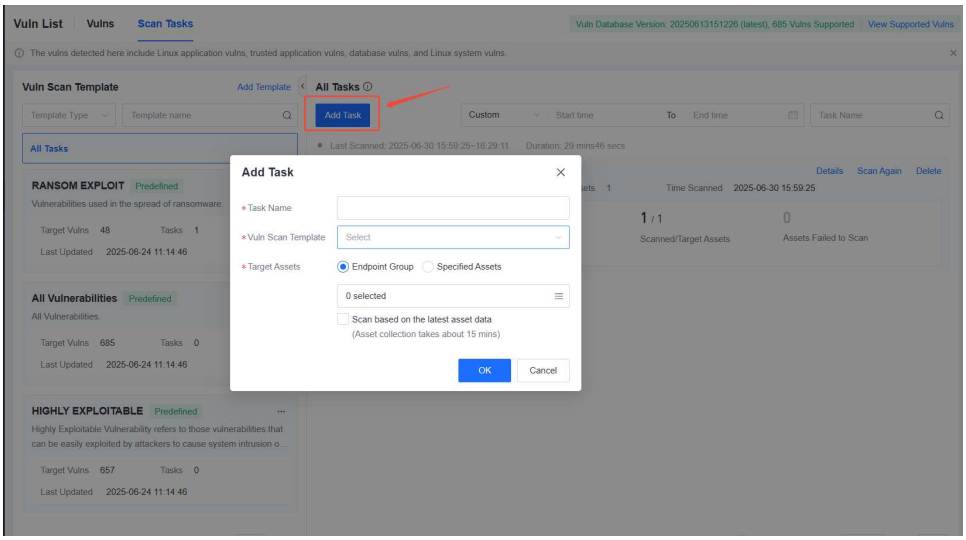
Steps

Step 1. On the **Vulns** tab, click **Scan Tasks** to go to the **Scan Tasks** tab. Then, click **Add Task**.

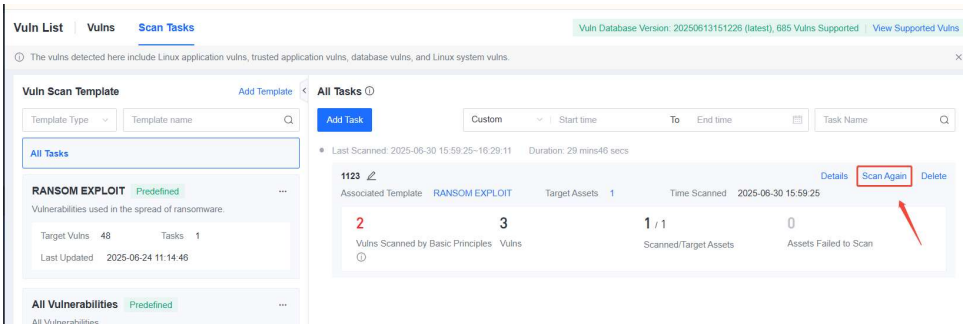


In the **Add Task** dialog box that appears, configure the following parameters:

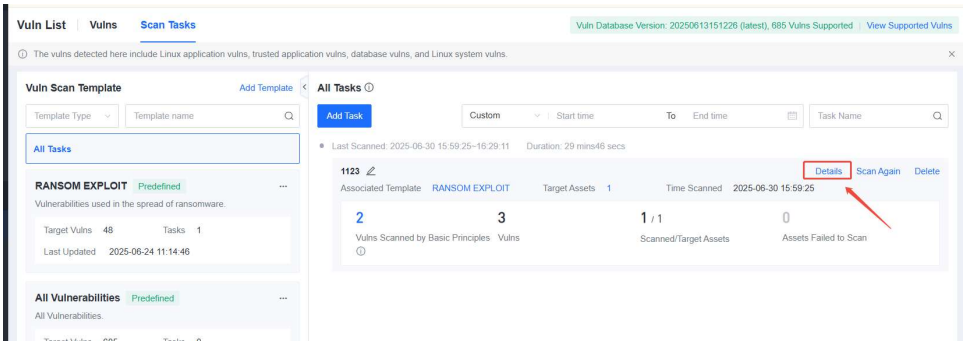
- **Task Name**: Specify the name of the scan task.
- **Vuln Scan Template**: Select a vulnerability scan template.
- **Target Assets**: Select the endpoint group or endpoint to which this scan task will apply.

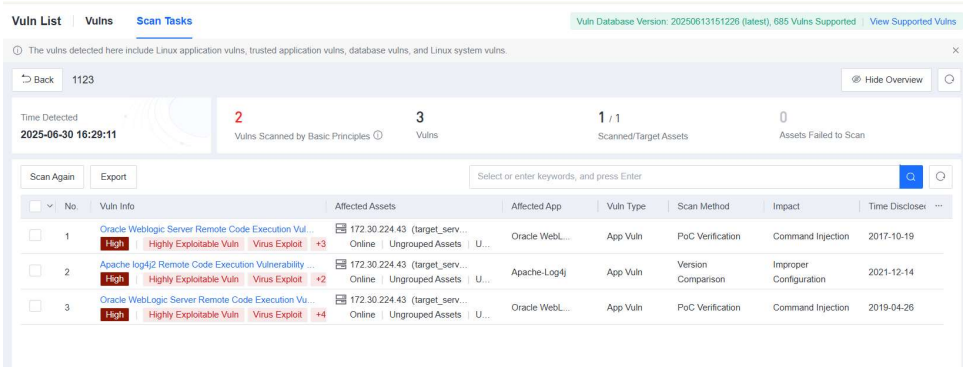


Step 2. Click **OK**. The scan task is created and automatically executed. If you need to conduct a scan again, click **Scan Again**.



Step 3. After the scan task is completed, click **Details** to view the scan result.





4.3.3 Compliance Checks

The Security Compliance module is for endpoints' compliance checks. The check content varies depending on the endpoint operating system.

4.3.3.1 Tasks

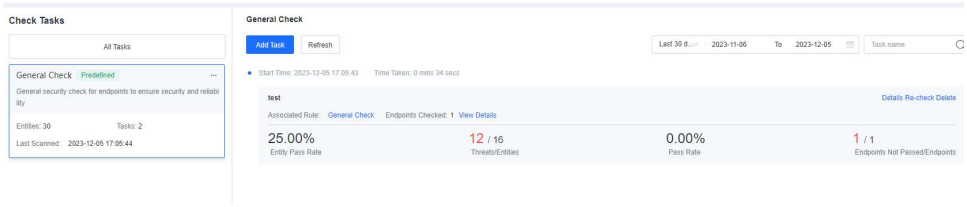
The supported security compliance check is as follows:

Windows endpoints: account policy, access control, security audit, history information protection, intrusion prevention, and malicious code prevention.

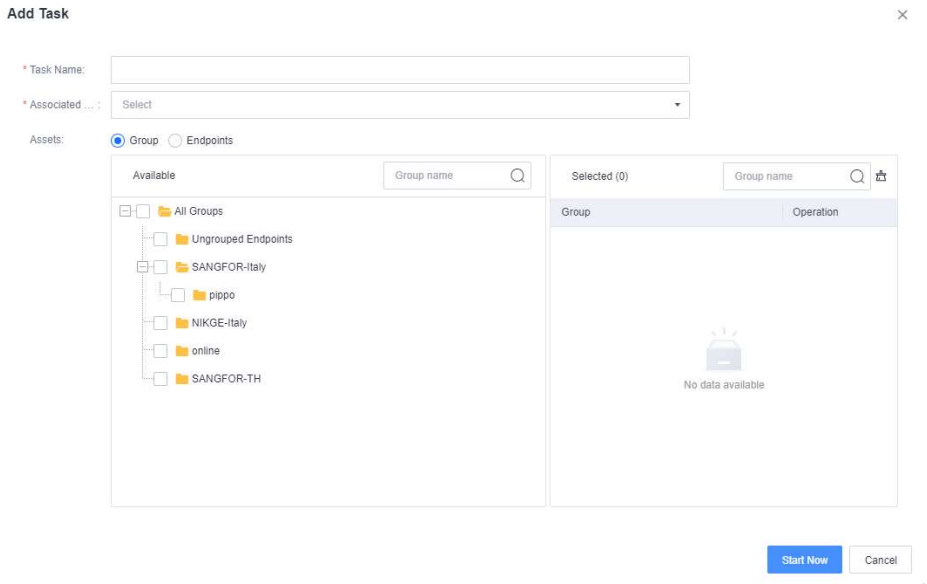
Linux endpoints: account policy, access control, security audit, SSH policy detection, intrusion prevention, and malicious code prevention.

Mac endpoints: not supported.

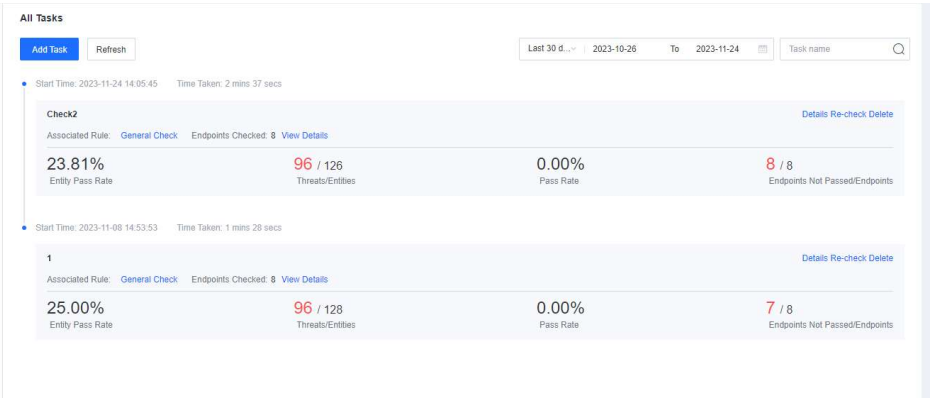
The following figure shows the configuration page.



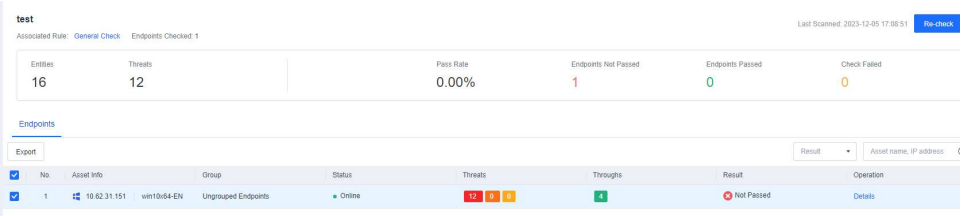
Click **Add Task** and select endpoints for which a compliance check is required, as shown in the following figure.



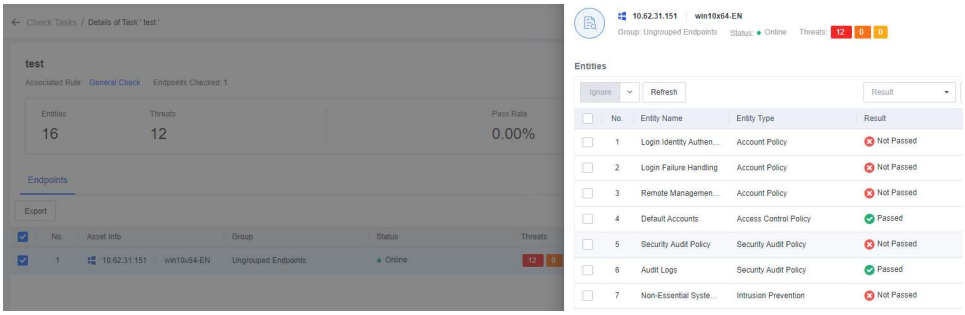
After detection is complete, you can view the detection result.



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



Click **Details** 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 **Export** to download the compliance check data.

4.4 Defense

4.4.1 Malware Scan

You can issue scan tasks from the NovaGuard manager to identify suspicious files on endpoints. The scan operation uses various engines, including Local Reputation Database, ForeNova Engine Zero, Behavioral Analytics Engine, Gene Analytics Engine, and Cloud-Based Engine.

Virus scan tasks include three types: quick scan, full scan, and forced scan. To select a task type, move the pointer over the **Quick Scan** button. The following table outlines the differences between these three task types.

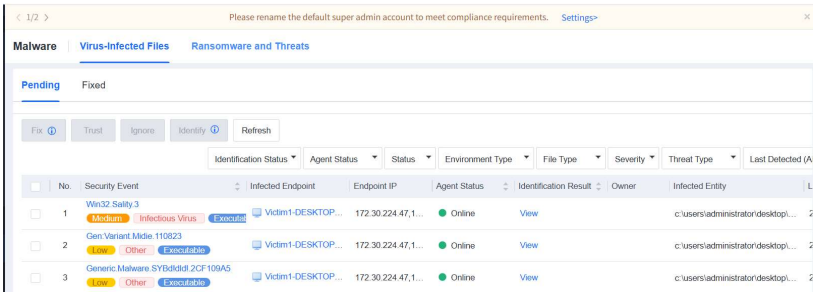
Full Scan	Scans all files on the endpoint hard disks.
Quick Scan	Scans important file directories on the system disk, which include the following ones on different operating systems: **Windows**:

	/Windows, /Windows/system32, and private directories under /Windows/system32 /Windows/system32/drivers and its subdirectories **Linux**: /bin, /sbin, /usr/sbin, /usr/bin, /lib, /lib64, /usr/lib/usr/lib64, /usr/local/lib, /usr/local/lib64, /tmp, /var/tmp, /dev, and /proc **macOS**: /private/tmp, /Users/[Current account name]/Downloads, /Users/[Current account name]/Desktop, /Users/[Current account name]/Documents
Forced Scan	For stubborn viruses, you can use the dedicated tool on the NovaGuard manager to handle viruses in bulk. It helps you respond rapidly to widespread, stubborn viruses. Currently, this feature applies to Windows systems only.

4.4.1.1 Malware

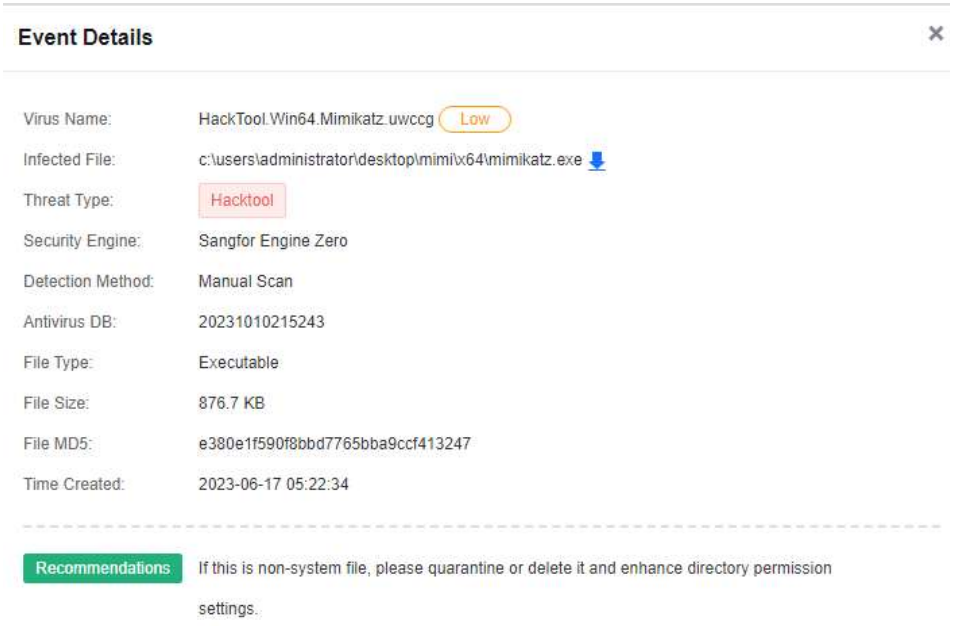
4.4.1.1.1 Virus-Infected Files

Go to **Defense > Malware Scan > Malware** to find the details of detected security events, including malware, ransomware, cryptomining, backdoor programs, and worms, as shown in the following figure.



You can also filter security events by endpoint status, handling status, file type, severity, threat type, last detection time, and endpoint name/IP address/virus name/file path as an administrator. For example, to handle online security events only, filter events by selecting **Online** for **Endpoint Status**.

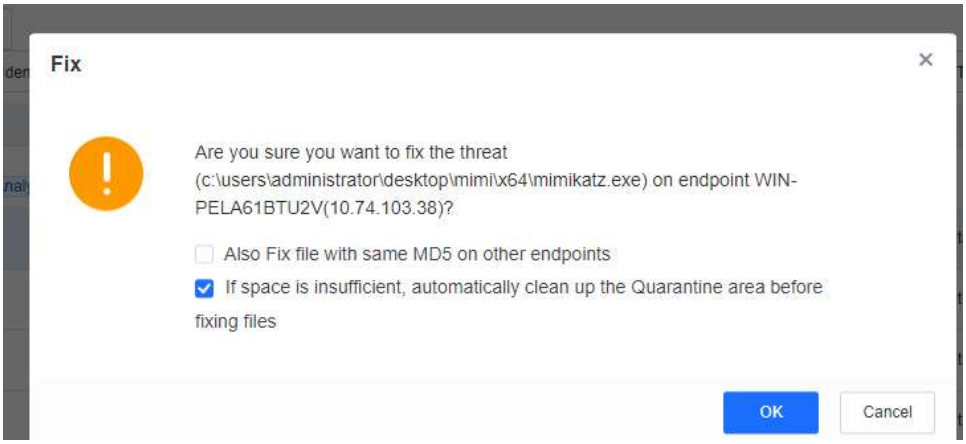
Click the name of a security event to check its details, as shown in the following figure.



Pending:

The **Pending** tab displays a list of pending security events. Under the **Operation** column, you can click **Fix**, **Trust**, or **Ignore** to handle the event. For example, for an infected file you want to quarantine, click **Fix** for the

corresponding event, as shown in the following figure.



Select **Also Fix file with same MD5 on other endpoints** to fix the same infected file on other endpoints in bulk.

If you select the **If space is insufficient, automatically clean up the Quarantine area before fixing files**, the files in the Quarantine area will be automatically cleaned up if the number of files in the Quarantine area has reached the upper limit.

NOTE

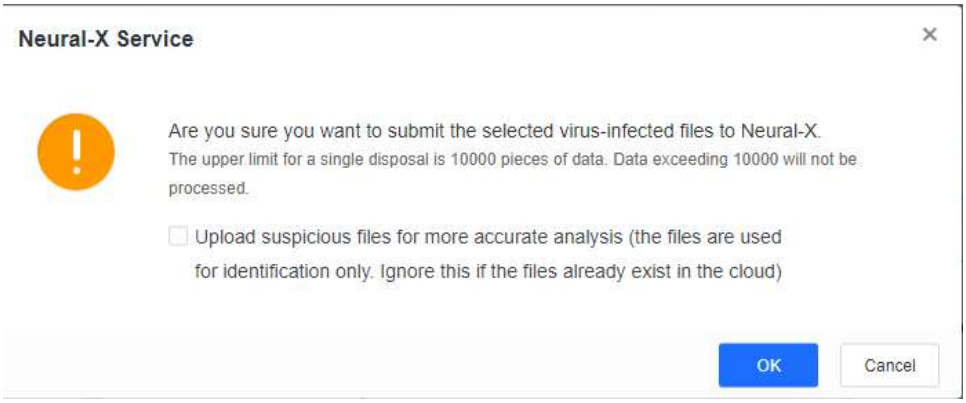
If the **If space is insufficient, automatically clean up the Quarantine area before fixing files** is selected, half of the files in the Quarantine area will be automatically cleaned up sequentially.

If you are unsure whether a file is malicious, click **Identify** or **Analyze** to submit the file to Neural-X Threat Intelligence for further analysis and identification.

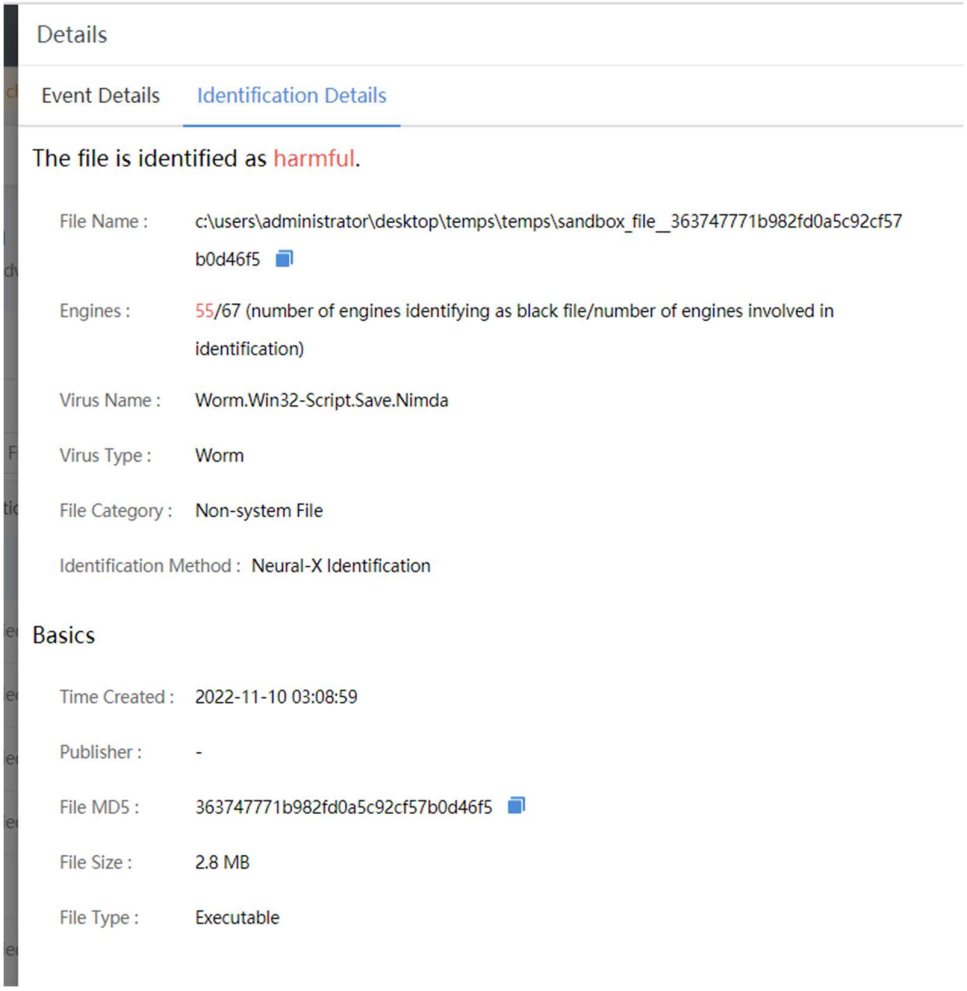
The Neural-X service provides file identification capabilities backed by security experts, sandboxes, and engines, and analyzes files using a Cloud-Based Engine and the collected intelligence. It provides more accurate identification results and a closed-loop approach to event handling.

When the NovaGuard manager is connected to the Internet, any detected infected files are automatically identified by Neural-X, which will then provide

relevant results. In cases where files cannot be automatically identified, you can manually submit them to Neural-X for identification.

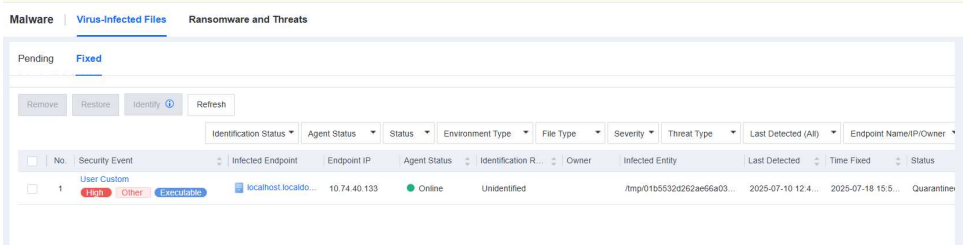


After identification is complete, click **View** to review the identification details.

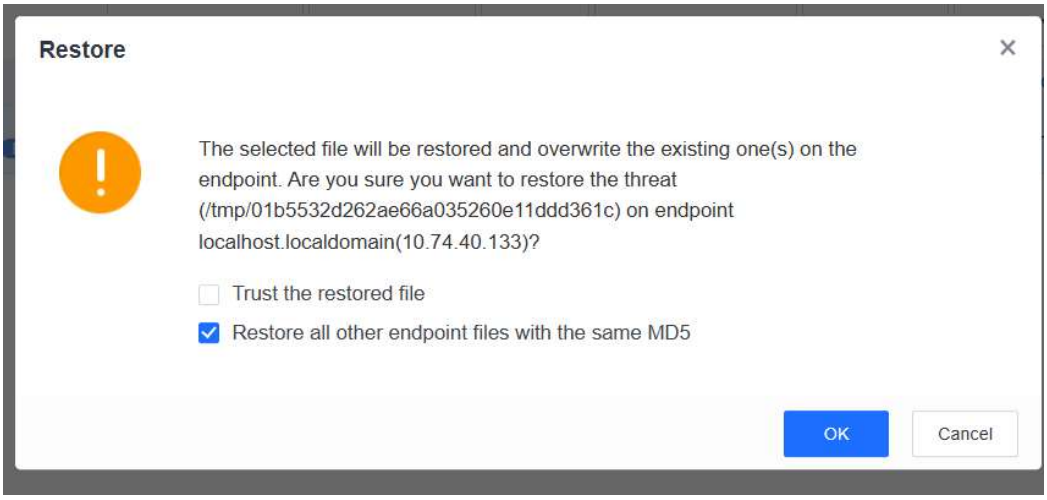


Fixed:

The **Fixed** tab displays all infected files that have been quarantined. You can **Remove**, **Restore**, or **Ignore** the files, as shown below.



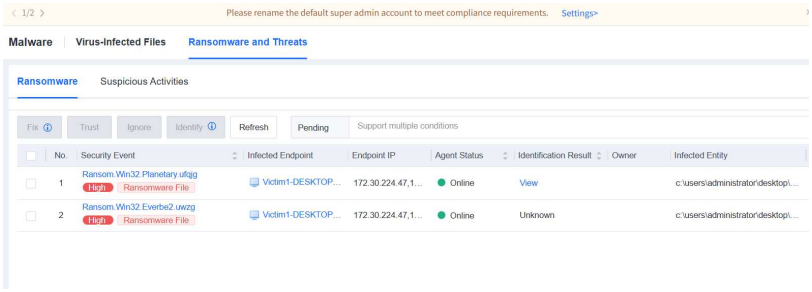
Select infected files and click **Remove** to delete quarantined files in bulk, or click **Restore** to restore quarantined files in bulk, as shown in the following figure.



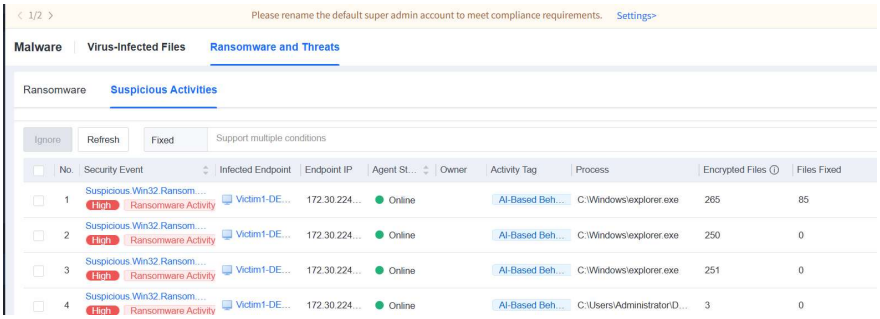
You can fix up to 10,000 infected files at a time. To fix all infected files at a time, check the box in the upper left corner of the list, click **Select all on all pages**, and then click **Fix**, as shown in the following figure.

4.4.1.1.2 Ransomware and Threats

Ransomware: Ransomware attacks include **malicious files** and **suspicious activities**. NovaGuard can detect ransomware files and identify ransomware attacks by using ForeNova Engine Zero before the ransomware encrypts host files. This proactive approach ensures early detection and timely prevention.



Suspicious activities: Suspicious activities refer to ransomware attacks, such as ransomware encryption, sending a ransom note, and baiting, identified via ForeNova Engine Zero. NovaGuard ensures early detection and timely prevention before the ransomware encrypts host files, as shown in the following figure.



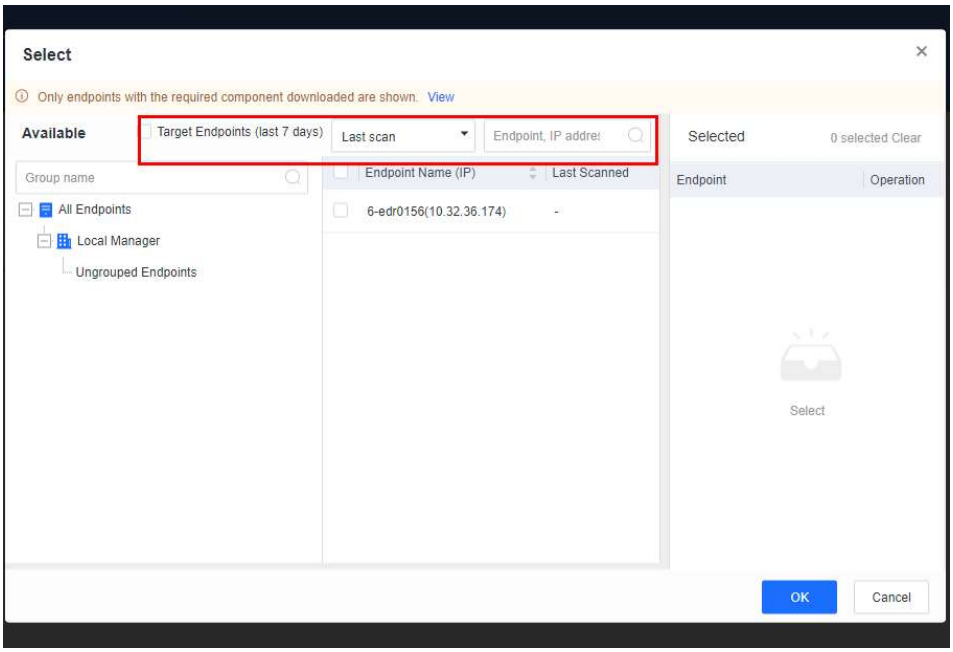
The actions to be taken when detecting malicious files are according to the configurations on the **Policies** > **General Policies** > **Anti-Malware** tab.

4.4.1.2 Tasks

Go to **Defense** > **Malware Scan** > **Tasks**, move the pointer over the **Quick Scan** button, and select **Quick Scan** or **Full Scan,** as shown below.

Endpoints: You can view the target endpoints of the last seven days, view endpoints that have not been scanned in the last seven days, 30 days, or 90 days, view the last scanned time of an endpoint, and search for specific

endpoints by name or IP address as an administrator.



CPU Usage: Includes three modes: **High CPU, Adaptive**, and **Low CPU**, each with the following distinct characteristics:

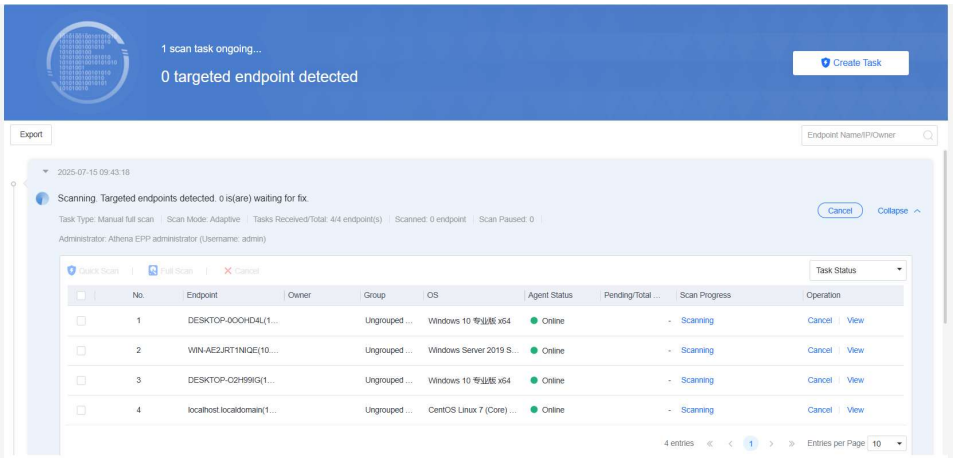
- **High CPU:** Consumes the most CPU resources (<50% when CPU usage restriction is enabled).
- **Adaptive:** Dynamically adjusts CPU resources based on the CPU usage. It optimizes the scan speed by leveraging ample CPU resources when the CPU usage is low and minimizing resource consumption when the CPU usage is high, thus ensuring smooth service operations.
- **Low CPU:** Consumes no more than 10% of CPU resources (<5% when CPU usage restriction is enabled).

NOTE

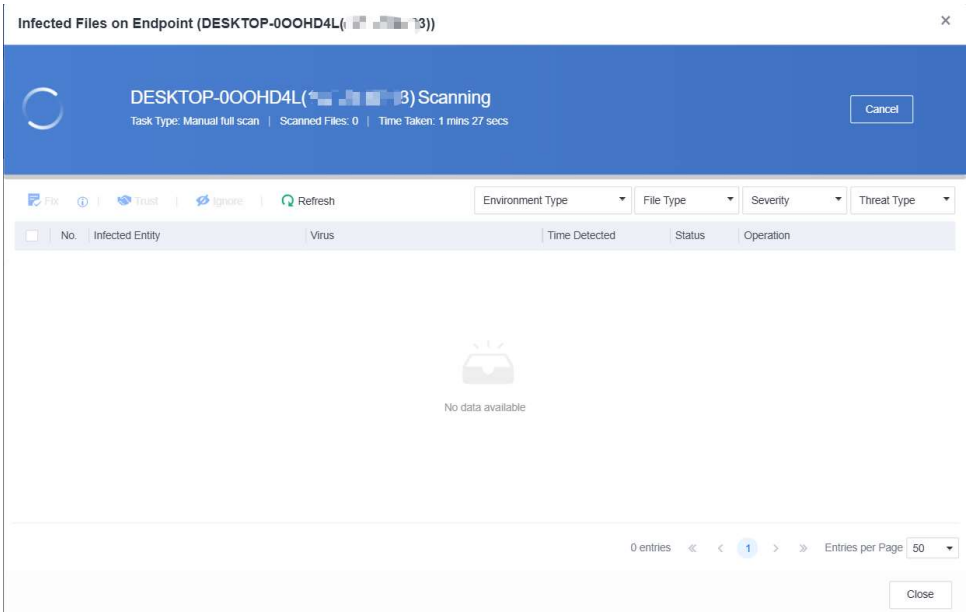
The adaptive mode applies to Windows endpoints only, while an adaptive scanning mode is designed for Linux endpoints, with a limitation of 30% on CPU usage during virus scans.

In-depth Analysis: Once in-depth analysis for infectious viruses is enabled, the scan will take 5% longer. It is advised to enable it only when infectious viruses are on the endpoints. This is only applicable to Windows endpoints.

Select endpoints and issue virus scan tasks. Then, check the task status of the endpoints, as shown in the following figure.

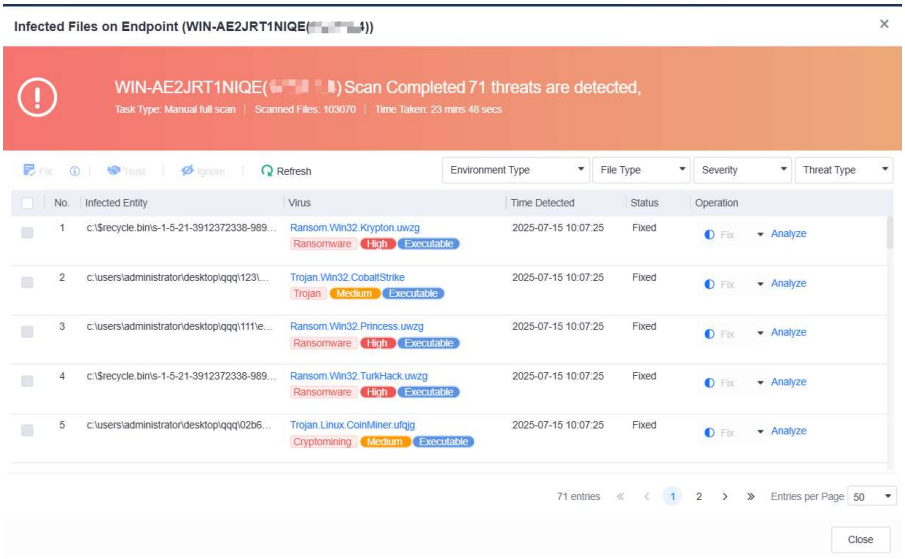


Click **View** on the right of a specific endpoint and view its scan progress, as shown in the following figure.

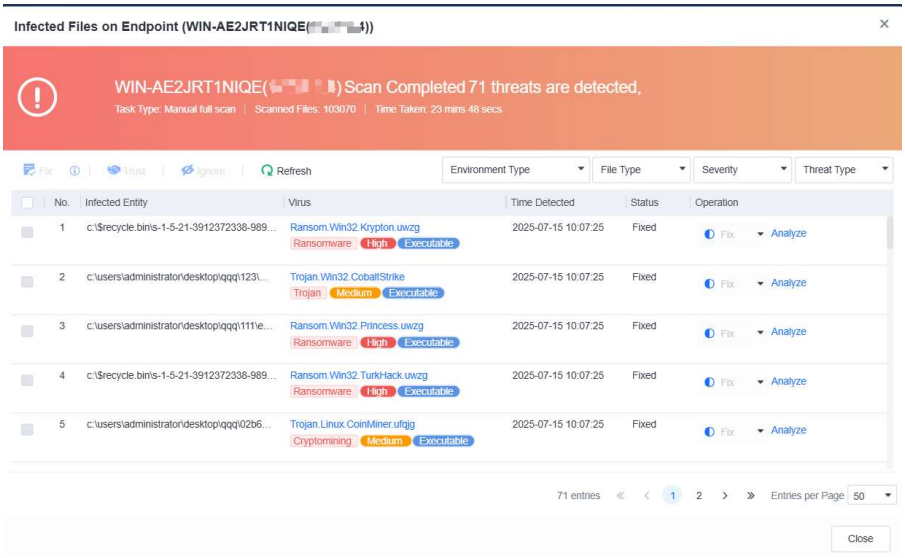


After the scan is complete, review the scan results, which include details such as the task type, CPU usage, number of tasks received by endpoints, scanned endpoints, paused endpoints, endpoint names and IP addresses, groups, operating systems, endpoint status, pending/total viruses, and scan progress,

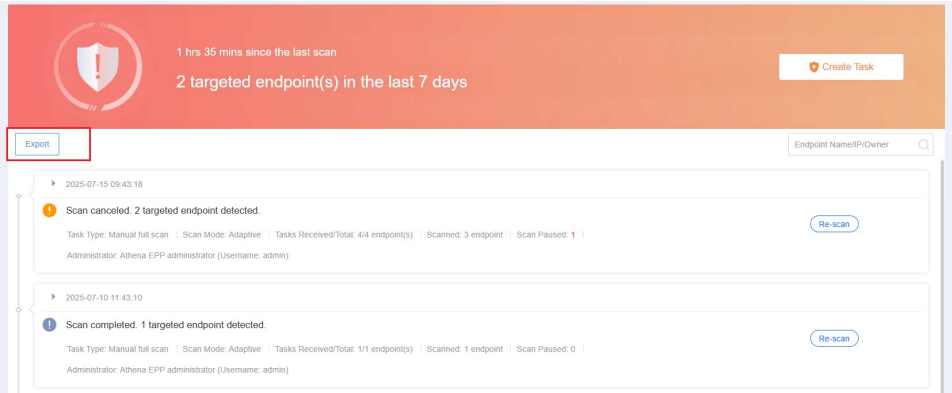
as shown in the following figure.



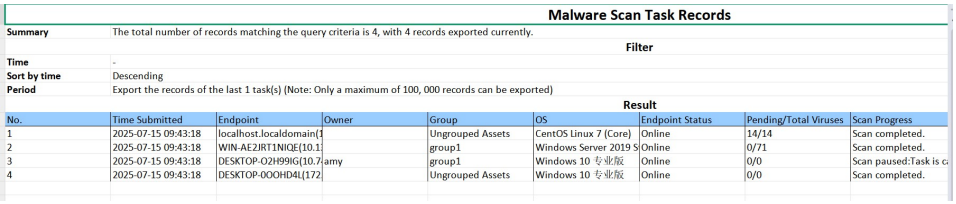
Handle the detected infected files by either fixing or trusting them. If the infected files seem suspicious, click **Analyze** to access Neural-X Threat Intelligence for analysis. Then, fix the files based on the analysis result, as shown in the following figure.



Click **Export** to export the virus scan results within a selected period.



The virus scan results are exported as an Excel file, as shown in the following figure.



Malware Scan Task Records

Summary	The total number of records matching the query criteria is 4, with 4 records exported currently.
	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 Submitted	Endpoint	Owner	Group	OS	Endpoint Status	Pending/Total Viruses	Scan Progress
1	2025-07-15 09:43:18	localhost.localdomain(1		Ungrouped Assets	CentOS Linux 7 (Core)	Online	14/14	Scan completed.
2	2025-07-15 09:43:18	WIN-AE2JRT1NIQE(10.1		group1	Windows Server 2019 S	Online	0/71	Scan completed.
3	2025-07-15 09:43:18	DESKTOP-O2H99IG(10.7	amy	group1	Windows 10 专业版	Online	0/0	Scan paused:Task is c
4	2025-07-15 09:43:18	DESKTOP-0OOHD4L(172		Ungrouped Assets	Windows 10 专业版	Online	0/0	Scan completed.

4.5 Endpoints

The **Endpoint** page of the NovaGuard manager consists of **Endpoint Groups**, **Endpoint Inventory**, **Endpoint Discovery**, and **Changes**, allowing you to manage endpoints and groups based on policies.

4.5.1 Endpoint Groups

NovaGuard organizes endpoints in a tree structure. On the **Endpoint Groups** page, you can create groups, import groups, synchronize the Lightweight Directory Access Protocol (LDAP) information, allow users to assign groups, and manage endpoints.

4.5.1.1 Create Groups

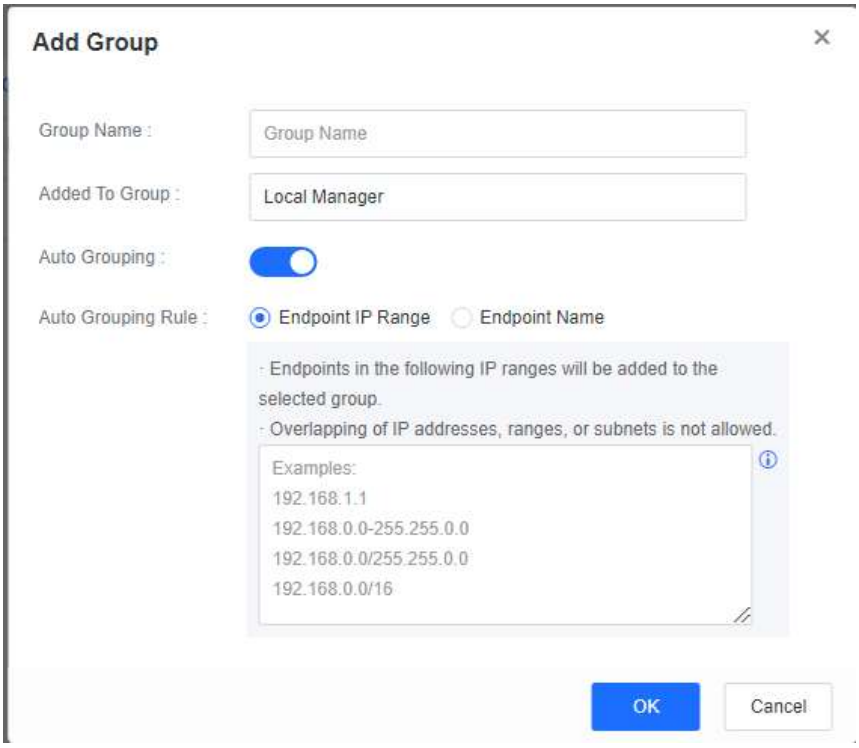
Applicable Scenario

In scenarios that involve a few groups, you can create groups manually for automatic endpoint grouping by endpoint IP range or endpoint name.

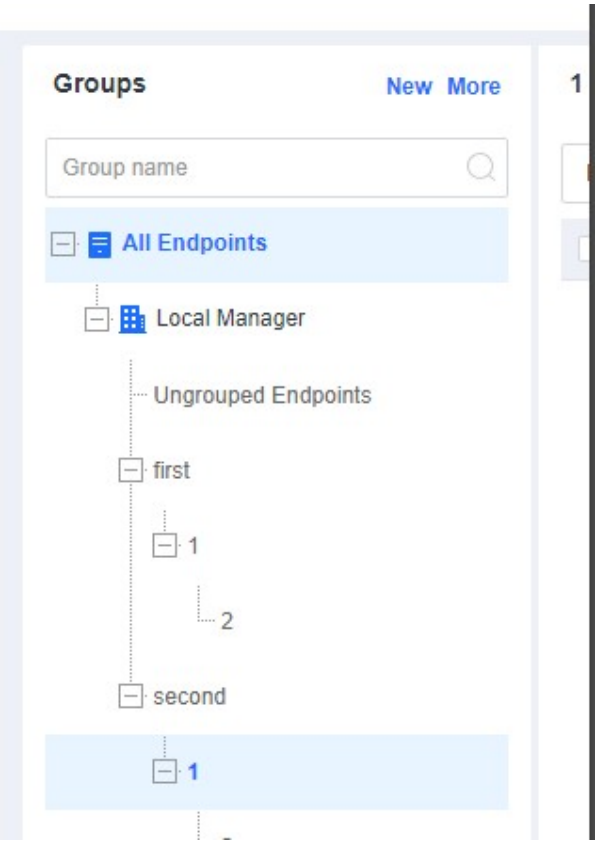
Configuration Guide

Plan business groups and IP addresses in advance, create groups according to asset attributes, and enable automatic grouping by endpoint IP range or endpoint name. Then, the endpoints with NovaGuard agent installed will automatically join the corresponding groups based on their IP addresses or names when they go online.

To create a group, go to **Endpoint** > **Endpoint Groups** and click **New**. In the **Add Group** dialog box, enable **Auto Grouping**, select **Endpoint IP Range** or **Endpoint Name** for **Auto Grouping Rule**, and enter IP ranges or keywords, as shown in the following figure.



A sample organizational structure of groups is as follows.



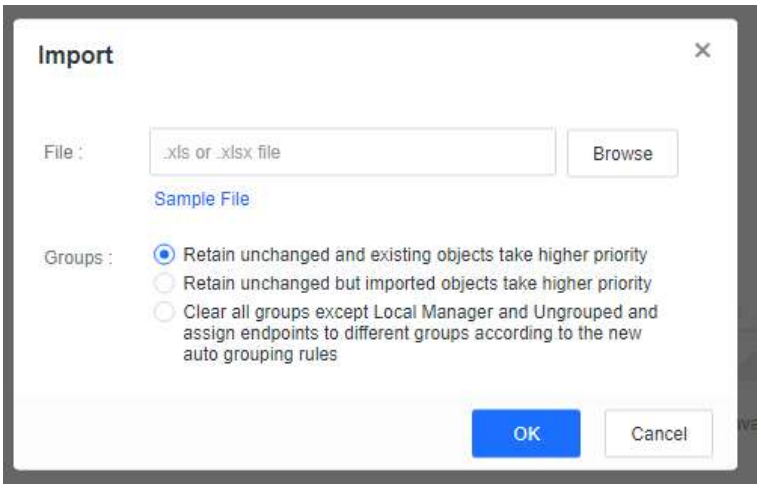
4.5.1.2 Import Groups

Applicable Scenario

You can import groups using an Excel file if there are many groups.

Configuration Guide

Go to **Endpoint** > **Endpoint Groups** and click **More** > **Import**. In the **Import** dialog box, click **Sample File** to download the template. Add the group information to the Excel template and select the template to import all groups.



A	B	C	D	E	F	G
Group Name	Parent Group	Auto-grouping IP Range	Auto Grouping Rule (Endpoint Name)	Status		
example1	Local Manager	192.168.0.1-192.168.0.255;192.168.1.1-192.168.1.255		disable		
example2	example1	192.168.2.1;192.167.0.1/16;192.168.4.1/255.255.255.0		enable		
example3	example2		key1;key2	enable		
example4	example2					

4.5.1.3 LDAP Sync

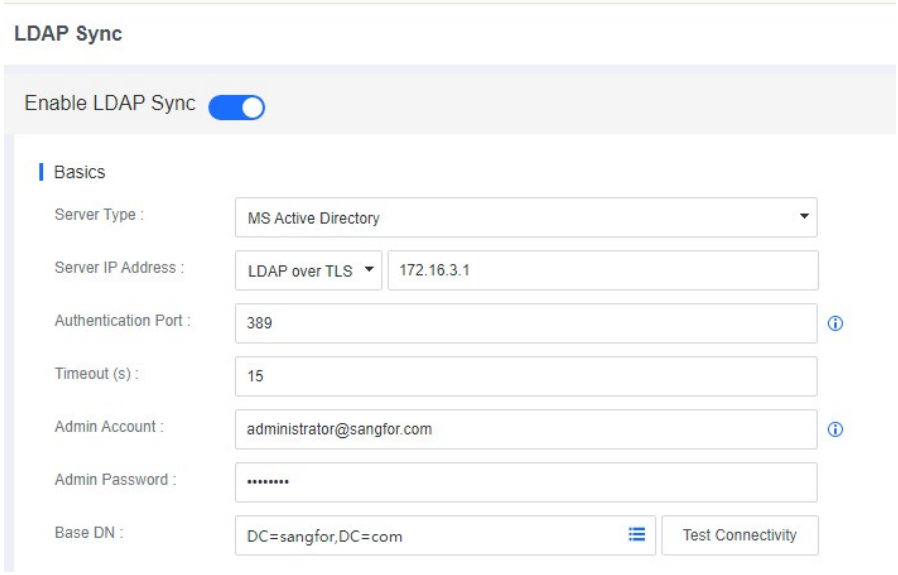
Applicable Scenario

In scenarios where the customer has deployed an AD domain server in the internal network to which endpoints are connected for unified management, administrators can enable LDAP synchronization to automatically synchronize specific OUs and users to NovaGuard for unified user management.

Configuration Guide

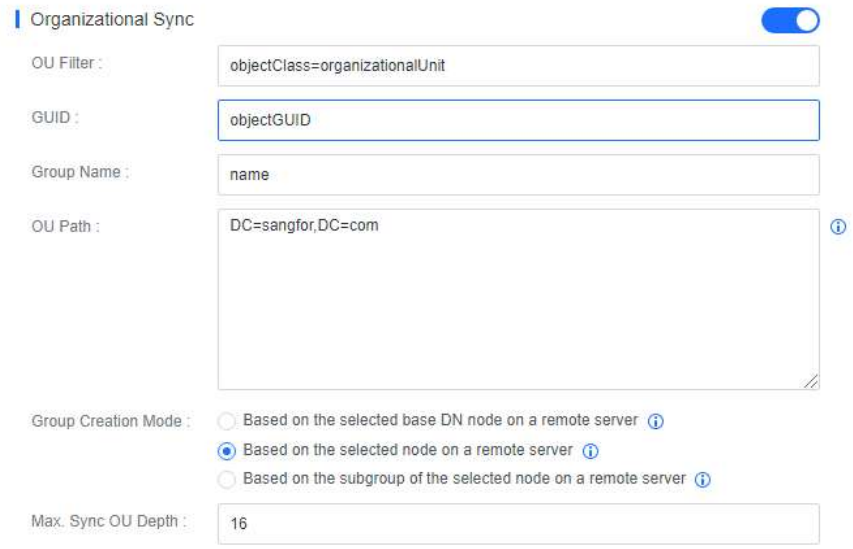
Go to **System** > **System** > **LDAP Sync** and configure parameters based on the configurations in the following figure.

1. **Basics**



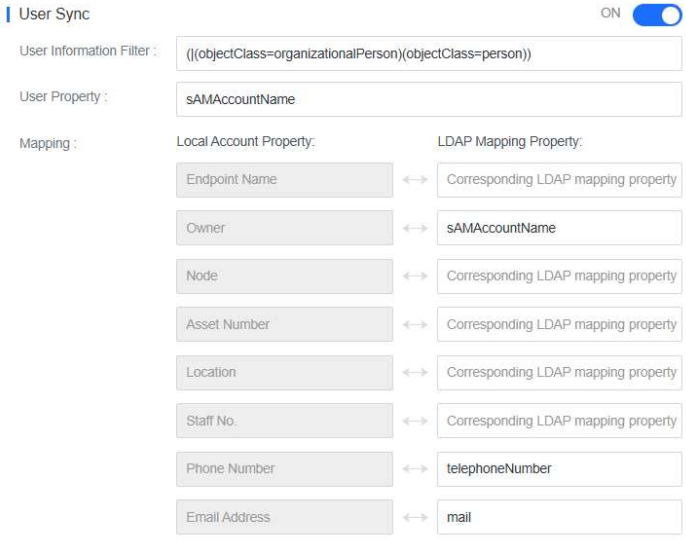
Basics: Specify the IP address of the AD domain server, the authentication port, the administrator account username, the administrator account password, and the Base DN. The administrator account username must be in the following format: administrator@domain.com.

2. **Organizational Sync**

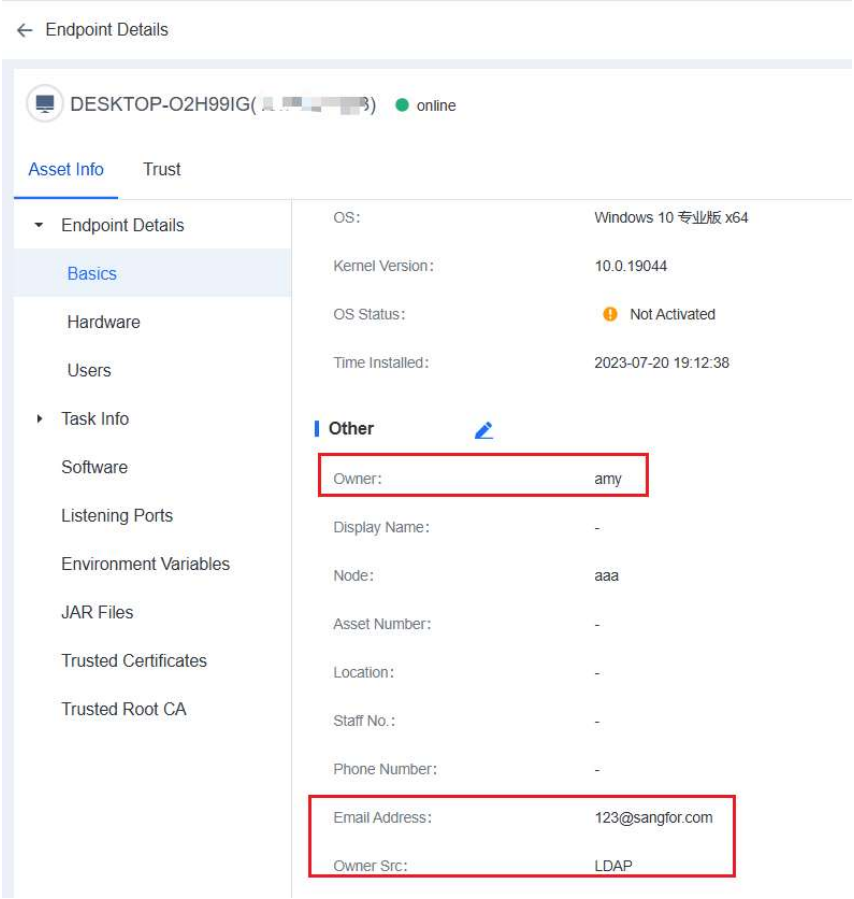


Organizational Sync: Specify OU paths and a group creation mode and keep other parameters at their defaults.

3. User Sync



User Sync: Map domain user properties to the NovaGuard manager and keep other parameters at their defaults, as shown in the following figure.



4. Group Sync



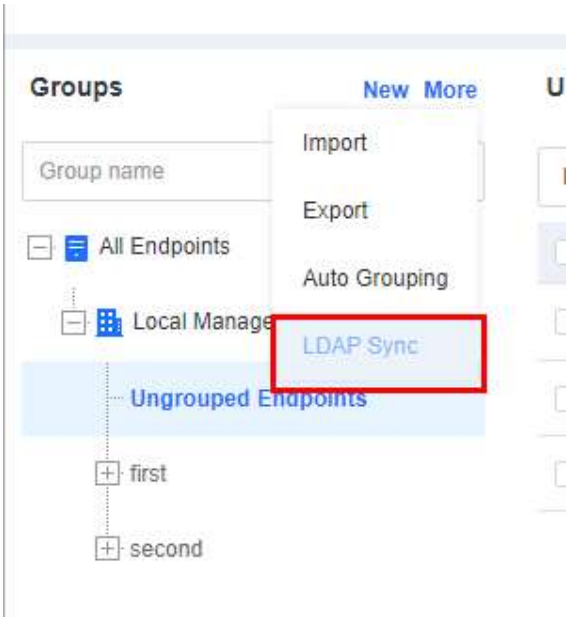
Group Sync: Endpoints are automatically grouped on the NovaGuard manager according to the structure in the AD domain. Automatic grouping is triggered after you log in to an endpoint with a domain account and trigger LDAP synchronization.

Trigger LDAP Sync

You can trigger LDAP synchronization manually or at a scheduled time.

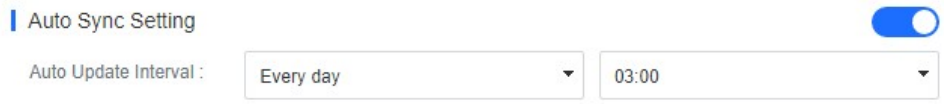
1. Manual synchronization

To synchronize the LDAP information manually, go to **Endpoints** > **Endpoint Groups** and click **More** > **LDAP Sync**, as shown in the following figure.



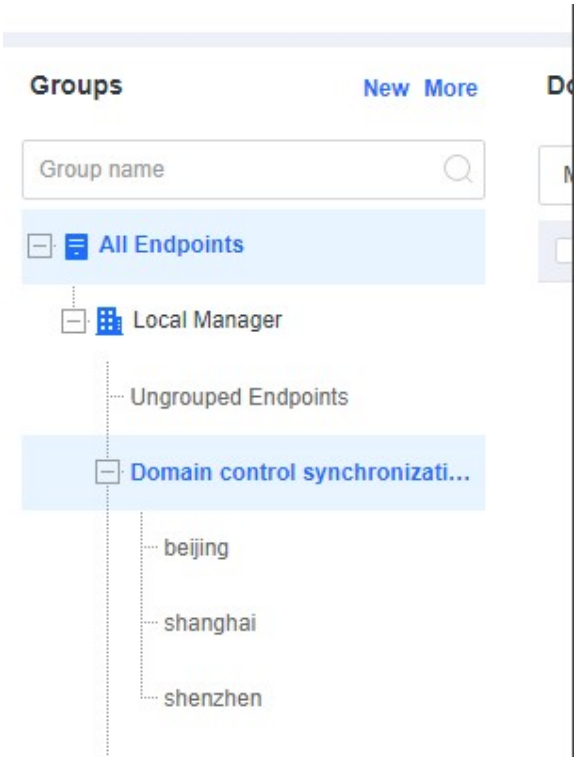
2. Automatic synchronization

To synchronize LDAP information automatically, enable **Auto Sync Setting**, select **Every day**, **Every week**, or **Every month**, and set a specific time, as shown in the following figure. Then, the NovaGuard manager will automatically synchronize OU and user information from the LDAP server.



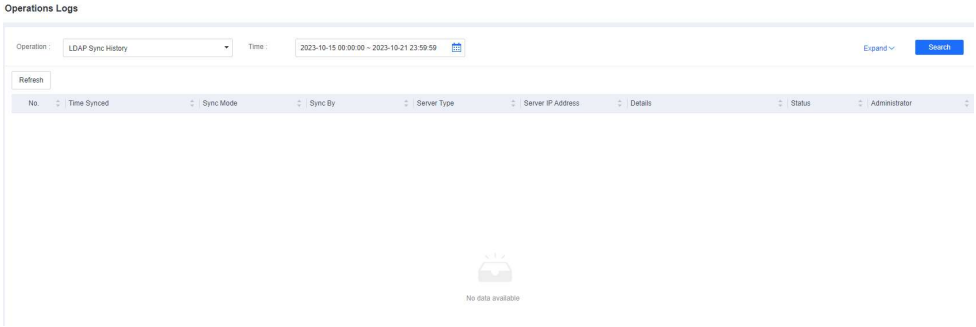
Effects

On the **Endpoint Groups** page of the NovaGuard manager, you can find the OUs synchronized from the LDAP server, as shown in the following figure.



The NovaGuard manager automatically groups endpoints with the NovaGuard agent installed to the corresponding OUs when you log in to the endpoints with domain accounts.

You can view LDAP synchronization details by going to **System** > **Logs** > **Operations Logs**, as shown in the following figure.



4.5.1.4 Allow Users to Assign Groups

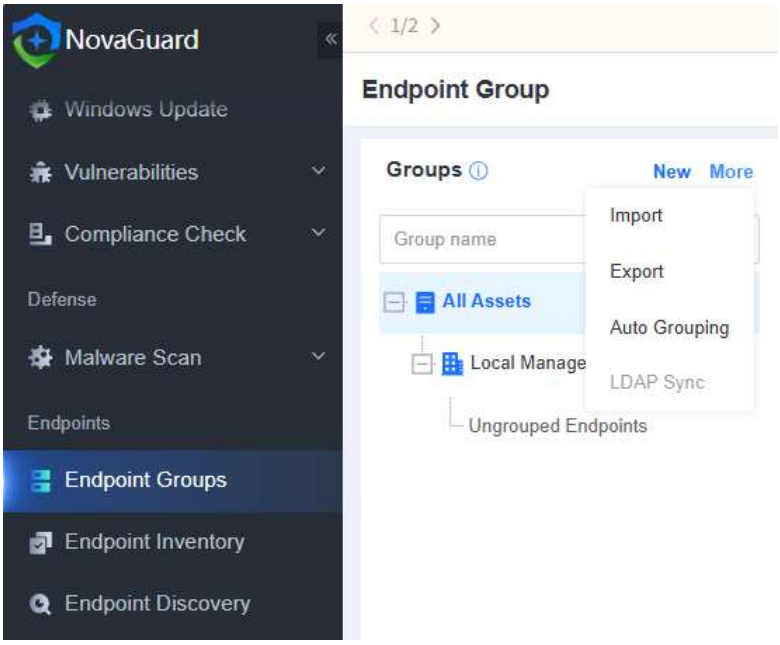
Applicable Scenario

In multi-branch scenarios without any AD controller, automatic grouping by IP range is not applicable because IP address conflicts may exist between the endpoints of different branches. In this case, you can enable endpoint users to assign groups to their endpoints.

Configuration Guide

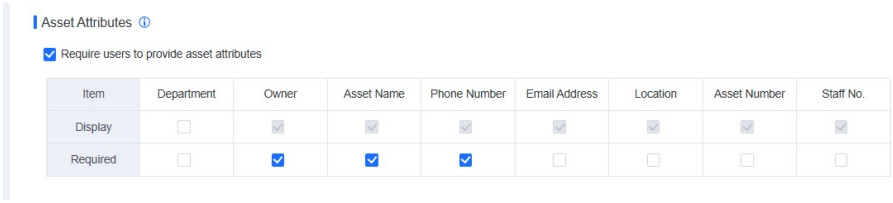
Step 1. Create or import groups.

Go to **Endpoints** > **Endpoint Groups** > **Auto Grouping** to disable the automatic grouping, as shown in the following figure.



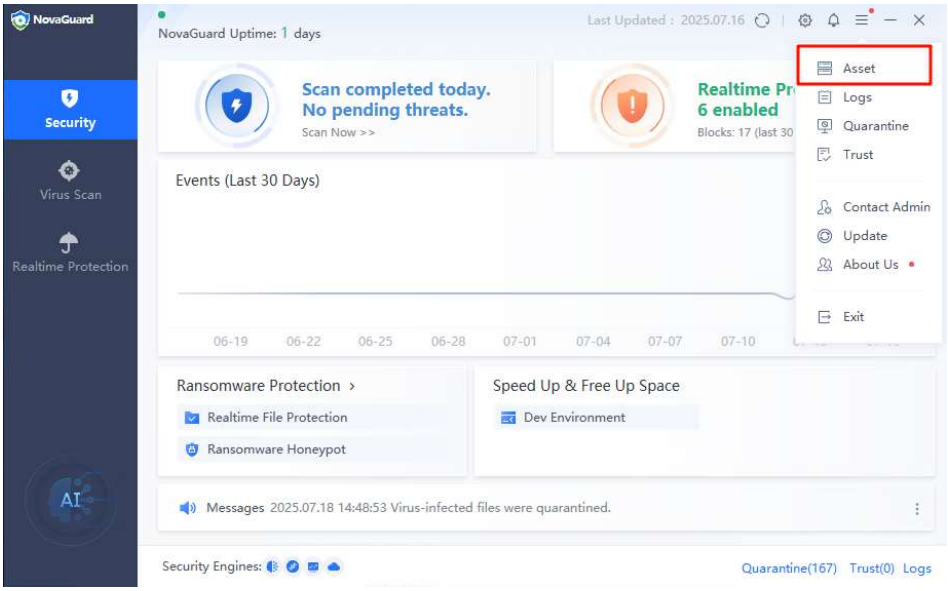
Step 2. Select **Require users to provide asset attributes**.

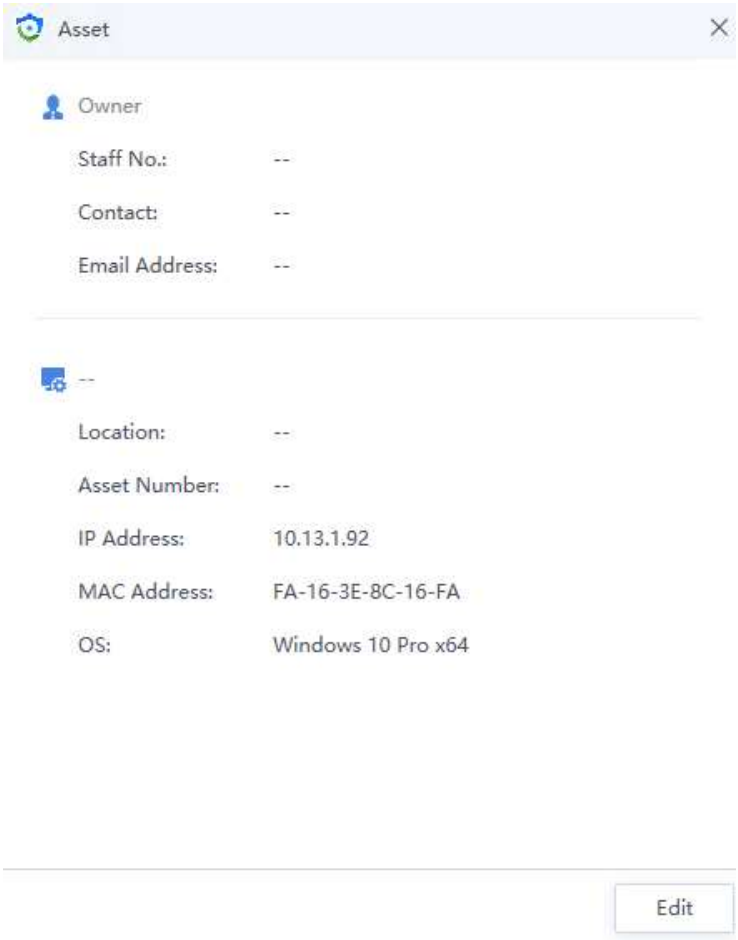
Go to **Policies** > **General Policies** > **Basic Config**, select **Require users to provide asset attributes**, and then select **Display** and **Required** in the **Department** column, as shown in the following figure.



Step 3. Users assign groups to their endpoints.

Users can set organizational information for their endpoints during asset registration during the first installation of the NovaGuard agent or edit organizational information after the installation is complete, as shown in the following figure.


NovaGuard
NovaGuard Uptime: 1 days
Last Updated : 2025.07.16
Security
Virus Scan
Realtime Protection
Scan completed today.
No pending threats.
Scan Now >>
Realtime Pr
6 enabled
Blocks: 17 (last 30
Asset
Logs
Quarantine
Trust
Contact Admin
Update
About Us
Exit
Events (Last 30 Days)
06-19
06-22
06-25
06-28
07-01
07-04
07-07
07-10
Ransomware Protection
Realtime File Protection
Ransomware Honeypot
Speed Up & Free Up Space
Dev Environment
Messages 2025.07.18 14:48:53 Virus-infected files were quarantined.
Security Engines:
Quarantine(167) Trust(0) Logs

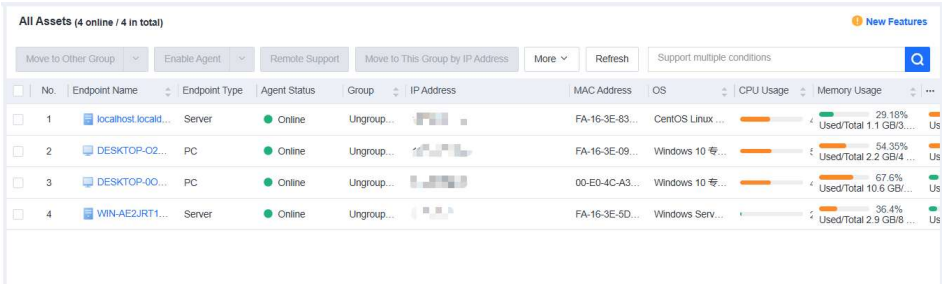

Asset
Owner
Staff No.: --
Contact: --
Email Address: --
--
Location: --
Asset Number: --
IP Address: 10.13.1.92
MAC Address: FA-16-3E-8C-16-FA
OS: Windows 10 Pro x64
Edit

4.5.1.5 Manage Endpoints

On the **Endpoint Groups** page, you can view endpoint information, move endpoints to other groups, manage remote endpoints, enable remote support, send messages, and export endpoints.

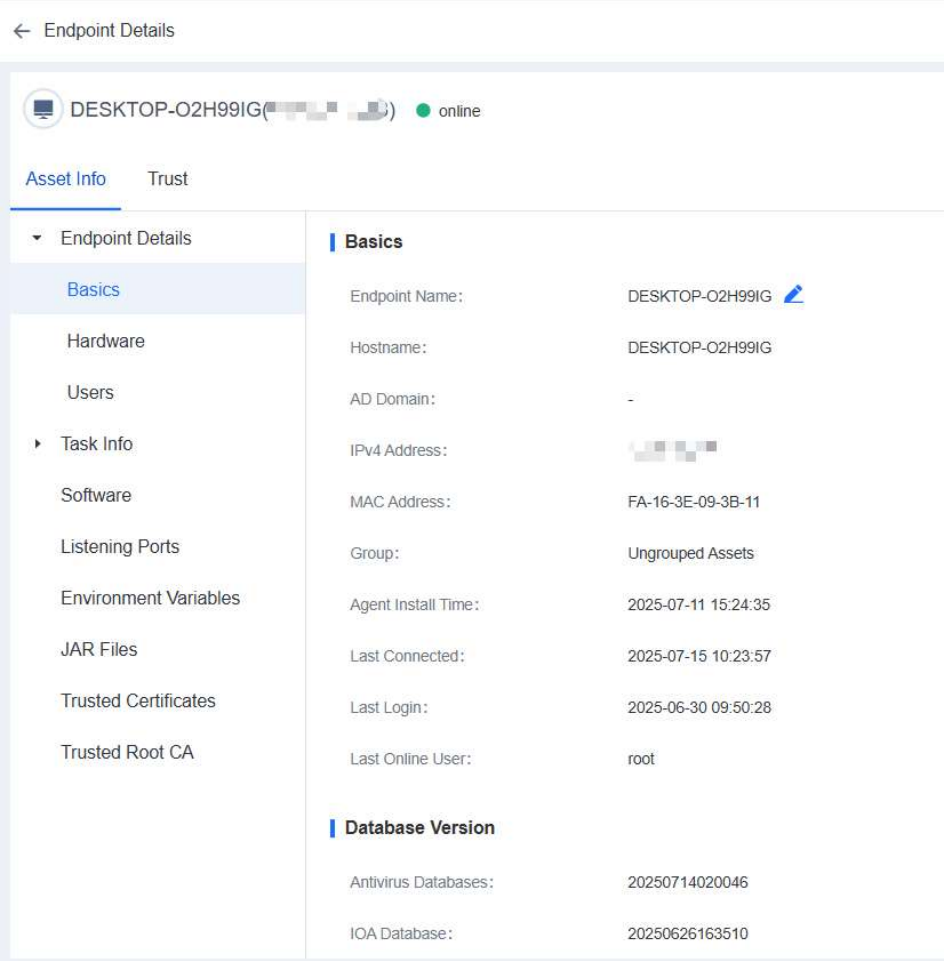
View endpoint information:

On the **Endpoint Groups** page, you can view the basic information of all endpoints, as shown in the following figure.



The page includes columns such as **Endpoint**, **Asset Status**, **Group**, **IP Address**, **MAC Address**, **OS**, **Realtime Protection Status**, **CPU Usage**, **Memory Usage**, **Asset User**, **Asset Number**, and **Location**. Administrators can determine whether to display a column by clicking **...** on the right.

You can click the name of an endpoint to go to its details page, as shown in the following figure.



On the **Endpoint Details** page, you can run **Vulnerability Scan**, **Quick Scan**, and **Full scan**. You can also **Enable**, **Disable**, or **Uninstall NovaGuard agent** on the same page.

1. **Basics**

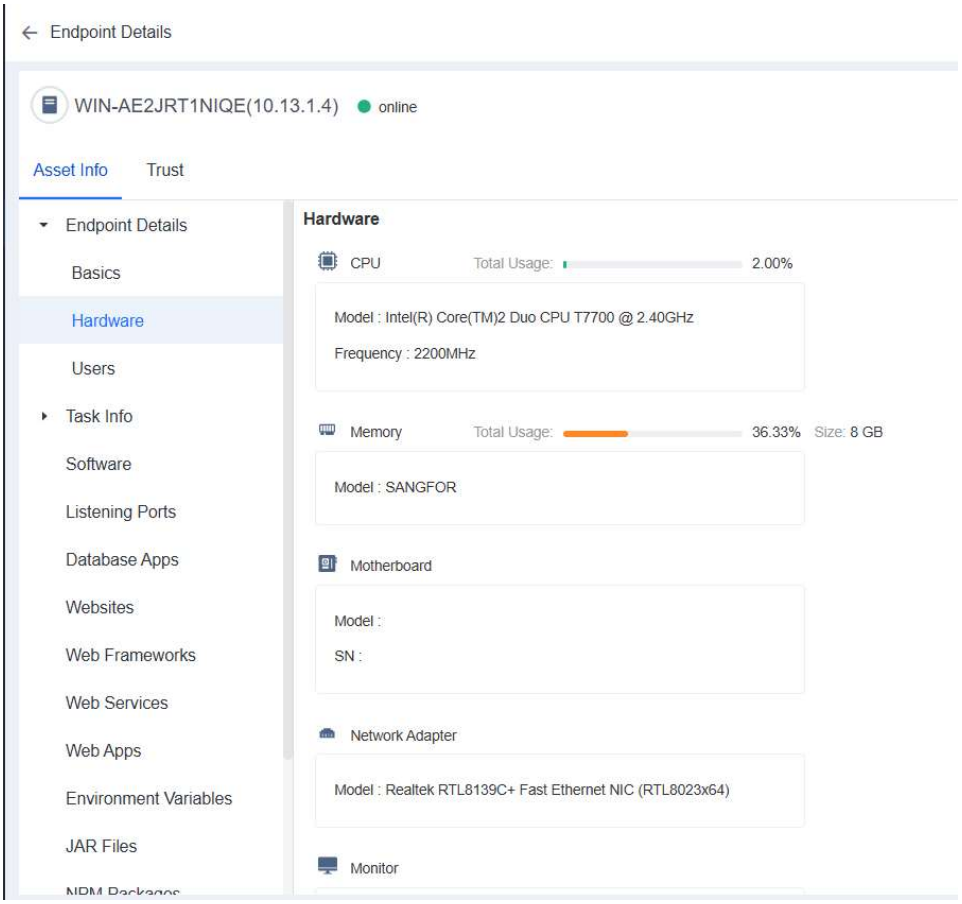
Basics: Includes information such as **Endpoint** (editable), **Hostname**, **IPv4 Address**, **MAC Address**, **Group**, **Agent Installation Time**, **Last Connected**, **Last Login**, and **Last Online User**.

System Information: Includes information such as **OS**, **Version**, **OS Status**, and **Time Installed**.

Other (editable): Includes information such as **Asset User**, **Node**, **Asset Number**, **Location**, **Staff No.**, **Phone Number**, and **Email Address**.

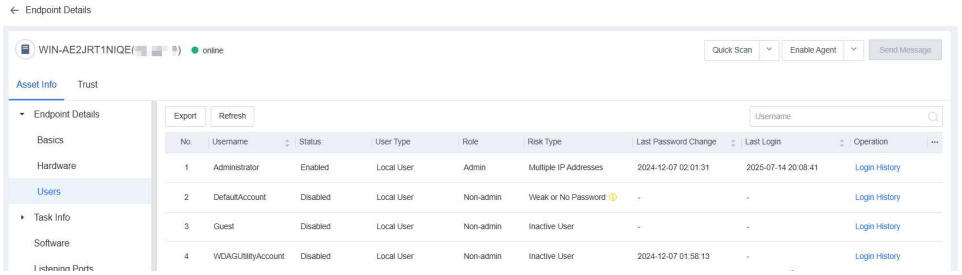
2. Hardware

Hardware: Includes the models and usage of the **CPU**, **Memory**, **Hard Disk**, **Motherboard**, **Network adapter**, **Graphics card**, **Sound card**, and **Monitor**.



3. Users

Users: Includes the endpoint's account information such as **Account**, **Status**, **Account Type**, **Role**, **Risk Type** (you can move the pointer over the exclamation icon to view the risk details), **Password Change**, **Last Login**, **Password Status**, and **Login History**.



NOTE

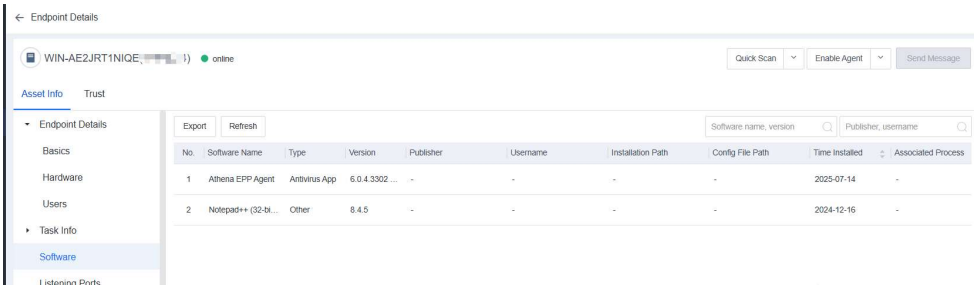
Click **...** on the right to determine whether to display a hidden column.

4. Task Info

Task Info includes information such as **Processes**, **Services**, **Connections**, **Startup Items**, **Scheduled Tasks**, **Sharing**, and **Registry**.

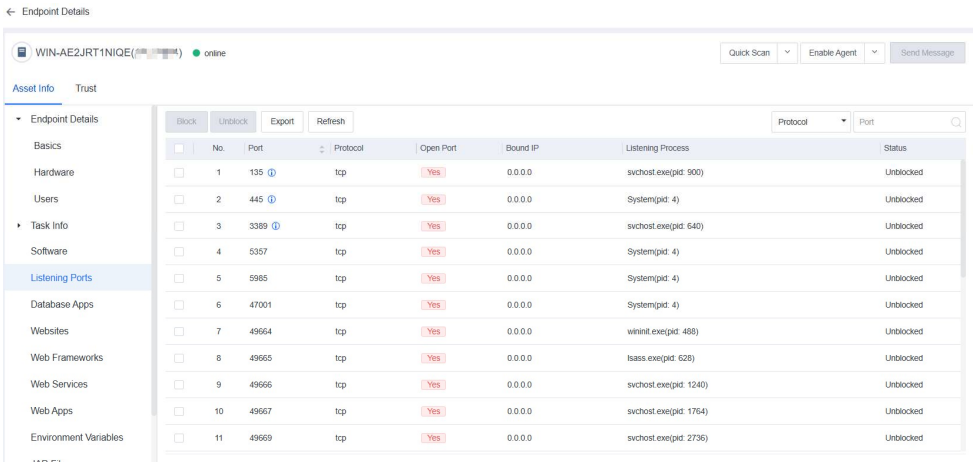
5. Software

Software includes information such as **Name**, **Type**, **Version**, **Publisher**, **Installation Path**, and **Time Installed**. You can filter software by software name, version, or publisher and export software information.



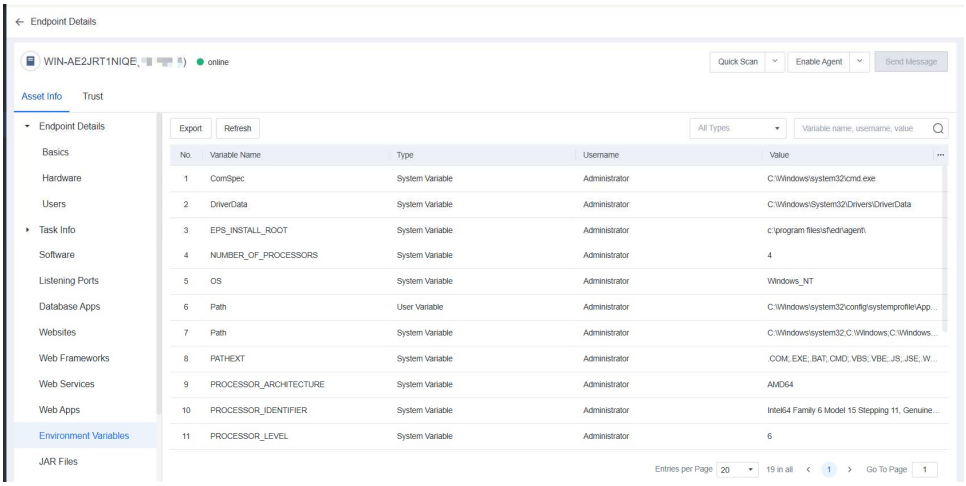
6. Listening Ports

Listening Ports includes information such as **Port**, **Protocol**, **IP Address**, **Listening Process**, **Open Port**, and **Status**. You can block or unblock ports, import port information, and search for ports by protocol or port number.



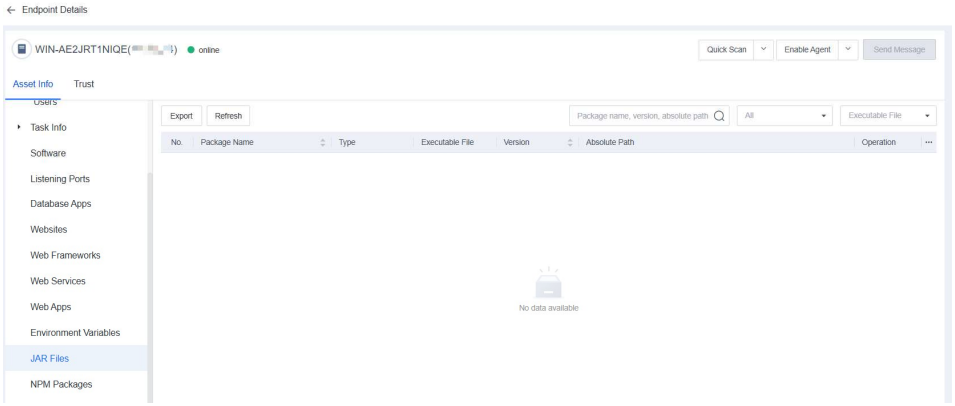
7. Environment Variables

Environment Variables include the environment information of the system and the currently logged-in user. Some programs use such information to determine where files (such as temporary files) are to be placed.



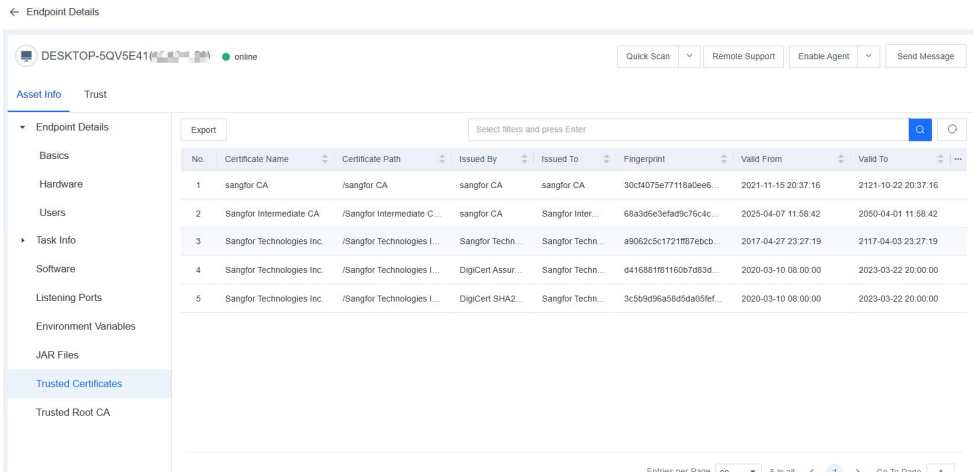
8. JAR Files

Java Archive (JAR) is a platform-independent file format that allows you to compress multiple files into one. **JAR Files** shows the JAR files of the endpoint on the NovaGuard manager.



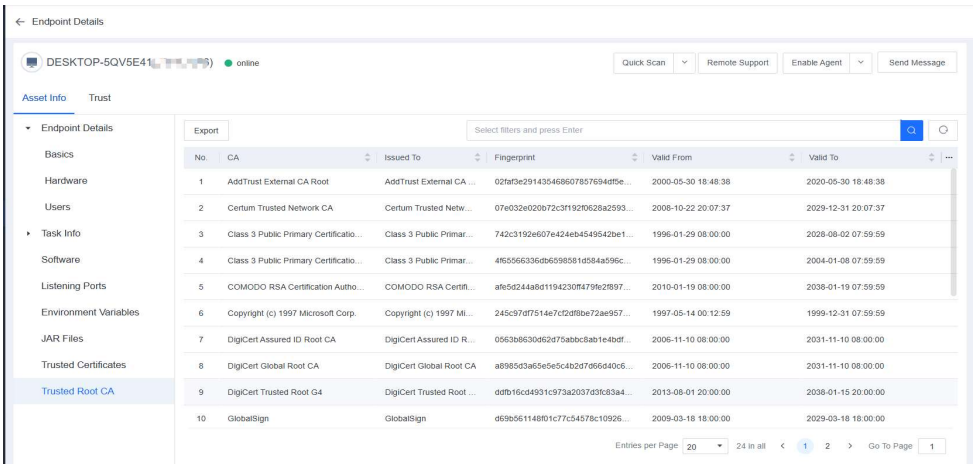
9. Trusted Certificates

Trusted Certificates displays all trusted files, paths, and processes added by the endpoint. Administrators can check such information to avoid viruses caused by improper addition, as shown in the following figure.



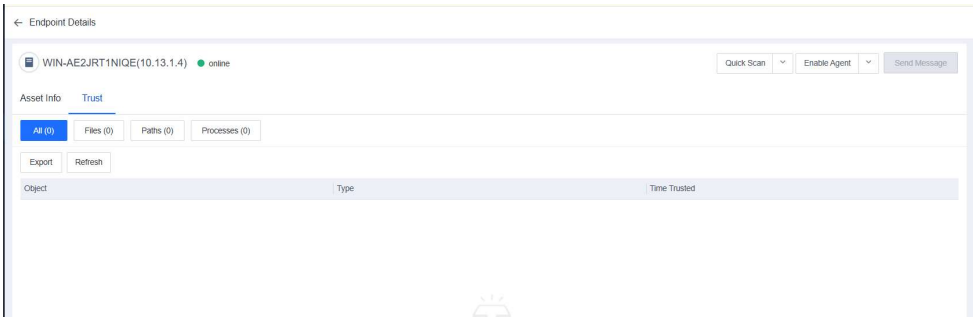
10. Trusted Root CA

The Trusted Root CA page allows you to view information such as the issuing authority, Issued To, Fingerprint, and time of Trusted Certificates.



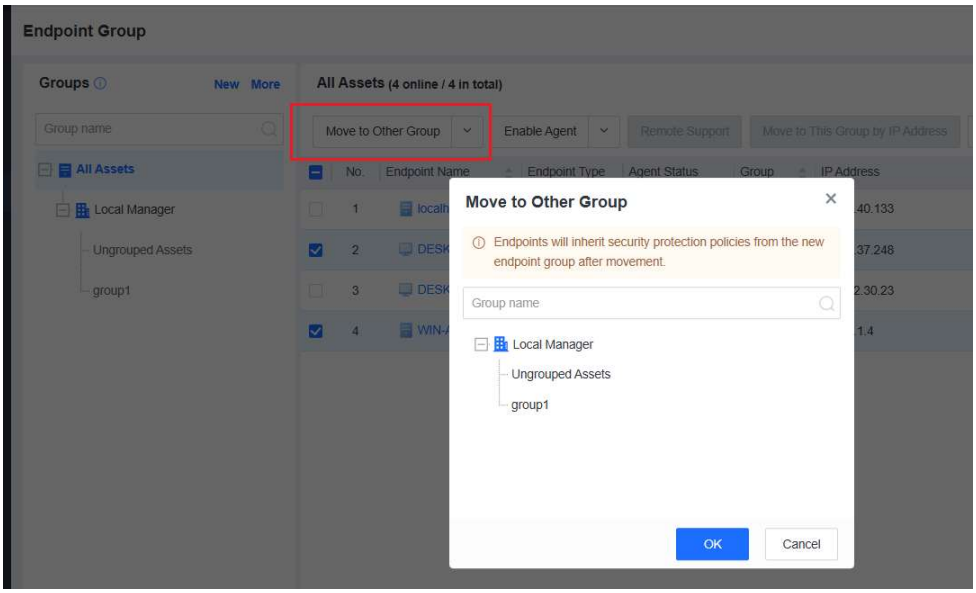
11. Trust

Support viewing Trust　policies have been added to the terminal.

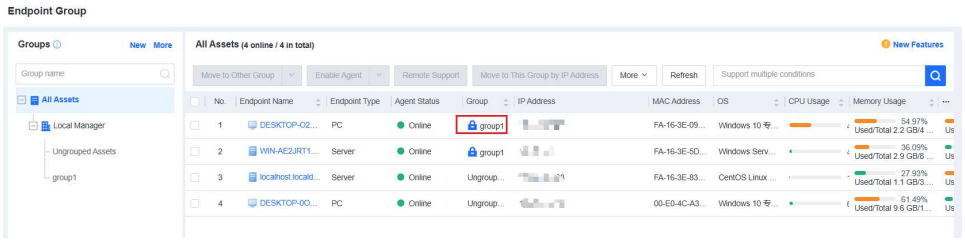


12. Move endpoints to other groups:

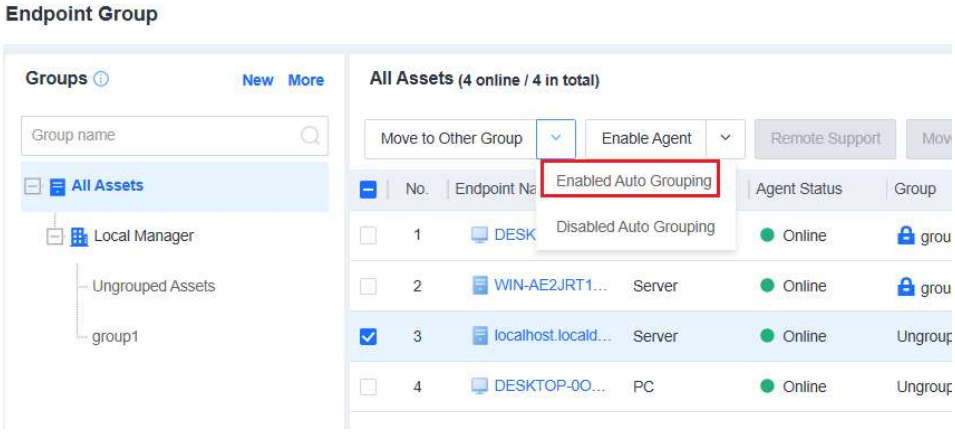
You can click **Move To Other Group** to move online endpoints to other groups, as shown in the following figure.



When **Endpoint IP Range** is selected as the auto grouping rule, the system automatically adds a tag to manually move endpoints to be locked into the current group and not automatically grouped based on their IP addresses, as shown in the following figure.



To recover auto grouping for an endpoint with a fixed group, select the endpoint and click **Enable Auto Grouping**, as shown in the following figure.



NOTE

When the agent goes online, it will trigger the auto grouping policy if the following two prerequisites are met:

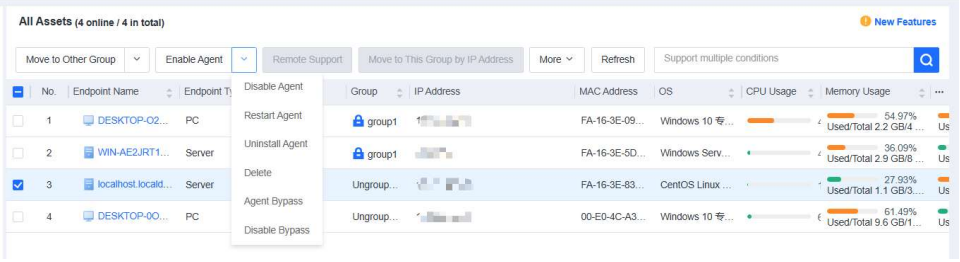
1. The auto grouping policy has been configured.

2. The group to which the endpoint belongs is not in a locked status.

Actions such as restarting the endpoint or agent will make the agent go online. Therefore, if you do not want a specific endpoint to be moved to a different group due to the automatic grouping policy, please manually move the endpoint to a specific group as described above.

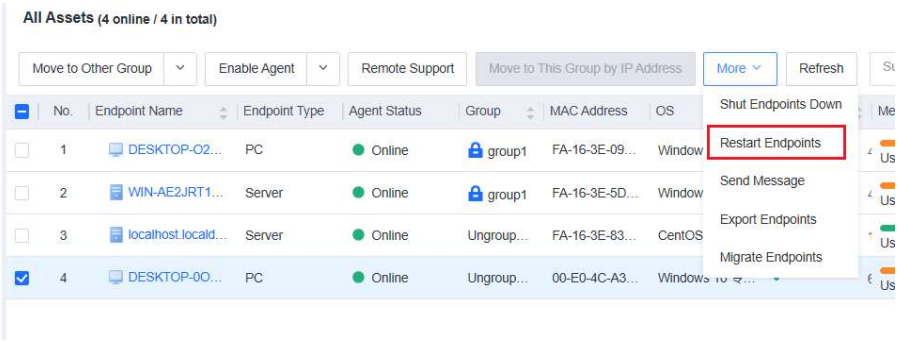
Manage remote endpoints:

You can enable, disable, restart, or uninstall the NovaGuard agent for selected endpoints, delete endpoints, and send messages to endpoints. You can also enable or disable **Agent Bypass** for Windows Server or Linux endpoints, as shown in the following figure.

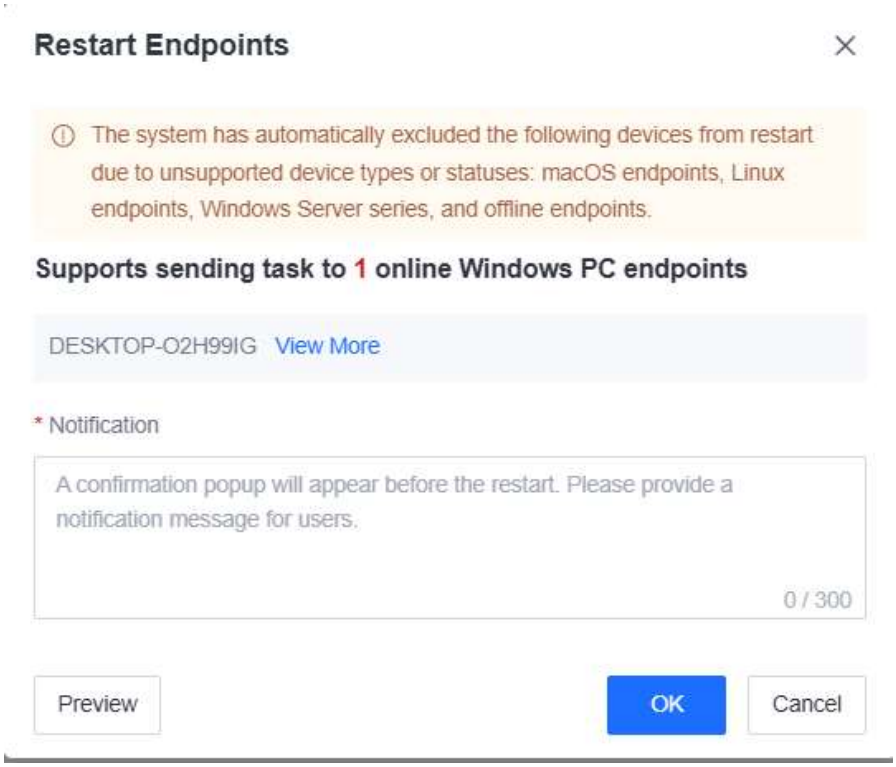


1. Restart endpoints

   You can restart one or more endpoints on the **All Endpoints** page, as shown in the following figure.



   Click **Restart Endpoints** to configure a restart policy.

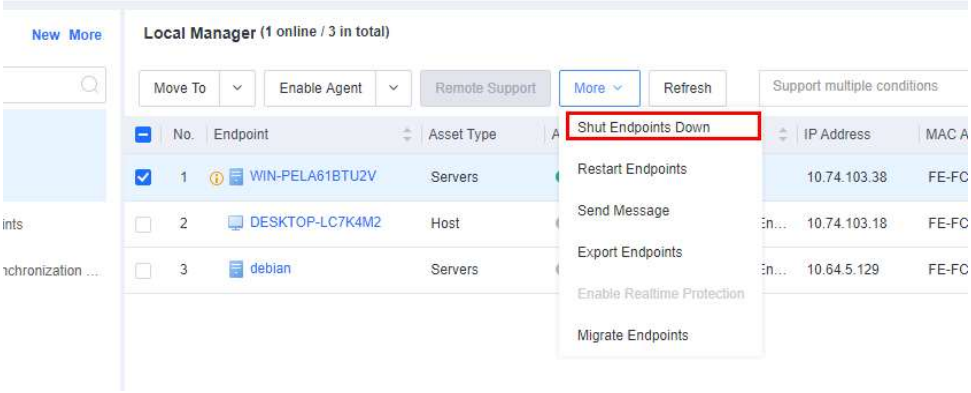


NOTE

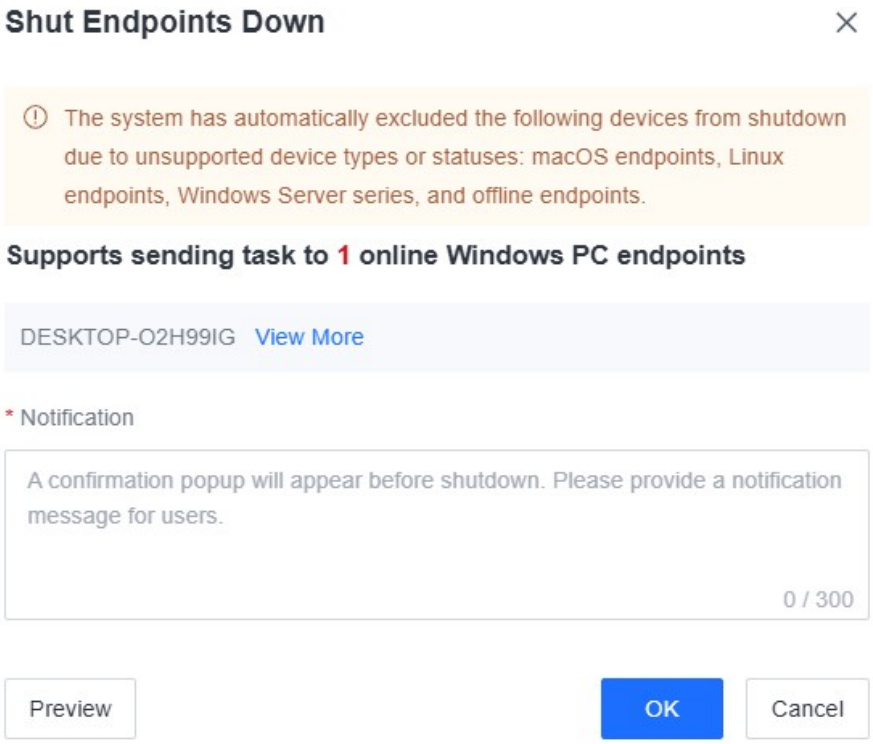
This applies to Windows endpoints only.

2. Shut down endpoints:

You can shut down one or more endpoints on the **All Endpoints** page, as shown in the following figure.



Click **Shut Endpoints Down** to set a shutdown policy.



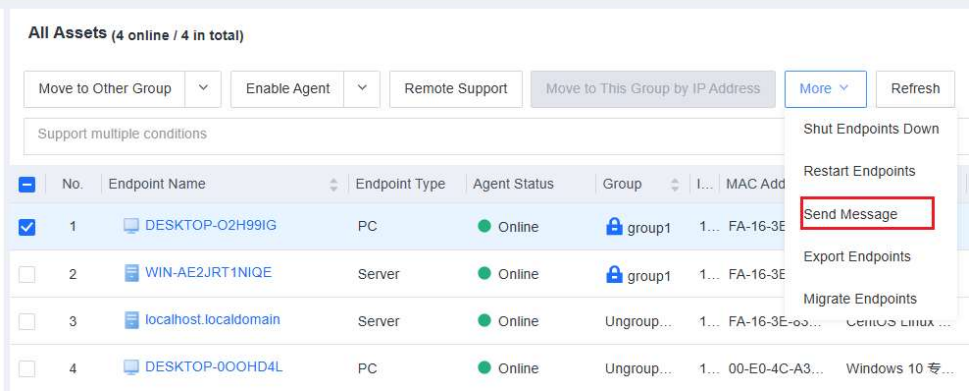
NOTE

This applies to Windows endpoints only.

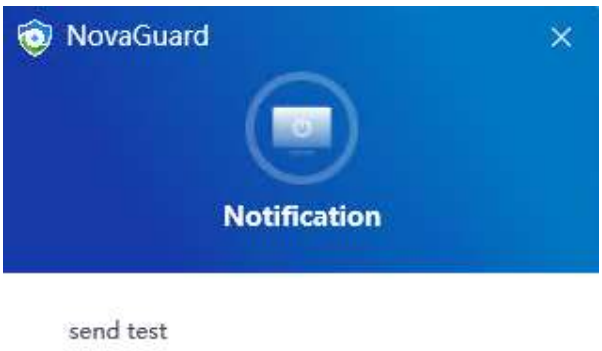
3. Send messages

You can send messages to one or more endpoints on the **All Endpoints** page. The procedure is as follows:

Step 1. On the **Endpoint** > **Endpoint Groups** > **All Endpoints** page, select one or more endpoints, and then select **Send Message** to go to the **Send Message** page, as shown in the following figure.

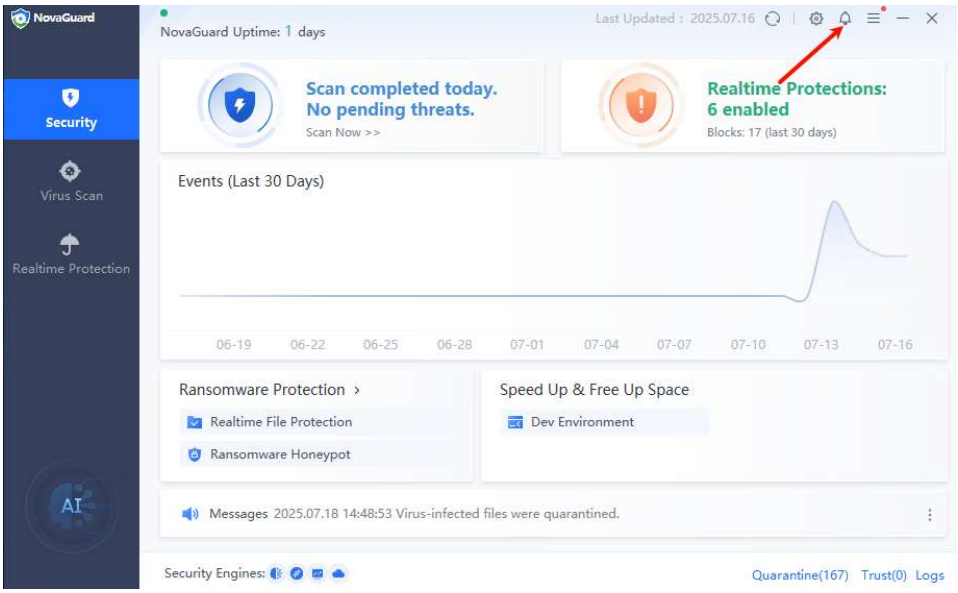


Step 2. Enter the message content. Then, users of the selected endpoints will receive the message, as shown in the following figure.



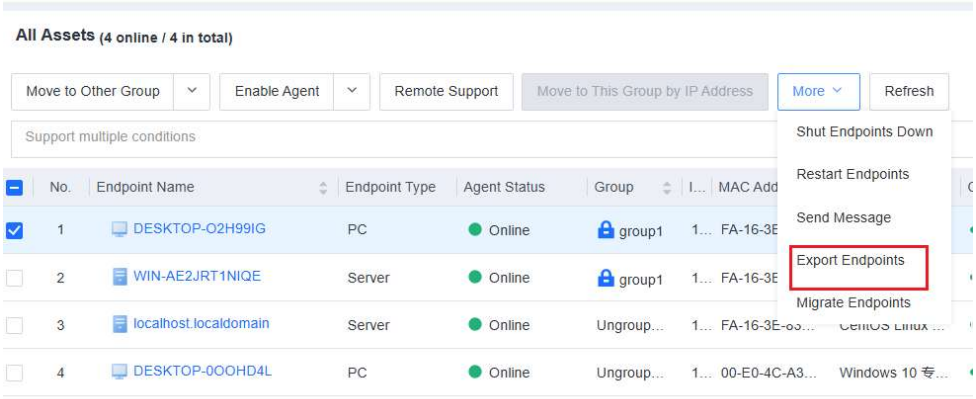
Step 3. Users can click the close (**X**) icon in the upper right corner to close the message and click the notification icon shown in the following figure to view

historical messages.



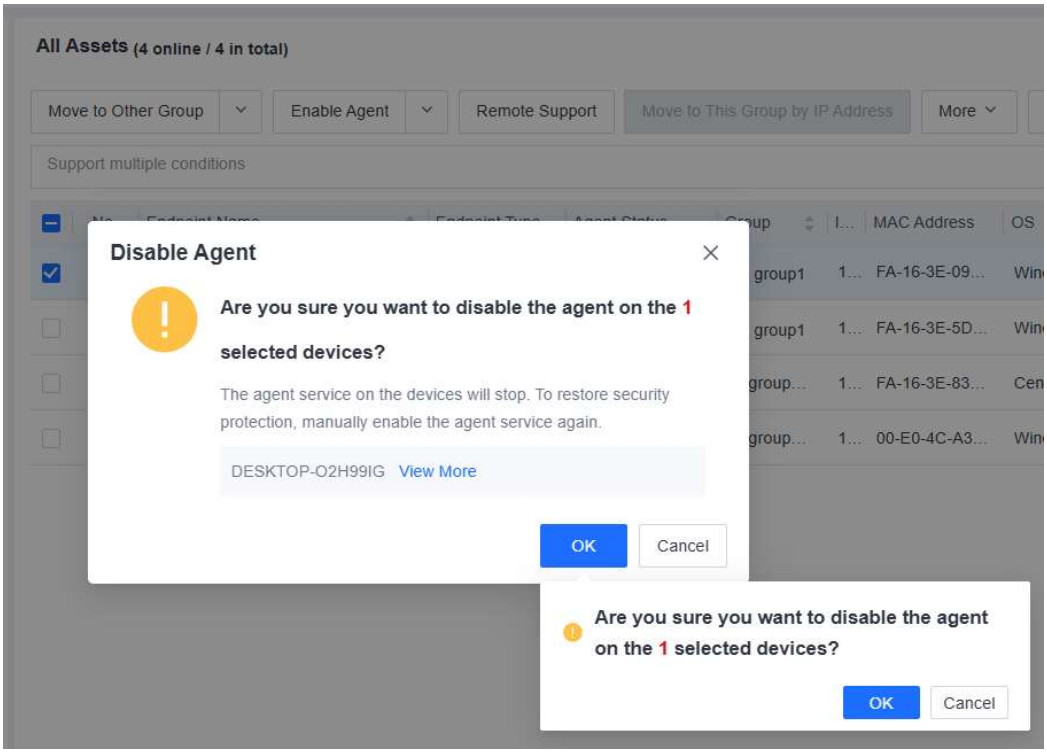
4. Export endpoints

To export an Excel file containing endpoint details, go to **Endpoint** > **Endpoint Groups**, select the endpoints to be exported, and click **More** > **Export Endpoints**, as shown in the following figure.

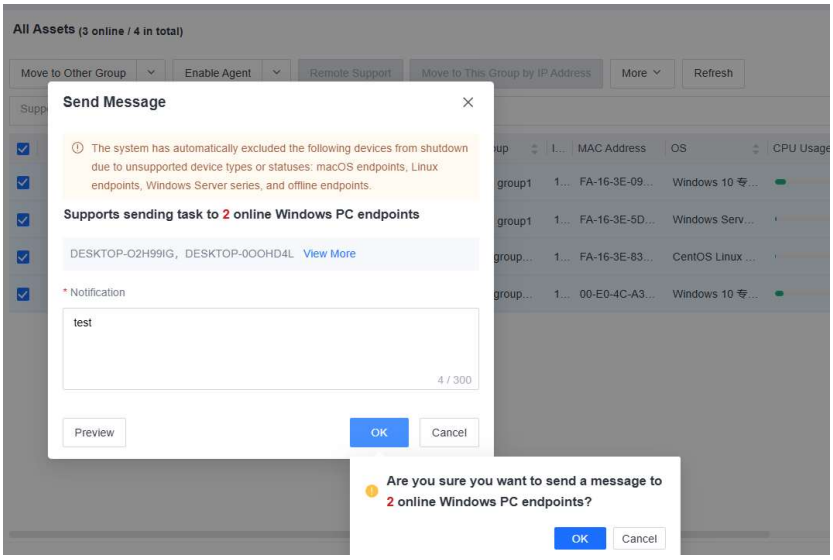


4.5.1.6 Batch operation of terminals

1. To perform O&M operations (such as disabling, enabling, uninstalling, removing, and bypassing the agent, and disabling agent bypass) and high-risk operations (such as endpoint shutdown, endpoint restart, message notification, and endpoint migration) to 100 or more endpoints, the administrator must enter **Confirm** in the secondary confirmation dialog box.

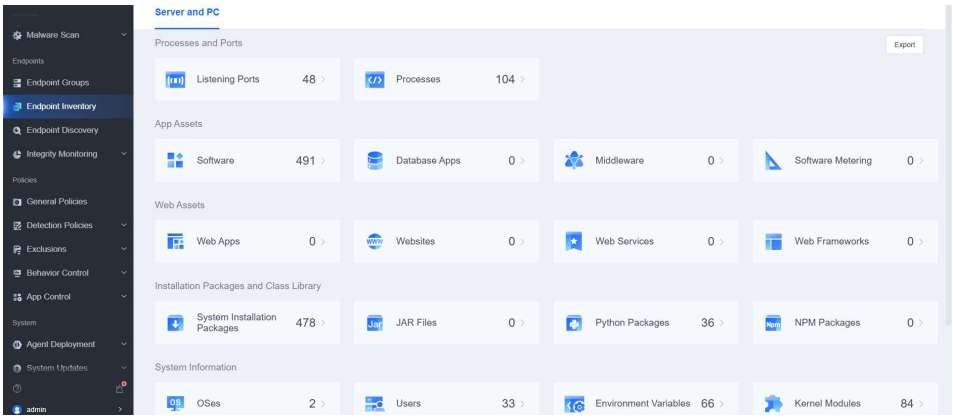


2. To perform these O&M and high-risk operations on less than 100 endpoints, the administrator must click **OK** in the dialog box.



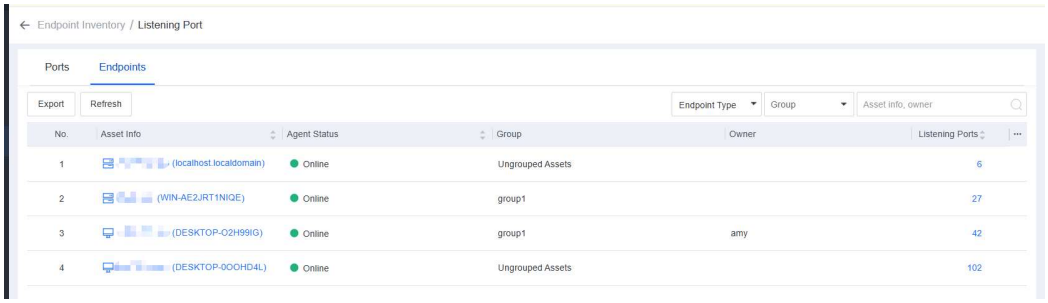
4.5.2 Endpoint Inventory

On the **Endpoint Inventory** page, you can view the statistics of all endpoints, including the **processes and ports**, **application assets**, **web assets**, **installation packages and class libraries**, and **system information** of servers and office PCs.

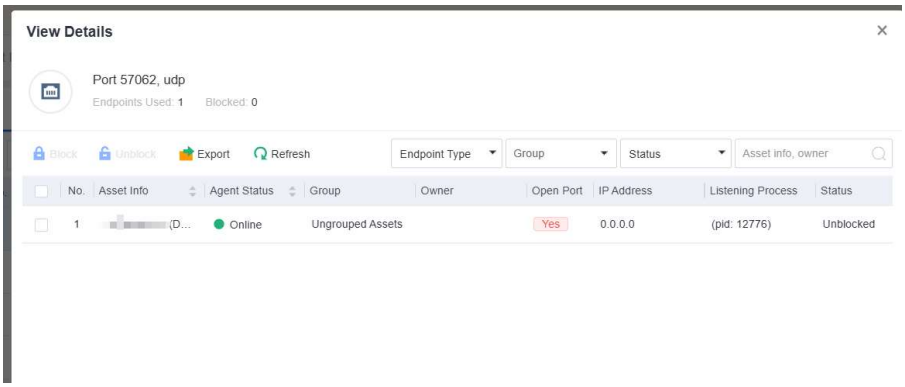


4.5.2.1 Listening Ports

On the **Listening Ports** page, you can efficiently view and check open ports on all endpoints as an administrator to identify and address risky ports by server or host or from a holistic perspective, as shown below.



The **Ports** tab, where you can view the number of endpoints with a specific port open. To further analyze these endpoints, click the number in the **Endpoints Used/Blocked** column to go to the **View Details** page, as shown in the following figure.

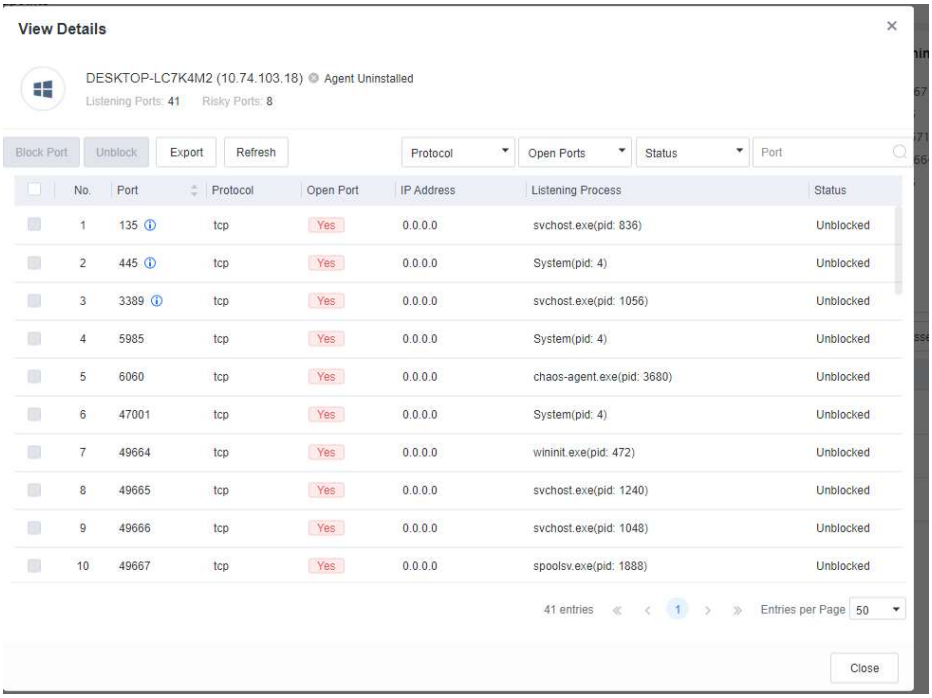


NOTE

Block Port: To block the port of an endpoint, select the endpoint and click **Block Port**. To unblock the port of an endpoint, select the endpoint and click **Unblock**.

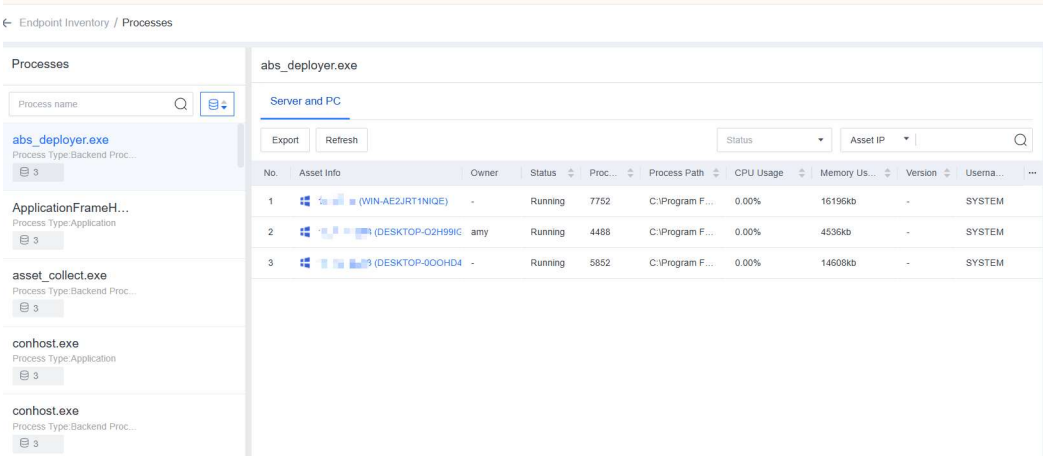
Export: To export the endpoint details in the form of a table for further analysis by administrators, click **Export**.

5. In the **Endpoints** tab, you can view the number of listening ports, status, name, IP address, and group of each endpoint. To view the listening port details or block the listening ports as needed, click the number in the **Listening Ports** column, as shown in the following figure.



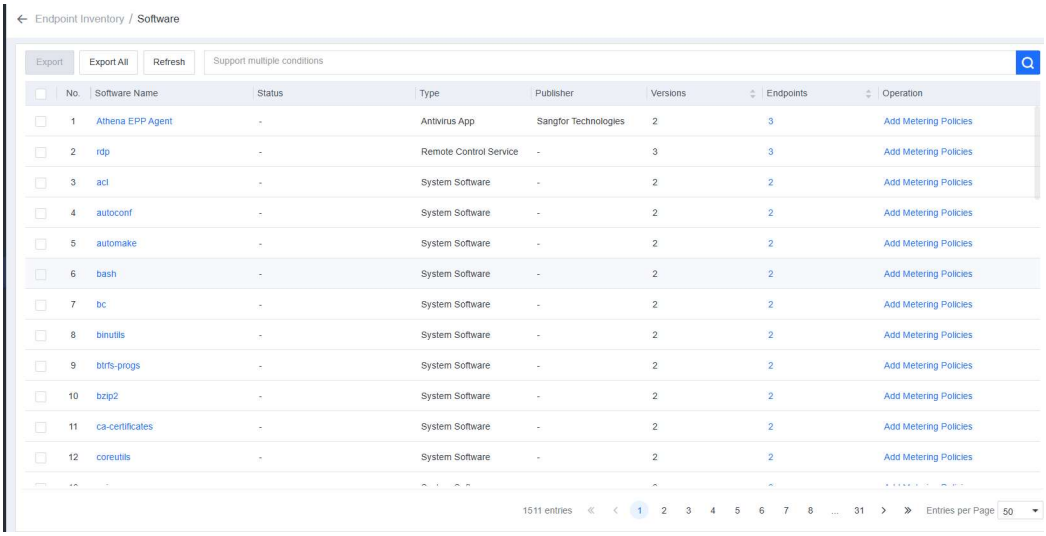
4.5.2.2 Processes

On the **Processes** page, you can view all processes in the left-side list and the details of endpoints hosting each process on the right, including the process status, process ID, process path, CPU usage, memory usage, version, username, parent process name, parent process ID, startup parameters, and startup time.

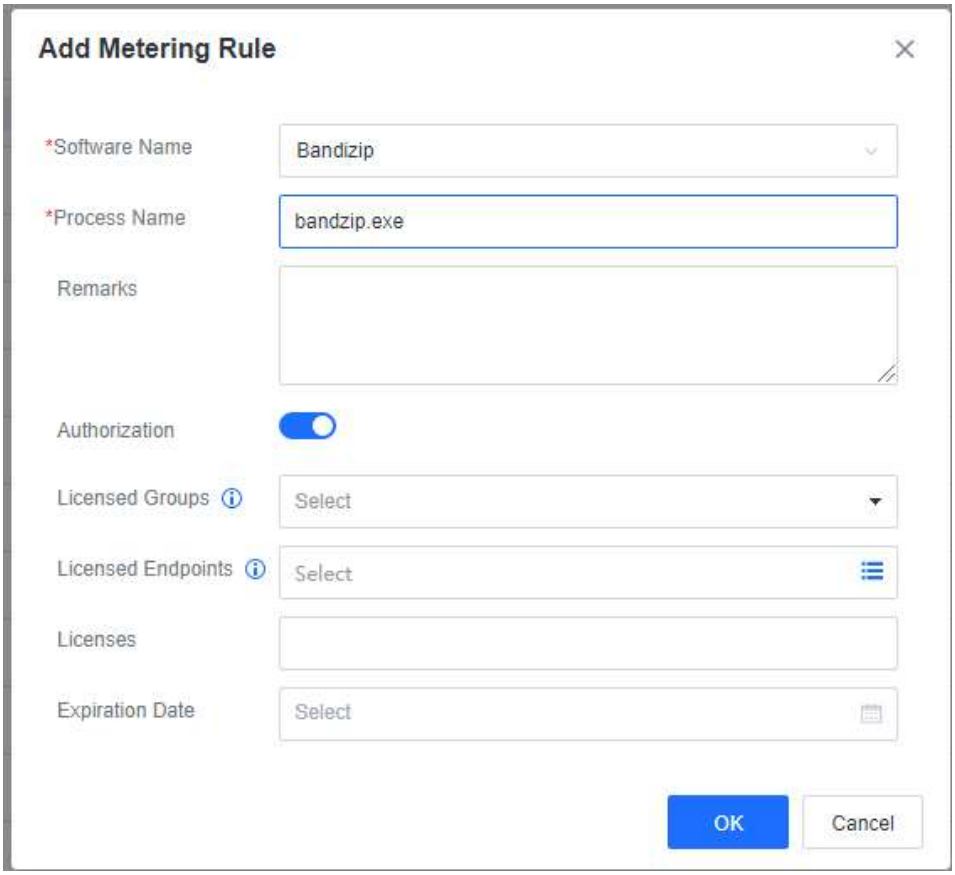


4.5.2.3 Software

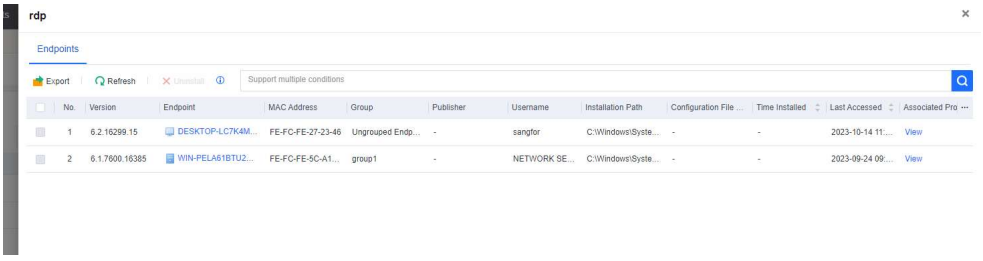
On the **Software** page, you can view software distribution across all endpoints sorted in descending order of the total number of installations and the number of endpoints for each piece of software, as shown below.



To add metering policies, click **Add Metering Policies**. You can also enable **Authorization** to issue a certain number of software licenses to specific groups or endpoints and set a license expiration date.



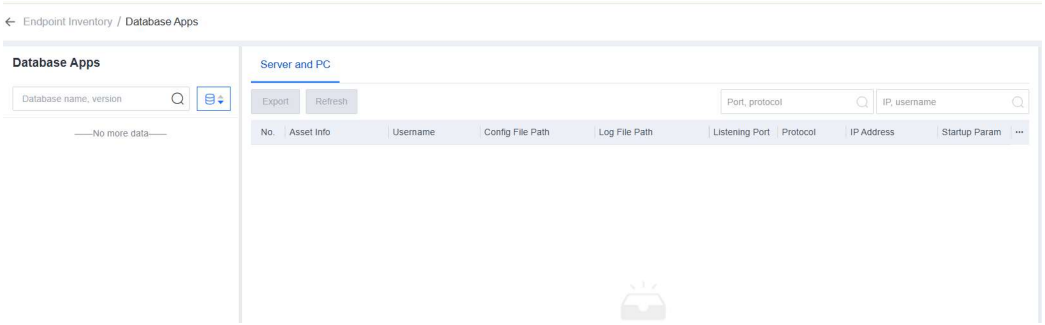
To view all the endpoints with a specific software installed, click the software name, as shown in the following figure.



You can also search for endpoints by software name or publisher and export the search result to an Excel file.

4.5.2.4 Database Apps

On the **Database Apps** page, you can view the summary and details of database applications installed on all endpoints to assess whether security measures such as version upgrades and application security enhancement are needed, as shown below.

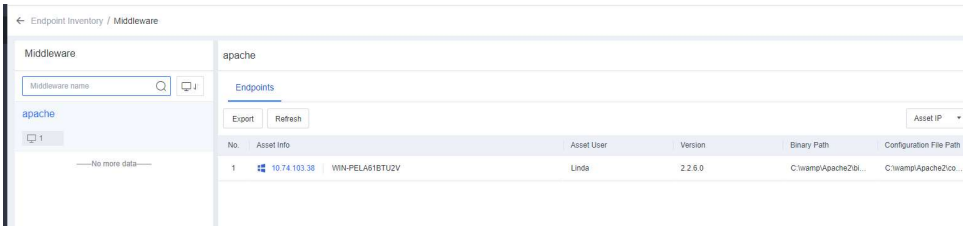


The page includes the following elements:

1. Database application distribution across all endpoints is sorted in descending order of the total number of installations and the number of endpoints for each database application.
2. A database search box that supports searching by database name or version, an endpoint search box that supports searching by port or protocol, and an endpoint search box that supports searching by IP address or username.

4.5.2.5 Middleware

On the **Middleware** page, you can view the summary and details of middleware installed on all endpoints as an administrator to understand the middleware types, versions, and quantities, as shown below.



The page includes the following elements:

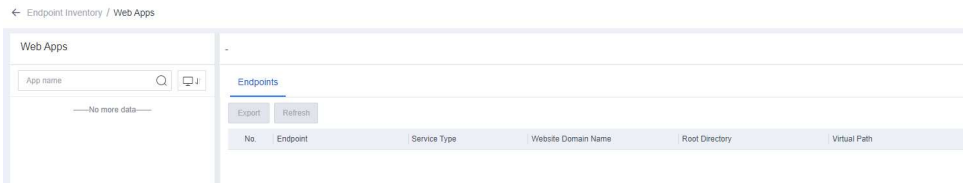
1. Middleware distribution across all endpoints is sorted in descending order

of the total number of installations and the number of endpoints for each piece of middleware.

2. A middleware search box that supports searching by middleware name and an endpoint search box that supports searching by asset IP address, asset user, or binary path.

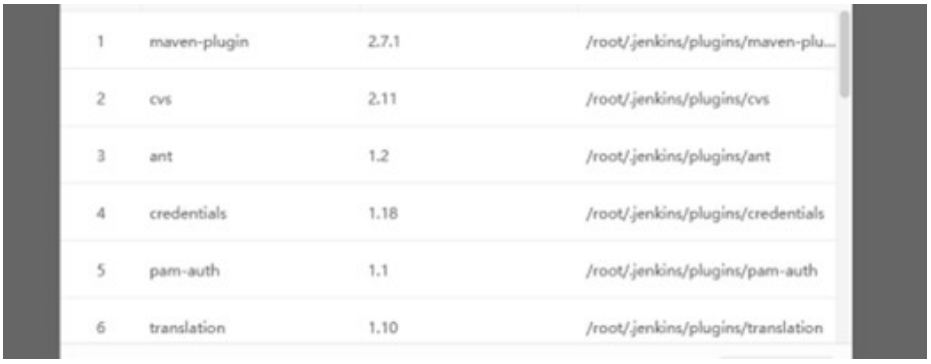
4.5.2.6 Web Apps

On the **Web Apps** page, you can view the summary and details of web applications installed on all endpoints as an administrator, as shown below.



The page includes the following elements:

1. Web application distribution across all endpoints is sorted in descending order of the total number of installations and the number of endpoints for each web application.
2. The plugin information of each web application on the endpoints.



3. A web application search box that supports searching by application name.

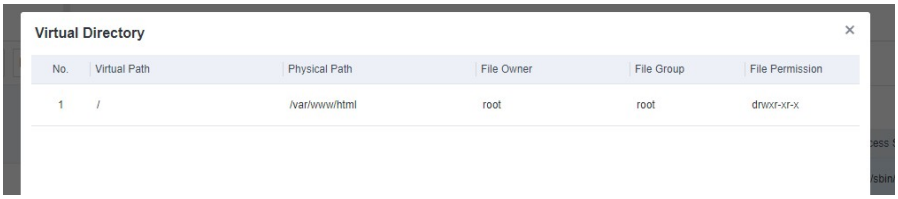
4.5.2.7 Websites

On the **Websites** page, you can view the summary and details of websites deployed on all endpoints as an administrator, as shown below.



The page includes the following elements:

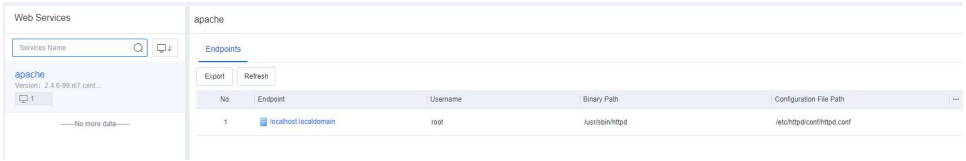
1. Website distribution across all endpoints is sorted in descending order of the total number of installations and the number of endpoints for each website.
2. The virtual directory information of each website on the endpoints.



3. A website search box that supports searching by port, protocol, or domain name and an endpoint search box that supports searching by IP address or username.

4.5.2.8 Web Services

On the **Web Services** page, you can view the summary and details of web services installed on all endpoints as an administrator, as shown below.

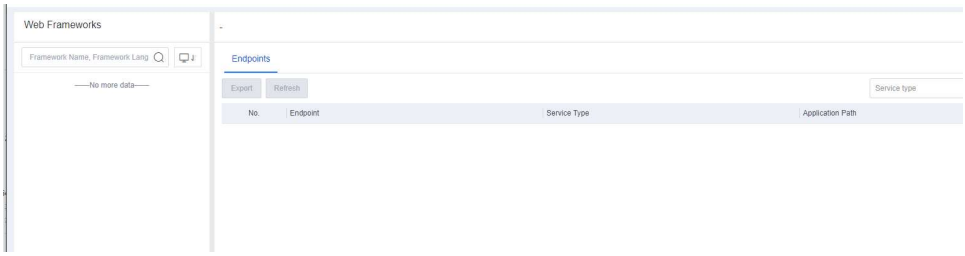


The page includes the following elements:

1. Web service distribution across all endpoints is sorted in descending order of the total number of installations and the number of endpoints for each web service.
2. A web service search box that supports searching by service name.

4.5.2.9 Web Frameworks

On the **Web Frameworks** page, you can view the summary and details of web frameworks installed on all endpoints as an administrator, as shown below.

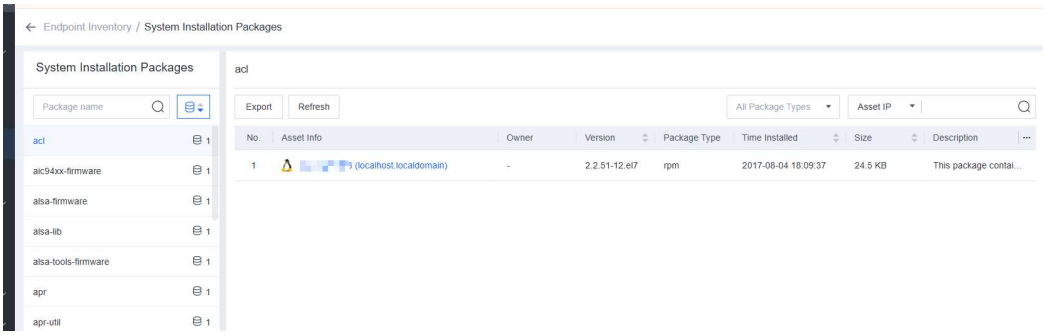


The page includes the following elements:

1. Web framework distribution across all endpoints is sorted in descending order of the total number of installations and the number of endpoints for each web framework.
2. A web framework search box that supports searching by framework name or language and an endpoint search box that supports searching by service type.

4.5.2.10 System Installation Packages

On the **System Installation Packages** page, you can view the summary and details of system installation packages on all Linux endpoints as an administrator, as shown below.

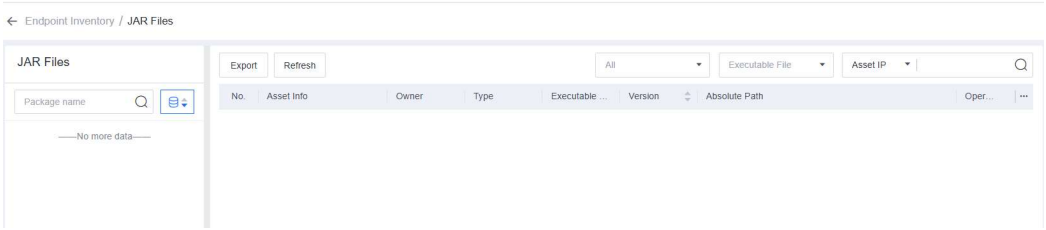


The page includes the following elements:

1. System installation package distribution across all Linux endpoints is sorted in descending order of the total number of installations and the number of endpoints for each system installation package.
2. A system installation package filter according to the package type, and a system installation package search box according to the asset IP, asset user, or version.

4.5.2.11 JAR Files

On the **JAR Files** page, you can view the summary and details of JAR files on all endpoints as an administrator, as shown below.

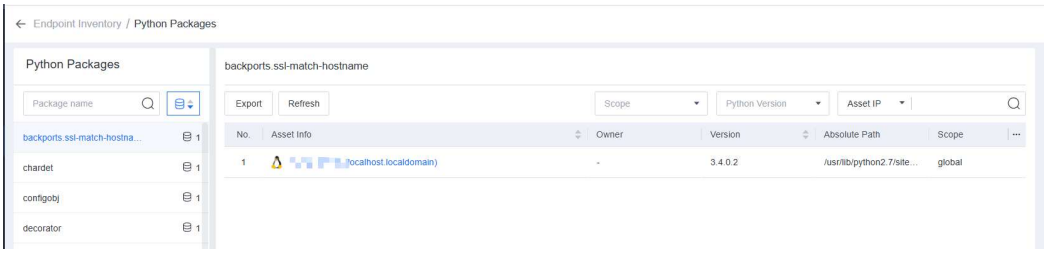


The page includes the following elements:

1. JAR file distribution across all endpoints is sorted in descending order of the total number of installations and the number of endpoints for each JAR file.
2. A JAR file filter that supports filter by file type (application, system library, web service library, and others). A JAR file that supports filter by executability file and a JAR file search box that supports searching by asset IP address, asset user, version, or absolute path.

4.5.2.12 Python Packages

On the **Python Packages** page, you can view the summary and details of Python packages on all endpoints as an administrator, as shown below.



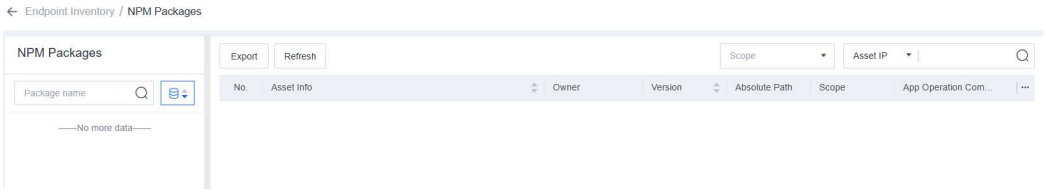
The page includes the following elements:

1. Python package distribution across all endpoints is sorted in descending order of the total number of installations and the number of endpoints for each Python package.

2. A Python package filter based on the scope (user and global), a Python package filter based on the Python version, and a Python package search box that supports searching by asset IP address, asset user, version, or absolute path.

4.5.2.13 NPM Packages

On the **NPM Packages** page, you can view the summary and details of NPM packages on all endpoints as an administrator, as shown below.

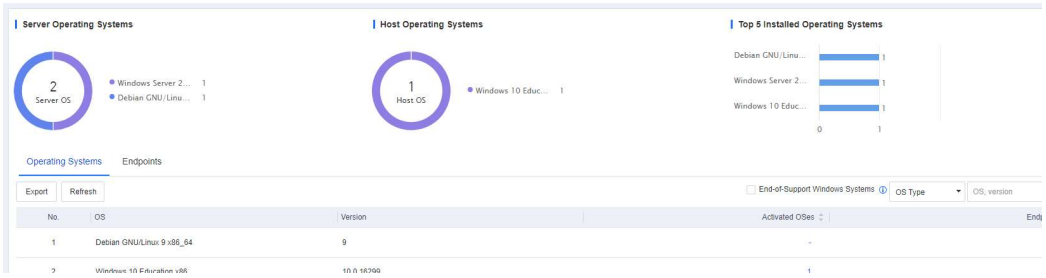


The page includes the following elements:

1. NPM package distribution across all endpoints is sorted in descending order of the total number of installations and the number of endpoints for each NPM package.
2. An NPM package filter based on the scope (user and global); An NPM package search box that supports searching by asset IP address, asset user, version, absolute path, PID, or application operation command.

4.5.2.14 OS

On the **OS** page, you can view the summary and details of operating systems on all endpoints as an administrator, as shown below.

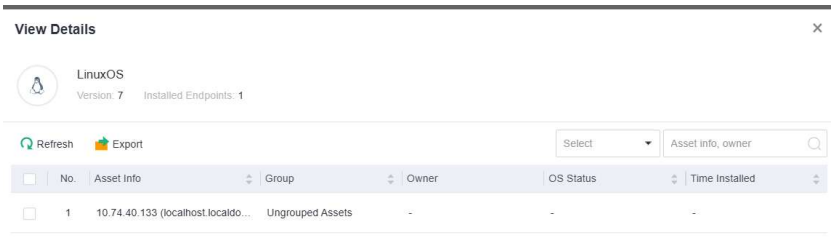


The page includes the following elements:

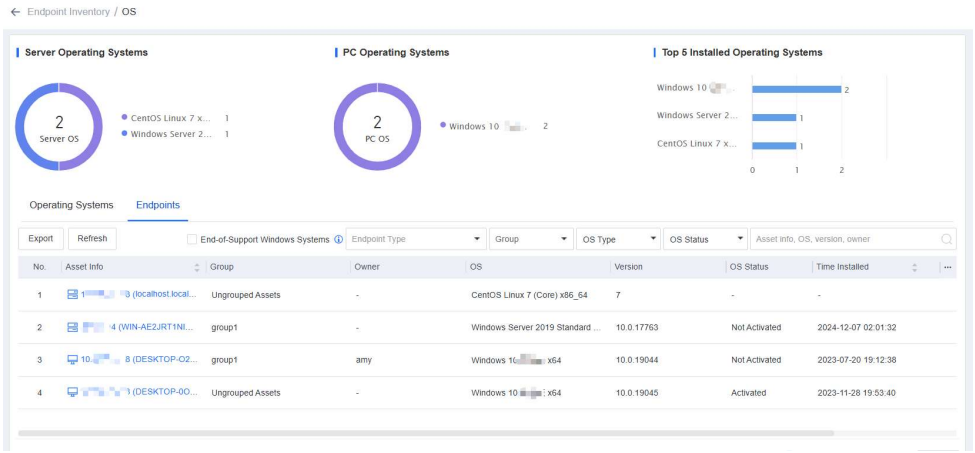
1. Distribution of different versions of server operating systems, distribution of different versions of host operating systems, and top 5 installed

operating systems.

In the **Operating Systems** tab, you can view the number of activated operating systems and endpoints with the corresponding operating system installed. You can click the number in the **Activated OSes** or **Endpoints** column to view details or click **Export** to export the operating system information in Excel format, as shown in the following figure.



2. In the **Endpoints** tab, you can view endpoint details such as the endpoint IP address, group, operating system type, operating system version, operating system status, installation time, and asset user, as shown in the following figure.



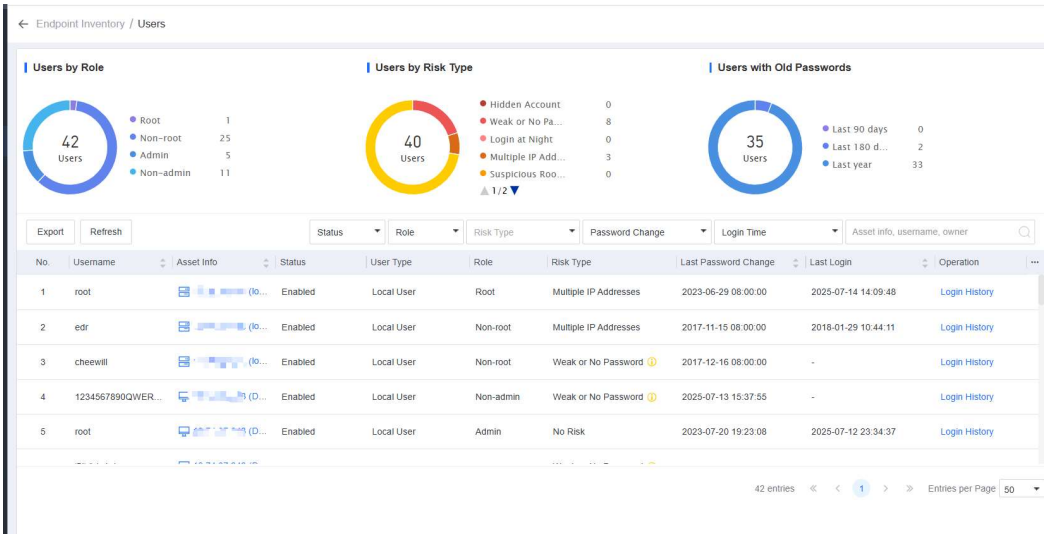
NOTE

You can click **Export** to export the details in an Excel file for further analysis as an administrator.

You can filter endpoints by endpoint type, group, operating system type, or status or directly search endpoints in the search box.

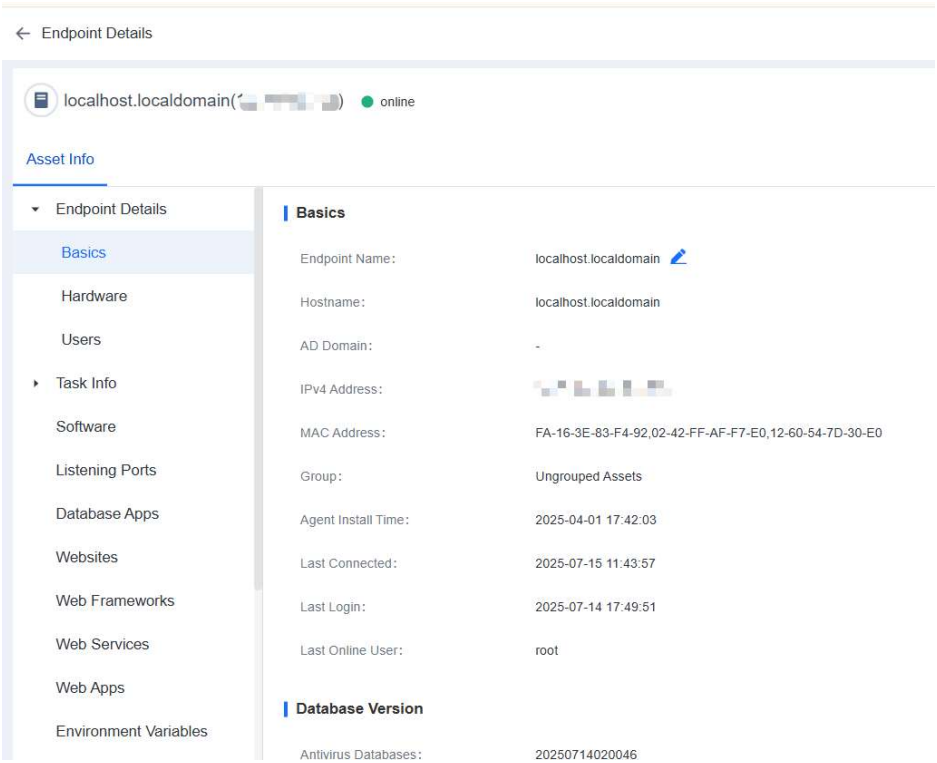
4.5.2.15 Users

On the **Users** page, you can check the user information of all endpoints to minimize the risk exposure of endpoints as an administrator. The displayed user information includes the account status, account type, account role, password status, risk analysis, and risk alerts (such as hidden account, weak or no password, suspicious root user, inactive user, login at night, and multiple IP addresses), as shown in the preceding figure.



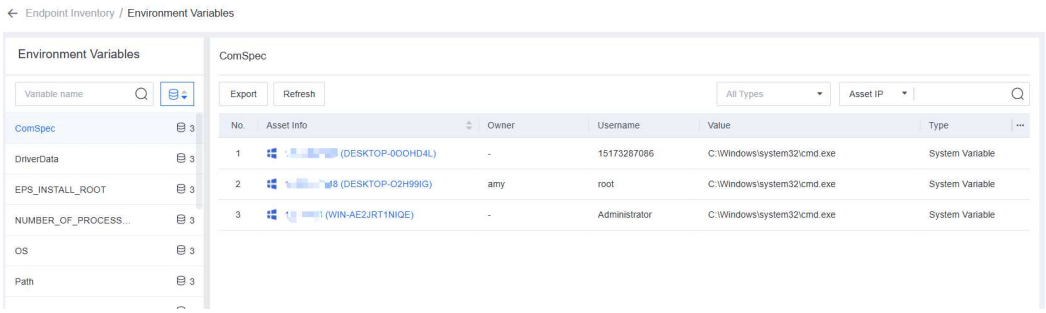
The page includes the following elements:

1. The distribution of users by role, users by risk type, and users with old passwords.
2. Filter by the account status, account role, risk type, latest password change, login time, and a search box that supports searching by endpoint name, IP, or username. Click the endpoint name to go to the **Endpoint Details** page, as shown in the following figure.



4.5.2.16 Environment Variables

On the **Environment Variables** page, you can view the summary and details of the environment variables of all endpoints as an administrator, as shown below.



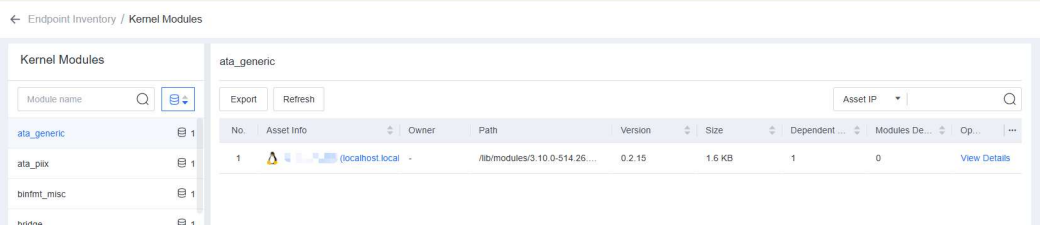
The page includes the following elements:

1. Environment variable distribution across all endpoints is sorted in descending order of the total number of installations and the number of endpoints for each environment variable.

2. An environment variable filter according to the environment variable type and an environment variable search box that supports searching by asset IP address, asset user, or environment variable value.

4.5.2.17 Kernel Modules

On the **Kernel Modules** page, you can view the summary and details of kernel modules on all endpoints as an administrator, as shown below.

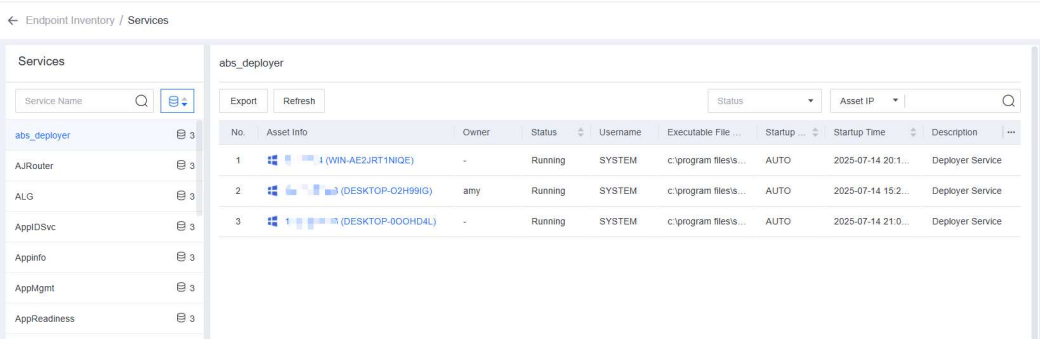


The page includes the following elements:

1. Kernel module distribution across all endpoints is sorted in descending order of the total number of installations and the number of endpoints for each kernel module.
2. An asset search box that supports searching by asset IP address, asset user, module path, or module version.

4.5.2.18 Services

On the **Services** page, you can view the summary and details of services on all endpoints as an administrator, as shown below.



The page includes the following elements:

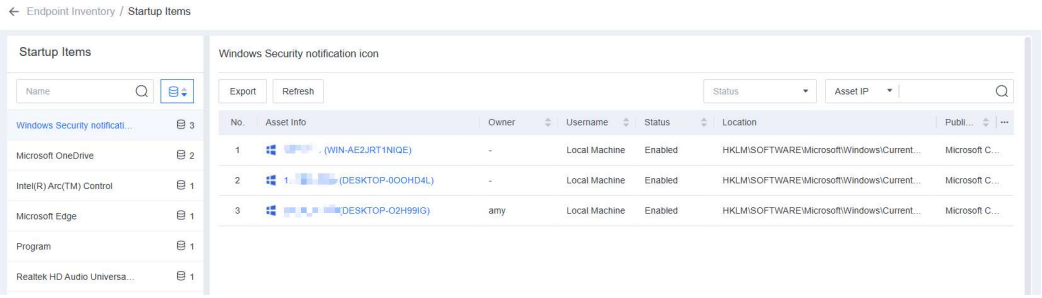
1. Service distribution across all endpoints is sorted in descending order of the total number of installations and the number of endpoints for each

service.

2. An asset filter according to the service status and an asset search box that supports searching by asset IP address, asset user, or executable file path.

4.5.2.19 Startup Items

On the **Startup Items** page, you can view the summary and details of the startup items of all endpoints as an administrator, as shown below.

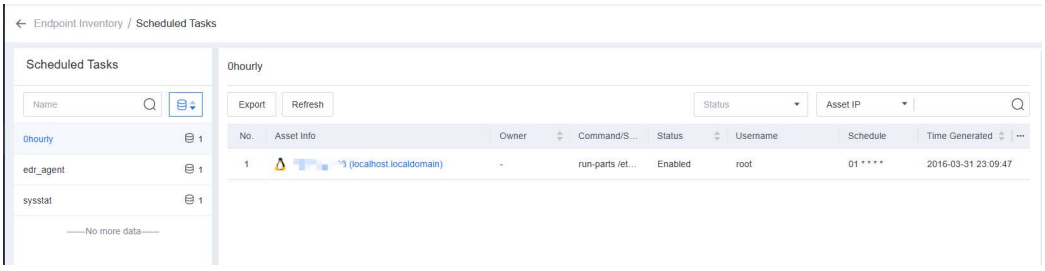


The page includes the following elements:

1. Startup item distribution across all endpoints is sorted in descending order of the total number of installations and the number of endpoints for each startup item.
2. An asset filter according to the service status and an asset search box that supports searching by asset IP address, asset user, or registry location.

4.5.2.20 Scheduled Tasks

On the **Scheduled Tasks** page, you can view the summary and details of the scheduled tasks of all endpoints as an administrator, as shown below.



The page includes the following elements:

1. Scheduled task distribution across all endpoints is sorted in descending order of the total number of installations and the number of endpoints for each scheduled task.
2. An asset filter according to the status and an asset search box that supports searching by asset IP address, asset user, or command/script.

4.5.2.21 Sharing

On the **Sharing** page, you can view the summary and details of shares on all endpoints as an administrator, including the shared path and sharing status, as shown below.

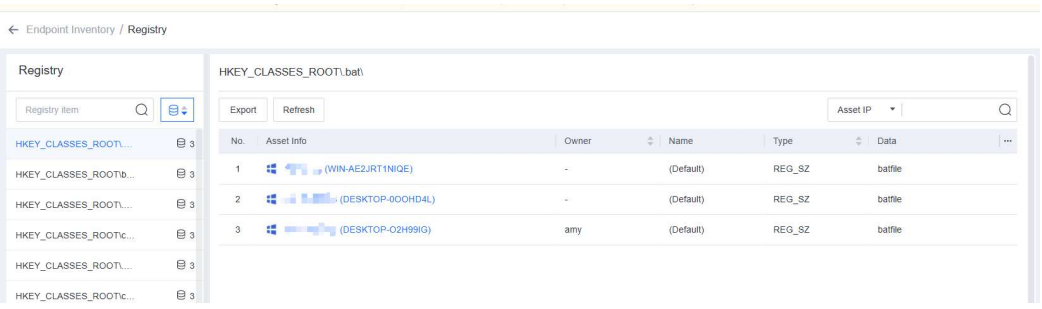


The page includes the following elements:

1. Sharing distribution across all endpoints is sorted in descending order of the total number of installations and endpoints for each sharing.
2. An asset filter according to the sharing status and an asset search box that supports searching by asset IP address, asset user, or shared path.

4.5.2.22 Registry

On the **Registry** page, you can view the summary and details of the registry items of all endpoints as an administrator, as shown below.

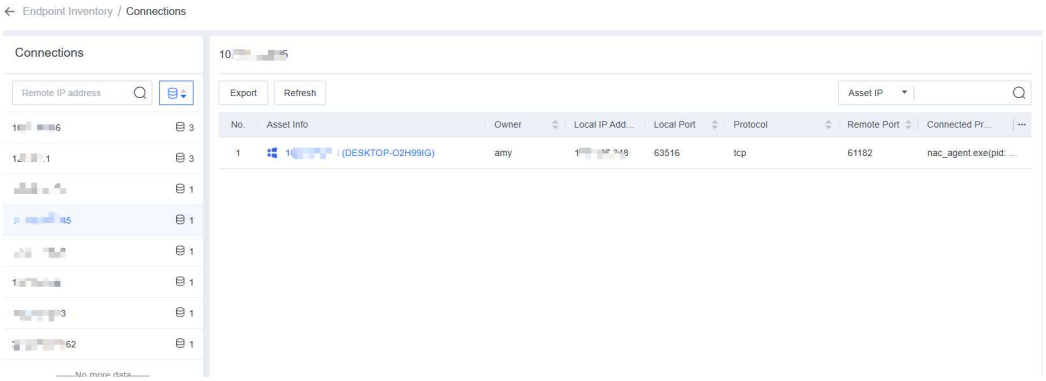


The page includes the following elements:

1. Registry item distribution across all endpoints is sorted in descending order of the total number of occurrences and endpoints for each registry item.
2. An asset search box that supports searching by asset IP address, name, or data.

4.5.2.23 Connections

On the **Connections** page, you can view the summary and details of the connections of all endpoints as an administrator, as shown below.

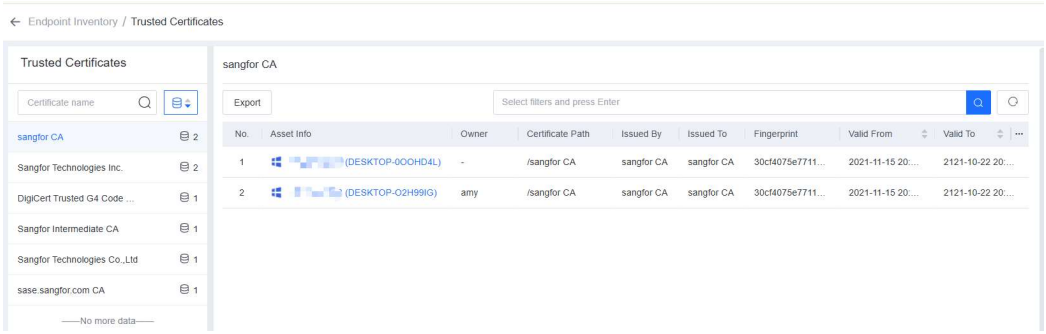


The page includes the following elements:

1. Connection distribution across all endpoint IP addresses in descending order of the number of connections and the number of endpoints connected to each remote IP address.
2. An asset search box that supports searching by asset IP address, asset user, local port, local IP address, remote port, or connected process.

4.5.2.24 Trusted Certificates

On the **Trusted Certificates** page, you can view the summary and details of the trusted certificates of all endpoints as an administrator, as shown below.

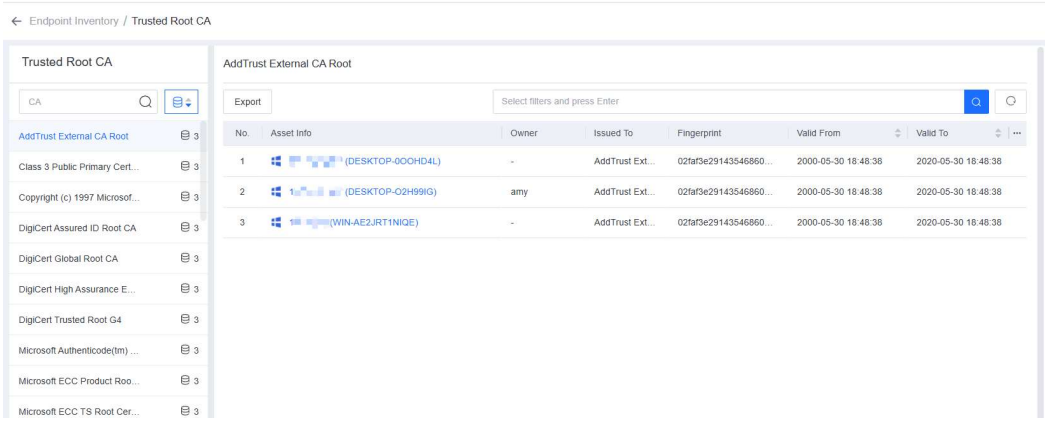


The page includes the following elements:

1. Trusted certificate distribution across all endpoints is sorted in descending order of trusted certificate usage and the number of endpoints for each trusted certificate.
2. An asset search box that supports searching by asset information, asset user, certificate path, issuer, receiver, fingerprint, validation time, or expiration time.

4.5.2.25 Trusted Root CA

On the **Trusted Root CA** page, you can view the summary and details of the trusted root certificate authorities (CAs) of all endpoints as an administrator, as shown below.



The page includes the following elements:

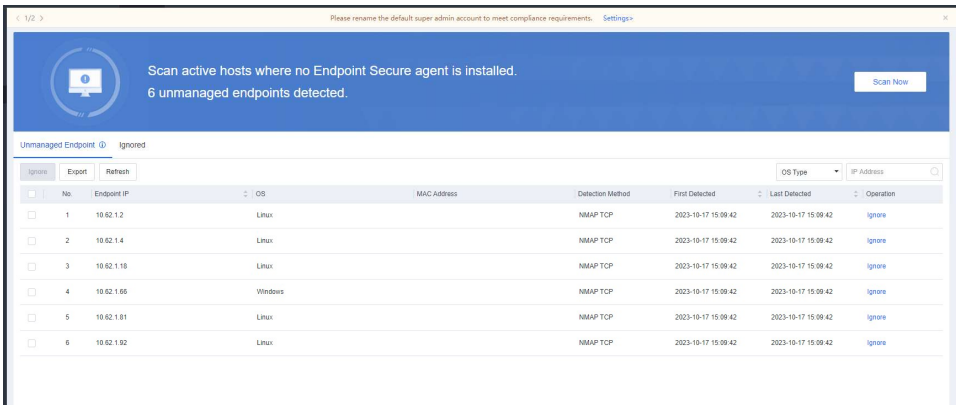
1. Trusted root CA distribution across all endpoints is sorted in descending order of the number of CAs and the number of endpoints for each CA.
2. An asset search box that supports searching by asset information, asset

user, receiver, fingerprint, validation time, and expiration time.

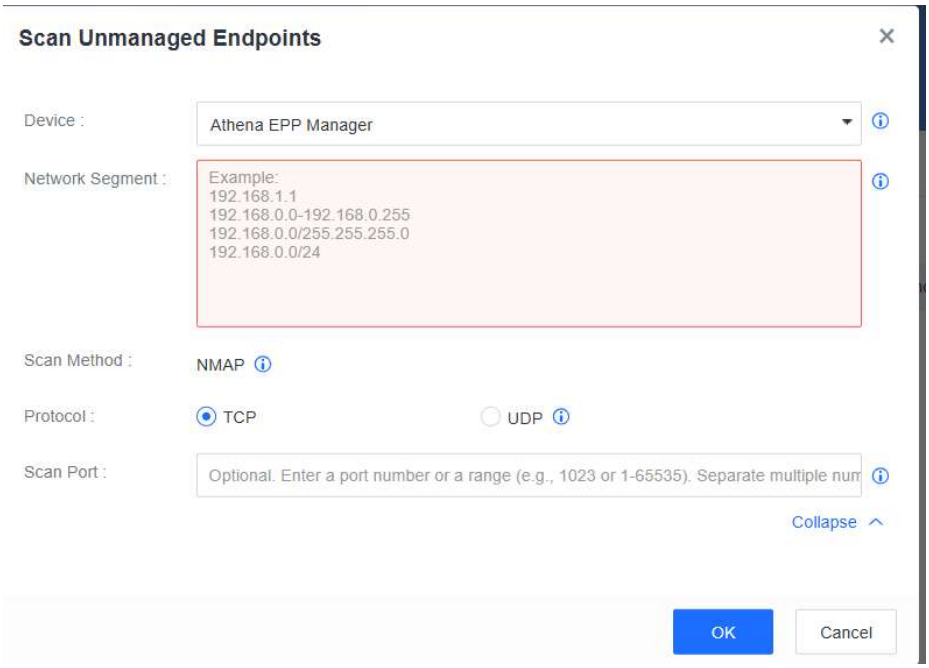
4.5.3 Endpoint Discovery

4.5.3.1 Unmanaged Endpoints

The **Unmanaged Endpoint** tab displays unmanaged endpoints (without the NovaGuard agent installed) in the enterprise's internal network that are proactively detected, as shown in the following figure.



1. Click **Scan Now** and set the following scan parameters to initiate a scan on the internal network:



Device: Select **NovaGuard manager** or **Endpoint**. Only Linux endpoints with the NovaGuard agent installed can initiate the scan if **Endpoint** is selected.

NOTE

Selecting multiple Linux endpoints with the NovaGuard agent installed is recommended to expedite the large-scale scanning.

Network Segment: Specify IP addresses, IP ranges, IP addresses and netmasks in a network segment.

NOTE

You can select a **Protocol** and specify a **Scan Port** in **Advanced** according to your needs.

2. Click **OK**. In the **OK** dialog box, read the content to fully understand the risks and click **OK** to start the scan.

NOTE

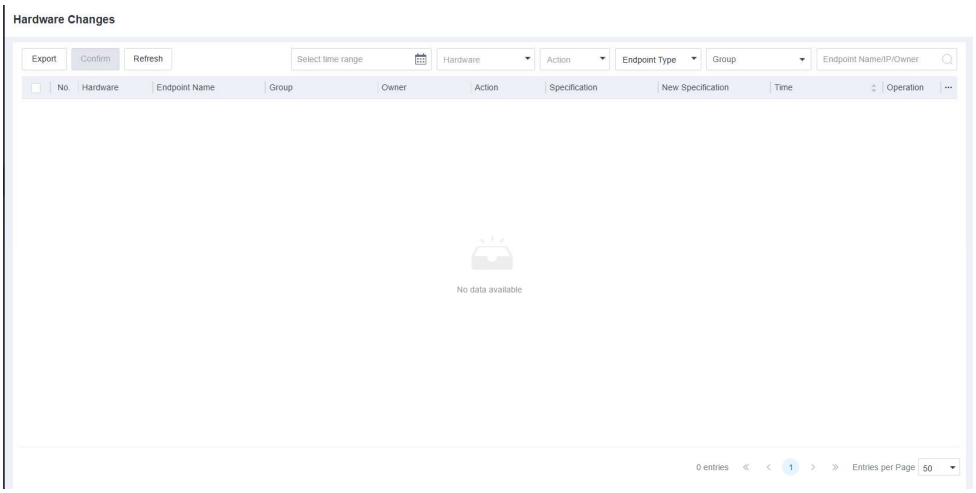
You can click **Cancel** to terminate the ongoing scan.

3. After the scan, view the endpoints without the NovaGuard agent installed on the page. To export the endpoint information in the form of a table for further analysis by administrators, click **Export** or click **Ignore** to ignore it.

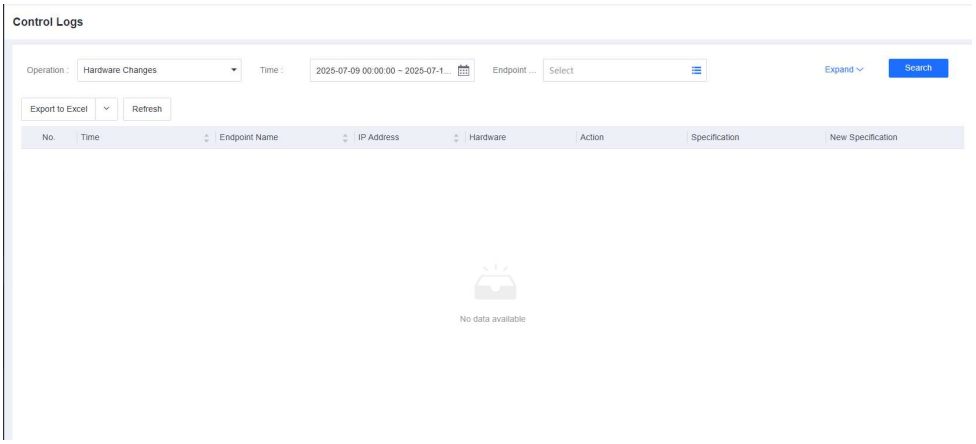
4.5.4 Integrity Monitoring

4.5.4.1 Hardware Changes

On the **Hardware Changes** page, you can view the hardware change time, hardware type, original hardware specification, and new hardware specification.



Changes on the **Hardware Changes** page are change logs administrators have not confirmed. Once an administrator clicks **OK** for a change log, the corresponding change log can be queried only on the **System** > **Logs** > **Control Logs** page.

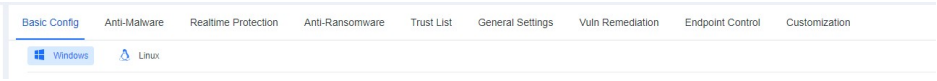


4.6 Policies

4.6.1 General Policies

You can configure security policies for different groups in this module. Policy settings include basic configurations, anti-malware, real-time protection, anti-ransomware, trust list, general settings, vulnerability remediation, endpoint control, and customization.

Go to **Policies** > **General Policies** to configure security policies for different groups, as shown in the following figure.



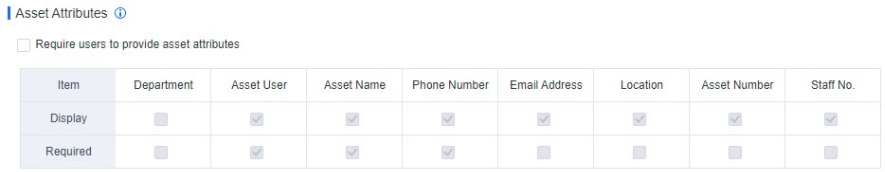
You can configure security policies for endpoints running on different operating systems by selecting the **Windows**, **Linux**, or **macOS** tab. The example used in this section illustrates the configuration of security policies for Windows endpoints, serving as a reference for configuring policies for endpoints running on other operating systems.

4.6.1.1 Basic Config

On this tab, you can configure the administrator's asset attributes, contact information, notifications, passwords, and policies for collecting endpoint behavior data and logs. For details, see the following description.

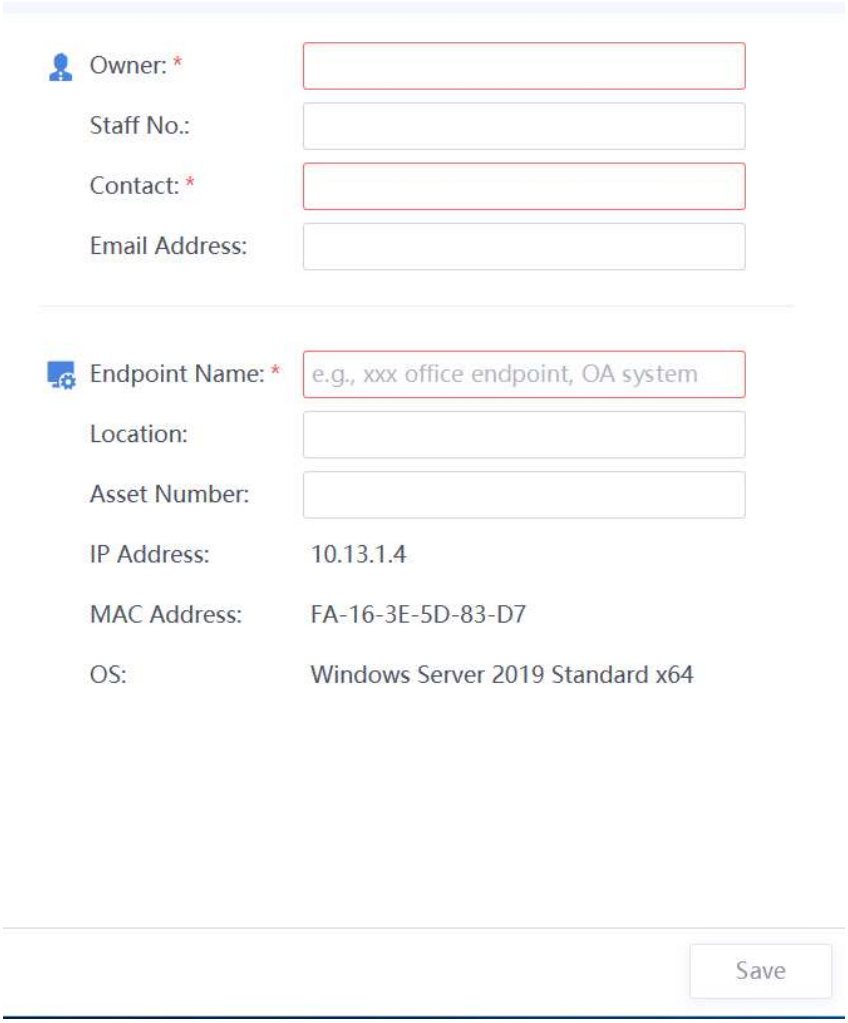
Asset Attributes

After selecting **Require users to provide asset attributes**, you can select asset attributes as needed, including the **Department, Asset User, Phone Number, Email Address, Location, Asset Number**, and **Staff No**., as shown in the following figure.



After the configuration, endpoint users can view the details in system messages and provide the asset information as required, as shown in the

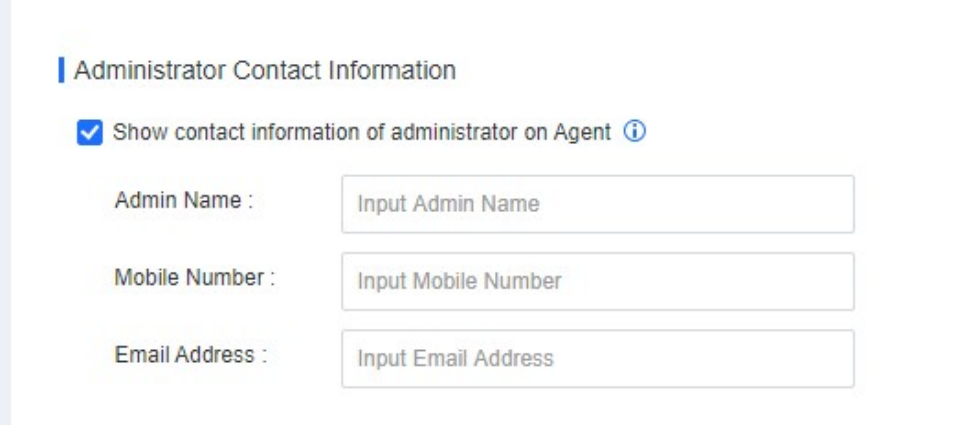
following figure.



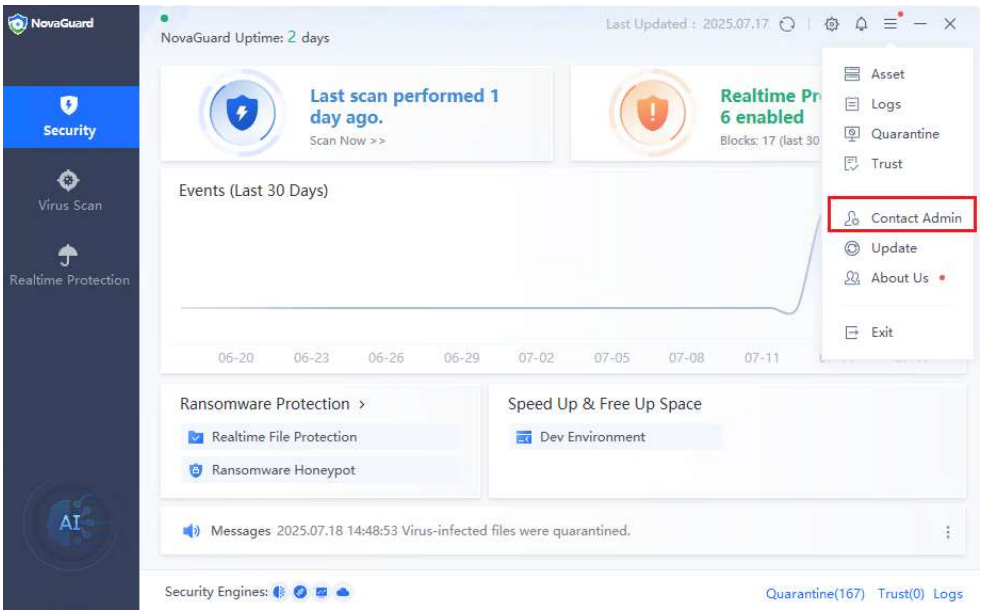
Administrator Contact Information

After selecting **Show contact information of administrator on Agent**, endpoint users can view the administrator's contact information, including the administrator name, mobile number, and email address, as shown in the

following figure.



The following figure shows how to view the administrator information on an endpoint.



Notifications (Mute notifications)

After selecting **Mute notifications**, endpoint users will not be notified when security issues are detected, as shown in the following figure.

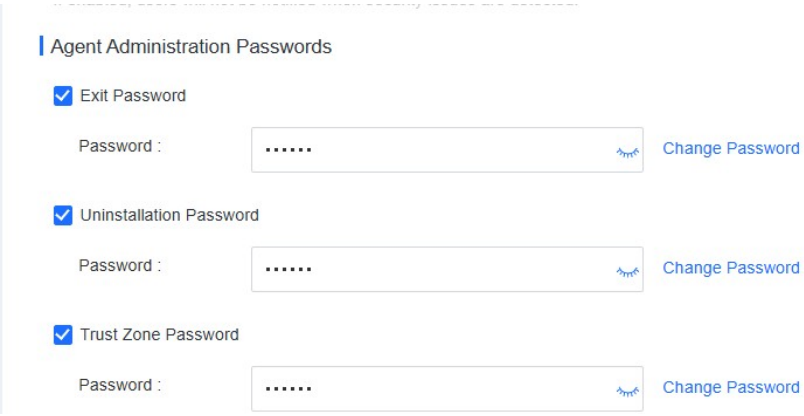


NOTE

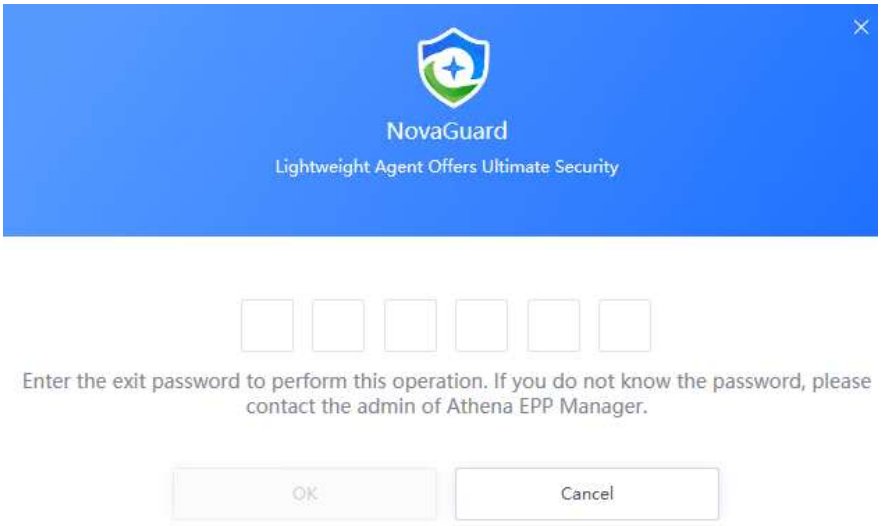
If the **Lock** icon is displayed, you cannot modify this option on the NovaGuard agent. If it is showing an **Unlock** icon, modification is allowed.

Agent Administration Passwords

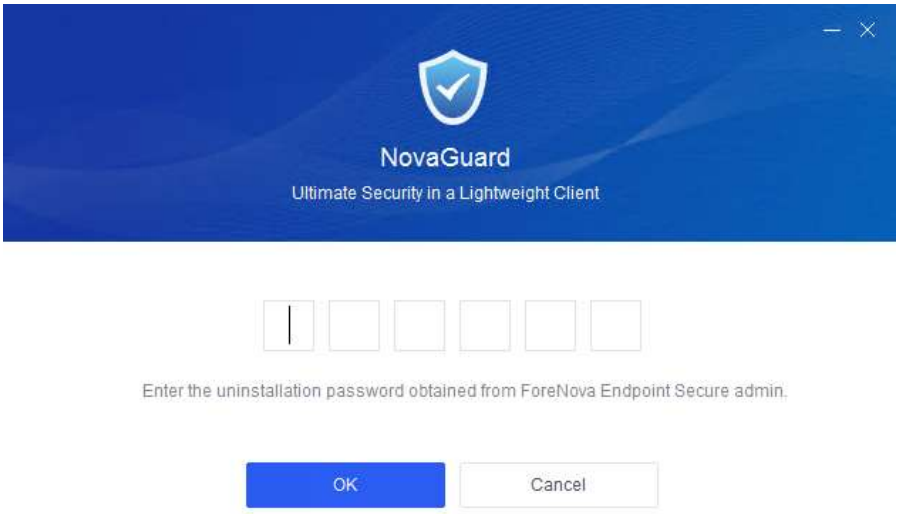
You can set **Exit Password**, **Uninstallation Password**, and **Trust Zone Password** as shown in the following figure.



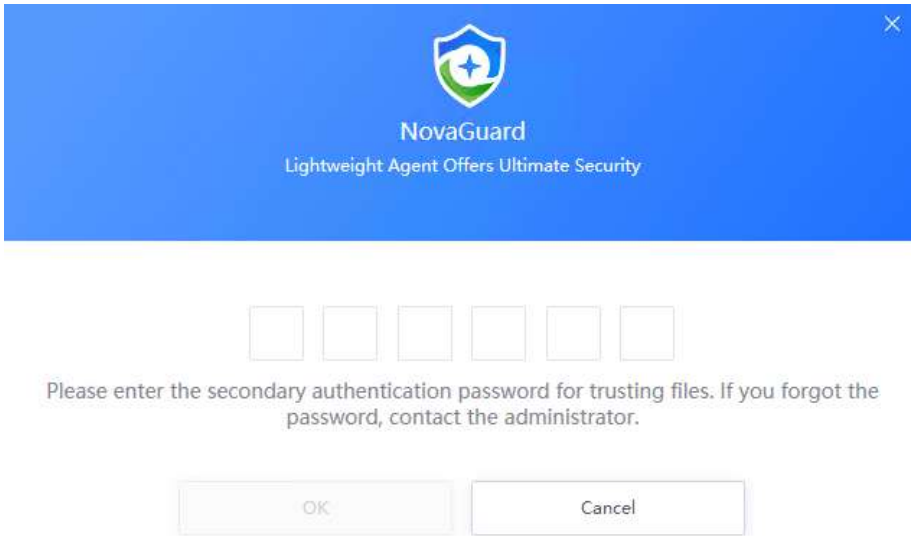
After selecting the **Exit Password,** an endpoint user is required to enter the password to exit the NovaGuard agent, as shown in the following figure.



After selecting the **Uninstallation Password**, an endpoint user is required to enter the password to uninstall the NovaGuard agent, as shown in the following figure.



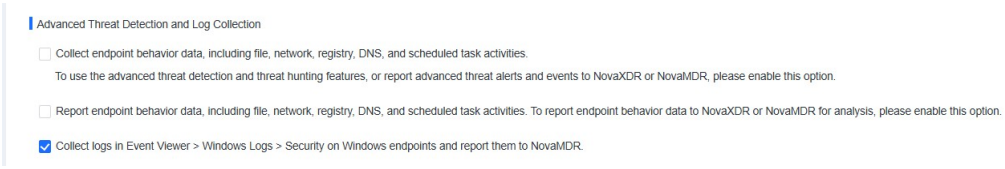
After selecting the **Enable password authentication for "trusted files"**, an endpoint user is required to enter the password to add a trusted file. It prevents unauthorized trust actions, ensuring that endpoints are protected on NovaGuard.



NOTE

The **Enable password authentication for "trusted files"** option is available for Windows endpoints only.

Advanced Threat Detection and Log Collection



Collect endpoint behavior data, including file, network, registry, DNS, and scheduled task activities: To use the advanced threat detecion and threat hunino features,or repot advaned threat alerts and events to NovaXDR or NovaMDR, please enable this option.

Report endpoint behavior data, including file, network, registry, DNS, and scheduled task activities: To report endpoint behavior data to NovaXDR or NovaMDR for analysis, please enable this option.

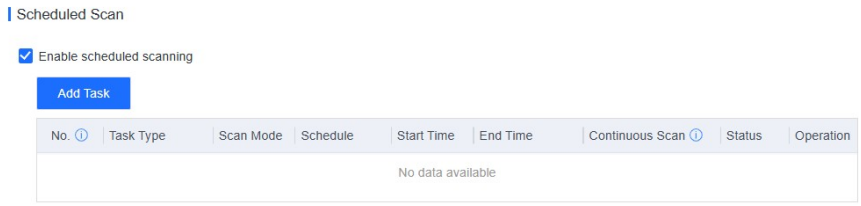
Collect logs in Event Viewer > Windows Logs > Security on Windows endpoints and report them to NovaMDR.

4.6.1.2 Anti-Malware

On this tab, you can configure the scheduled scan settings, malware scan settings, and antivirus database engine settings.

Scheduled Scan

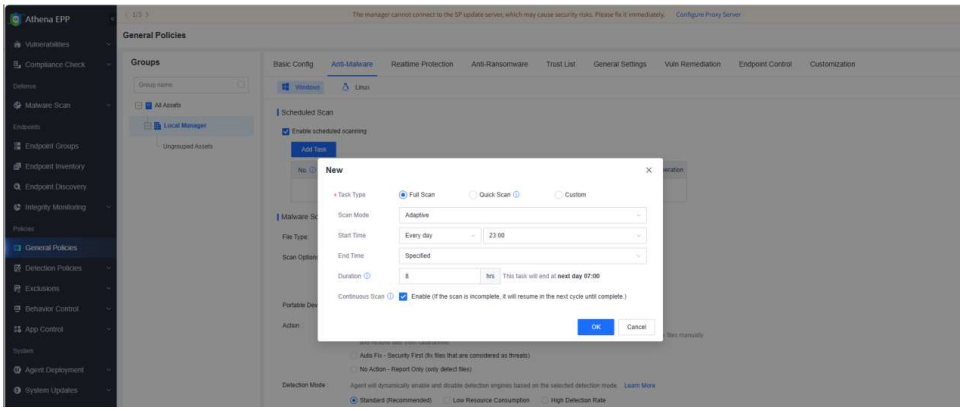
You can configure scheduled scan settings so that virus scans can be performed on endpoints in the internal network as scheduled, as shown in the following figure.



Scheduled scans can be performed in two ways: **Quick Scan** and **Full Scan**, each offering three CPU usage options: **High CPU**, **Adaptive**, and **Low CPU**, as described below:

- **High CPU:** Scanning consumes the most CPU resources, but the scan speed is the fastest.
- **Adaptive:** Dynamically adjusts CPU resources based on the CPU usage. It optimizes the scan speed by leveraging ample CPU resources when the CPU usage is low and minimizing resource consumption when the CPU usage is high, thus ensuring smooth service operations.
- **Low CPU:** Scanning consumes no more than 10% of CPU resources, but the scan speed is the slowest.

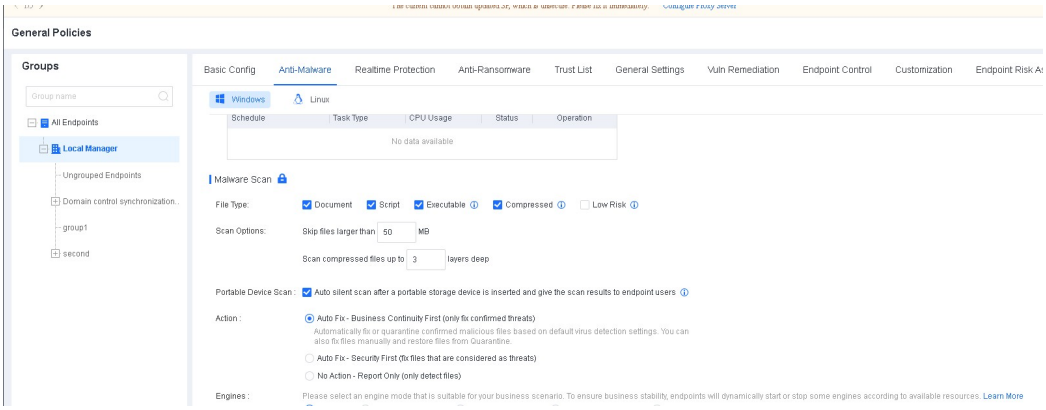
In addition, when you add a scheduled scan task for a Windows endpoint, you can choose to enable **Continuous Scan** as needed. For example, you have enabled **Continuous Scan** for a full scan task that is scheduled to run every day from 23:00 to 07:00 the next day. In this case, if the full scan task is not completed in the current cycle, the full scan task will resume in the next cycle until it is completed.



Malware Scan

You can configure settings such as the file types, scan options, actions required for malicious files, detection modes, and CPU usage, as shown in the following

figure.



NOTE

If the **Lock** icon is displayed, you cannot modify the settings on the NovaGuard agent. If the **Unlock** icon is displayed, modification is allowed.

File Type: Available options include **Document**, **Script**, **Executable**, **Compressed**, and **Low Risk**.

NOTE

1. A total of 23 compressed file extensions are supported, including 7z, XZ, BZIP2, GZIP, TAR, ZIP, and WIM. For details, click the ⓘ icon.

2. Selecting the **Low Risk** option is not recommended because these files are identified as posing an extremely minimal threat after analysis. Filtering out low-risk files can improve the scan speed and reduce the memory usage of ForeNova Engine Zero. Low-risk file types include the following 42 types:

.vmdk, .iso, .lib, .a, .nsf, .pdb, .dmp, .db, .hdmp, .idb, .pch, .vdf, .pak, .evtx, .imd, .aac, .webm, .ntf, .cvd, .mof, .mdf, .mdb, .otf, .tlb, .jpg, .jfif, .jpeg, .jpe, .jp2, .png, .gif, .bmp, .mp3, .mp4, .m4a, .mkv, .wmv, .wma, .tif, .tiff, .flv, and .ogg

Scan Options: You can specify the maximum file size and supported compressed file layers for scanning.

Portable Device Scan: You can initiate a silent scan when a portable device such as a USB flash drive, portable hard disk, mobile phone, or digital camera is connected to an endpoint. The endpoint user will receive the scan results once the scan is complete.

Action: You can specify the response to a detected malicious file. Select between **Auto Fix - Business Continuity First**, **Auto Fix - Security First**, and **No Action - Report Only**. The default action is **Auto Fix - Business Continuity First**.

- **Auto Fix - Business Continuity First:** Automatically fix or quarantine confirmed malicious files based on the default virus detection settings; do not automatically fix or quarantine suspicious files, but report them to the NovaGuard manager, allowing endpoint users to fix them.
- **Auto Fix - Security First:** Automatically fix or quarantine all malicious files and allow endpoint users to manually restore files from the Quarantine area. This option is suitable for scenarios with enhanced protection requirements.
- **No Action - Report Only:** Report malicious files to the NovaGuard manager, but do not automatically fix or quarantine them. This option suits scenarios where an on-duty security professional is responsible for fixing threats.

Detection Mode: Three detection modes are supported, including **Standard (Recommended)**, **Low Resource Consumption**, and **High Detection Rate**. Select a mode that aligns with your business scenario, as shown in the following figure.

Detection Modes

Detection Mode	Memory Usage	Detection Rate	False Positive Rate	Auto Fixing Rate
Standard	High	Medium	Low	High
Low Resource Consumption	Low	Low	Low	High
High Detection Rate	High	High	High	Medium

Detection Engines

Engine Zero
Uses AI and powerful generalization capabilities to detect unknown viruses and variants of known viruses.

Gene Analysis Engine
Extracts gene characteristics of virus families of hot events in depth to detect viruses more accurately. If enabled, it will use about 200 MB of memory. (© Bitdefender 1997-2025)

Behavioral Analysis Engine
Effective at detecting unknown virus variants by running them in virtual environments.

Cloud-Based Engine
Uses cloud-based capabilities to check unknown files based on indicators of compromise (such as file hash, DNS, URL, and IP address).

NOTE

1. In the **High Detection Rate** mode, false positives will be higher than other modes. Therefore, do not select this mode before a thorough assessment is carried out.

CPU Usage: If **Restrict** is selected, the CPU usage for NovaGuard is minimized. It may result in a longer virus scan duration. It applies to scenarios involving endpoints with legacy systems, virtual desktops, and overloaded systems.



NOTE

When **Restrict** is selected, the CPU usage of NovaGuard varies in different virus scan modes:

1. High CPU: Consumes no more than 50% of CPU resources.

2. Low CPU: Consumes no more than 5% of CPU resources.

Antivirus Database Engine

You can specify the antivirus database engine setting as **Update via Manager** or **Update via update servers**. If **Update via update servers** is selected, you can configure multiple update servers (including the NovaGuard manager), as shown in the following figure.



In the **Operation** column, you can click **Up** or **Down** to adjust the order of the update servers for the antivirus database.

4.6.1.3 Realtime Protection

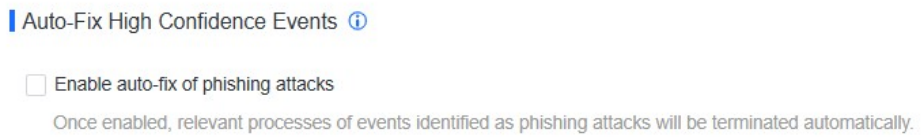
On this tab, you can configure settings such as **Auto-Fix of High Confidence Events**, **Realtime File Protection**, **Hacktool Protection**, **WebShell Detection**, **Brute-Force Attack Detection**, **Suspicious Login Detection**, and **Fileless Attack Protection**.

NOTE

You can click the icon on the right of a setting to lock it and prevent it from being modified on the NovaGuard agent.

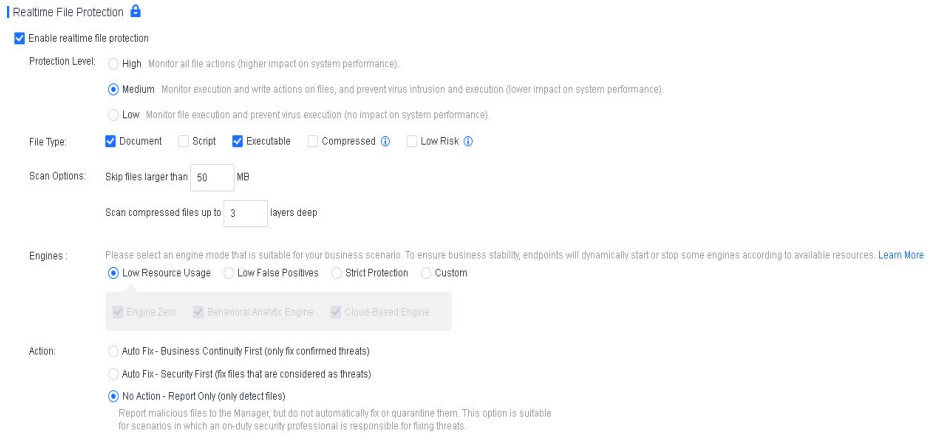
Auto-Fix of High Confidence Events

This feature can automatically analyze and fix advanced threats, skip core processes and business processes of the operating system, and automatically terminate processes of events identified as threats.



Realtime File Protection

You can enable real-time file protection to monitor the read, write, and execution actions on files within an endpoint. It can prevent the impact of malicious files on the endpoint, as shown in the following figure.



Relevant parameters are described as follows:

Protection Level: Three protection levels are available against malicious files, with the following differences:

- **High**: Monitor all file actions (higher impact on system performance).
- **Medium**: Monitor execution and write actions on files, and prevent virus intrusion and execution (lower impact on system performance).
- **Low**: Monitor file execution and prevent virus execution (no impact on system performance).

File Type: Available options include **Document**, **Script**, **Executable**, **Compressed**, and **Low Risk**.

NOTE

1. A total of 23 compressed file extensions are supported, including 7z, XZ, BZIP2, GZIP, TAR, ZIP, and WIM. For details, click the ⓘ icon.

2. The **Low Risk** option is not recommended because these files are identified as posing an extremely minimal threat after analysis. Filtering out low-risk files can improve the scan speed and reduce the memory usage of ForeNova Engine Zero. Low-risk file types include the following 42 types:

.vmdk, .iso, .lib, .a, .nsf, .pdb, .dmp, .db, .hdmp, .idb, .pch, .vdf, .pak, .evtx, .imd, .aac, .webm, .ntf, .cvd, .mof, .mdf, .mdb, .otf, .tlb, .jpg, .jfif, .jpeg, .jpe, .jp2, .png, .gif, .bmp, .mp3, .mp4, .m4a, .mkv, .wmv, .wma, .tif, .tiff, .flv, and .ogg

Scan Options: You can specify the maximum file size and supported compressed file layers for scanning. In most cases, malicious files are small.

Detection Mode: Two detection modes are supported, including **Low Resource Consumption (Recommended)** and **Standard**. Select a mode that aligns with your business scenario, as shown in the following figure.

Detection Mode	Memory Usage	Detection Rate	False Positive Rate	Auto Fixing Rate
Low Resource Consumption	Low	Medium-Low	Low	High
Standard	High	Medium	Low	High

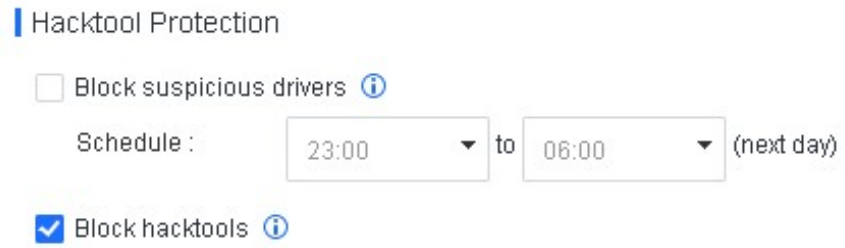
Action: You can specify the response to a detected malicious file. Select between **Auto Fix - Business Continuity First**, **Auto Fix - Security First**, and **No Action - Report Only**. The default action is **Auto Fix - Business Continuity First**.

- **Auto Fix - Business Continuity First**: Automatically fix or quarantine confirmed malicious files based on the default virus detection settings; do not automatically fix or quarantine suspicious files, but report them to the NovaGuard manager, allowing endpoint users to fix them.
- **Auto Fix - Security First**: Automatically fix or quarantine all malicious files and allow endpoint users to manually restore files from the Quarantine area. This option is suitable for scenarios with enhanced protection requirements.

- **No Action - Report Only**: Report malicious files to the NovaGuard manager, but do not automatically fix or quarantine them. This option suits scenarios where an on-duty security professional is responsible for fixing threats.

Hacktool Protection

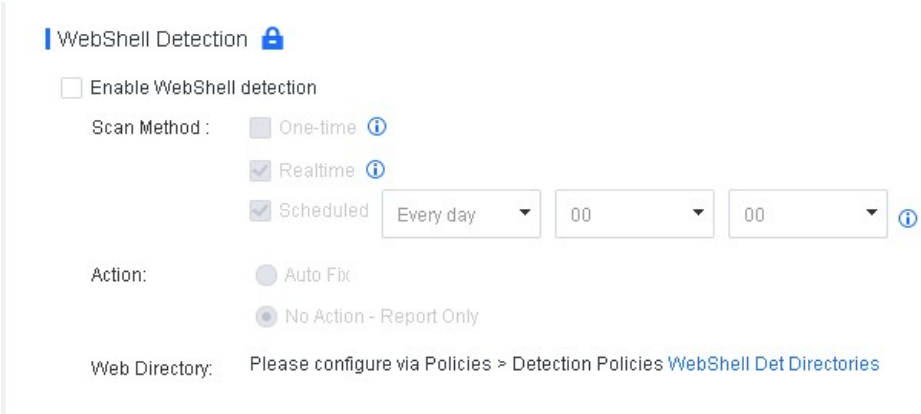
This feature can effectively block the defense evasion tactics that hackers employ during ransomware attacks, protecting endpoint users from ransomware.



- **Block suspicious drivers**: Give alerts and block suspicious drivers' loading, running, and other behaviors during the specified scheduled period.
- **Block hacktools**: Give alerts and block the loading, running, and other behaviors of untrusted drivers and hacktools.

WebShell Detection

When this feature is enabled, you can specify a scan method and the action for detected web shells, as shown in the following figure.



Relevant parameters are described as follows:

Scan Method: Available options include **One-time**, **Realtime**, and **Scheduled**.

- **One-time**: Scan the root directory and its subdirectories upon the first installation of the NovaGuard agent on an endpoint.
- **Realtime**: Scan new files on an endpoint in real time.
- **Scheduled**: Scan all files on an endpoint as scheduled.

Action: You can specify the action for detected web shells. Supported options include **Auto Fix** and **No Action - Report Only**.

Web Directory: You can configure the web shell detection directory, and it will be scanned by default. You can also specify a custom directory.

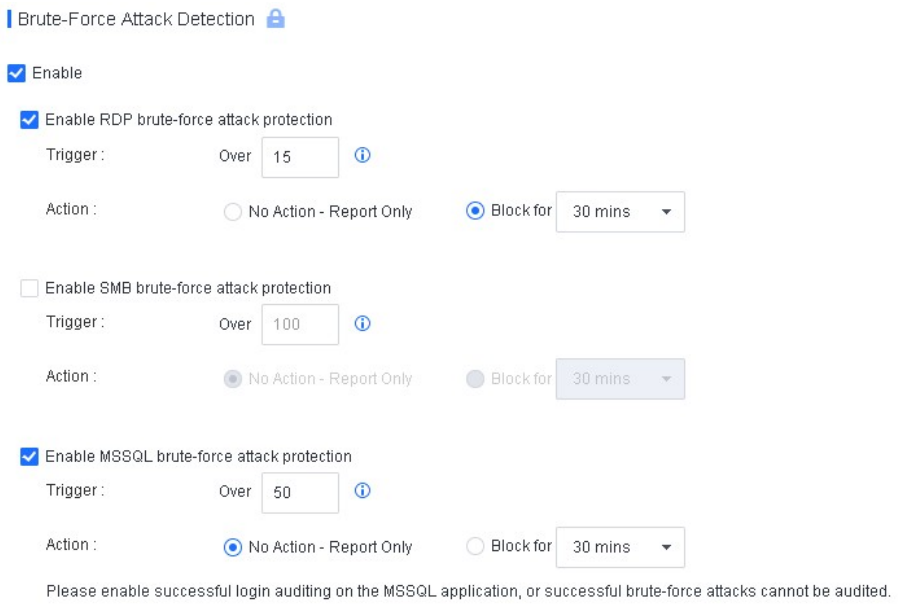
NOTE

Web shell detection is available for Windows Server and Linux endpoints.

Brute-Force Attack Detection

This feature detects and blocks RDP, SMB, Microsoft SQL Server, and SSH brute-force attacks. You can enable RDP, SMB, and Microsoft SQL Server brute-force attack protection for Windows endpoints and SSH brute-force attack protection for Linux endpoints.

Settings for **Windows** endpoints are shown in the following figure.



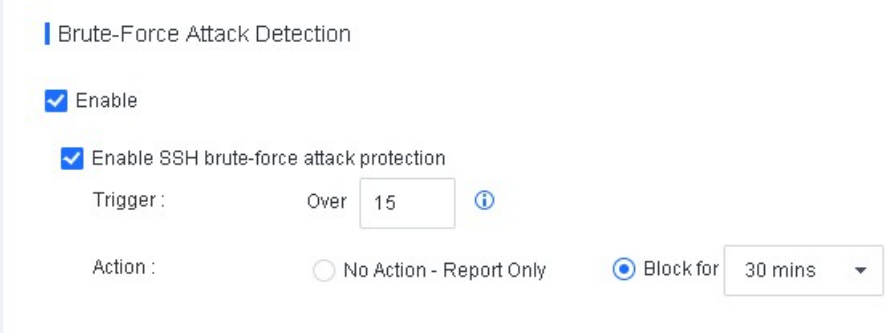
Relevant parameters are described as follows:

- **Trigger:** You can specify the threshold for identifying a quick brute-force attack. A brute-force attack is identified as a quick attack if the number of its consecutive attempts exceeds the specified value within a minute. For RDP and SMB quick brute-force attacks, you can specify an integer in the range of 1 to 100 and an integer in the range of 20 to 1,000, respectively. Slow and distributed brute-force attacks are identified based on an intelligent algorithm.
- **Action:** For identified attacks, select **No Action - Report Only** or **Block** for specific minutes.

NOTE

Enable successful login auditing on the Microsoft SQL Server application or successful brute-force attacks cannot be audited.

Settings for **Linux** endpoints are shown in the following figure.



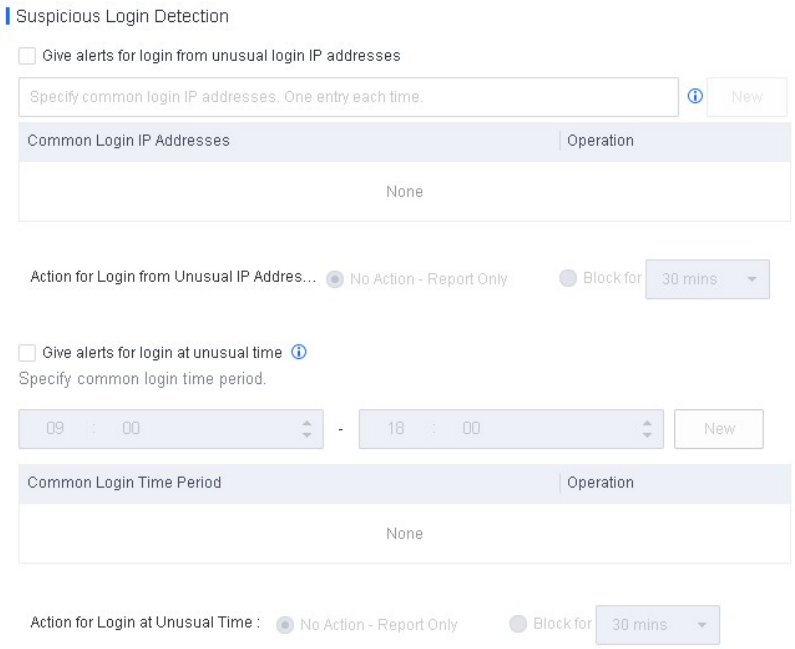
Relevant parameters are described as follows:

- **Trigger:** You can specify the threshold for identifying a quick brute-force attack. A brute-force attack is identified as a quick attack if the number of consecutive attempts exceeds the specified value within a minute. You can specify an integer from 1 to 100 for SSH quick brute-force attacks. Slow and distributed brute-force attacks are identified based on an intelligent algorithm.
- **Action:** For identified attacks, select **No Action - Report Only** or **Block** for specific minutes.

Suspicious Login Detection

NovaGuard can detect and automatically block logins at an unusual time or from uncommon IP addresses.

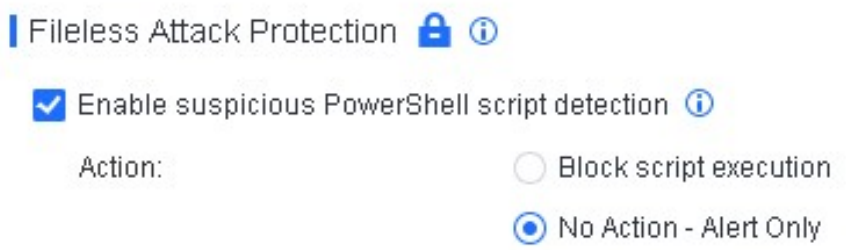
NovaGuard can detect suspicious logins on Windows endpoints (including PCs) via RDP and SMB and those on Linux endpoints via SSH.



Fileless Attack Protection

A fileless attack is an advanced technique employed by attackers to exploit vulnerable applications to inject code into the memory and normal system processes, such as the registry, PowerShell scripts, and Microsoft Office documents, aiming to gain access permissions and execute attack commands on target devices. Fileless attack protection enables the detection and handling of suspicious PowerShell scripts. The settings for this feature are shown in the

figure below:



Relevant parameters are described as follows:

Enable suspicious PowerShell script detection: This option takes effect only when **Realtime File Protection** is enabled.

Action: Available options include **Block script execution** and **No Action - Alert Only** (recommended). When suspicious PowerShell scripts are detected:

- For PCs, NovaGuard generates alerts and suspends the scripts. Endpoint users can then allow or block the scripts.
- For servers, NovaGuard generates alerts but does not suspend the scripts. Endpoint users can determine whether to block or ignore the scripts.

The following alert is generated when a suspicious script is detected.



4.6.1.4 Anti-Ransomware

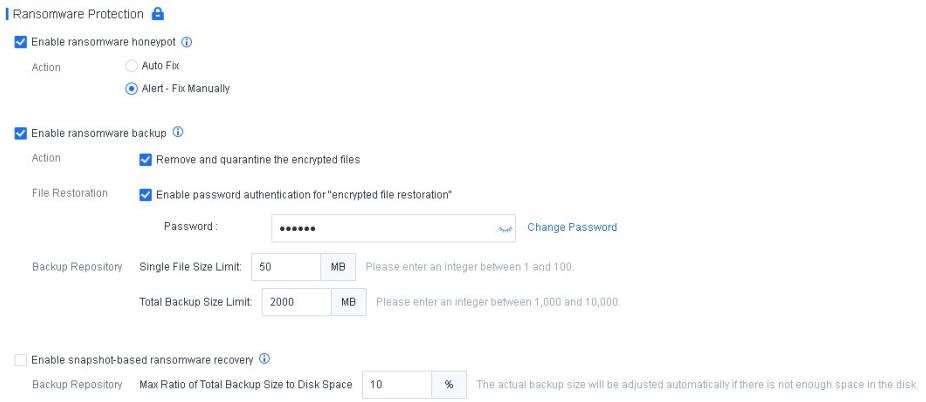
On this tab, you can configure policy settings for ransomware honeypot, RDP secondary authentication, and trusted processes.

Ransomware Protection

When **Ransomware Protection** is enabled, the NovaGuard agent promptly generates alerts and blocks any encryption behavior involving decoy files placed in crucial system directories on an endpoint. This proactive response is triggered upon detecting ransomware on the endpoint, effectively preventing the encryption of any business files. In addition, when a suspicious encryption process is detected, NovaGuard backs up certain file modifications or deletion operations performed by the process in real time and detects the encryption of certain files after the ransomware is already running. Finally, in scenarios

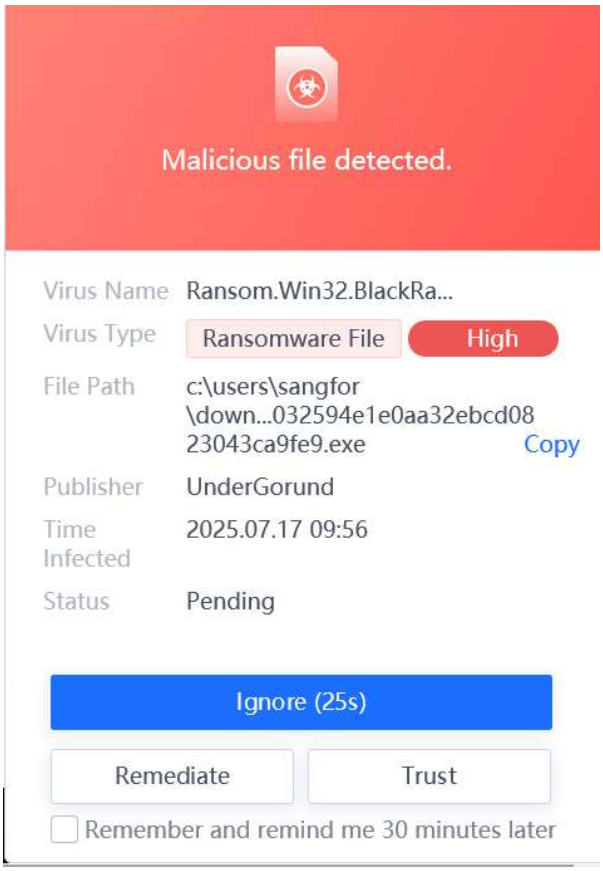
where ransomware successfully bypasses the current virus detection policies, this feature enables you to restore the endpoint based on the snapshot using Windows VSS in time, thereby minimizing the impact of encryption on business operations and contributing to establishing a comprehensive security protection system.

Settings for this feature are shown in the following figure.



Relevant parameters are described as follows:

- **Enable ransomware honeypot**: This option takes effect only when **Realtime File Protection** is enabled.
- **Action**: **Alert - Fix Manually** is recommended. When ransomware is detected on an endpoint, an alert will be displayed in the lower right corner of the screen.



Enable ransomware backup: This option is available only when the ransomware honeypot is enabled.

You can select **Remove and quarantine the encrypted files** to specify it as the action to take when ransomware is detected. If you uncheck the box, no action will be taken for the encrypted files.

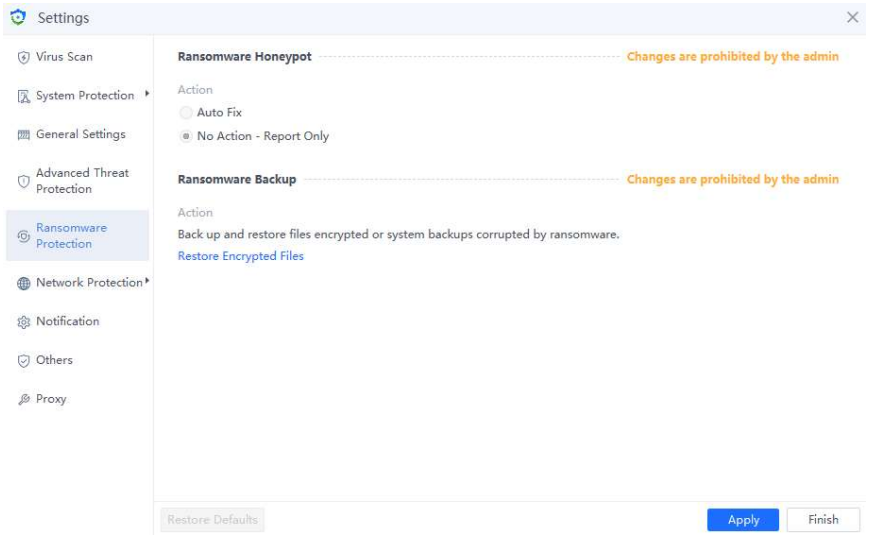
You can select **Enable password authentication for "encrypted file restoration"**.

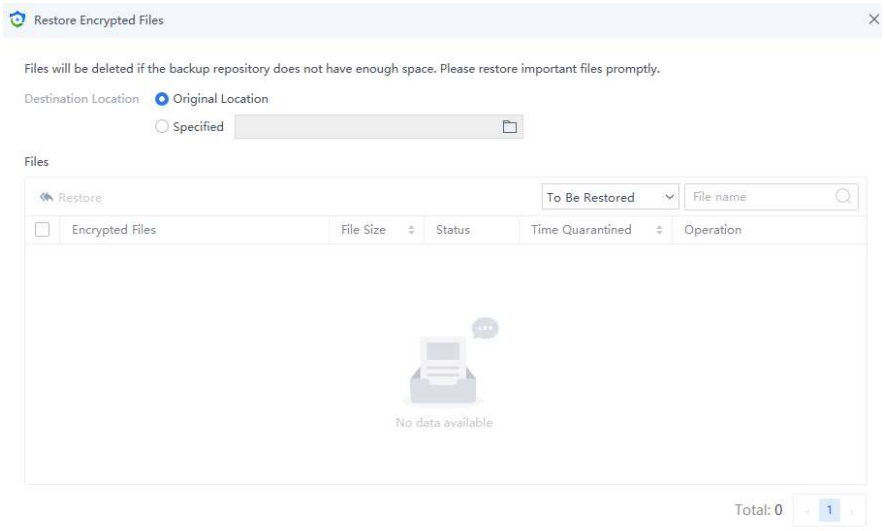
You can configure the following settings of the **Backup Repository**:

a) **Single file size limit**: Enter an integer from 1 to 100. The default size limit is 50 MB.

b) **Total backup size limit**: Enter an integer in the range of 1,000 to 10,000. The default size limit is 2,000 MB.

Endpoint users can restore encrypted files on the NovaGuard agent.





NOTE

Ransomware honeypot and backup are available for endpoints running on Windows PCs and Windows Server, and snapshot-based ransomware recovery is available for endpoints running on versions later than Windows Server 2003.

RDP Secondary Authentication

An RDP or SSH brute-force login is one of the common attack vectors, and it is recommended that this feature be enabled.

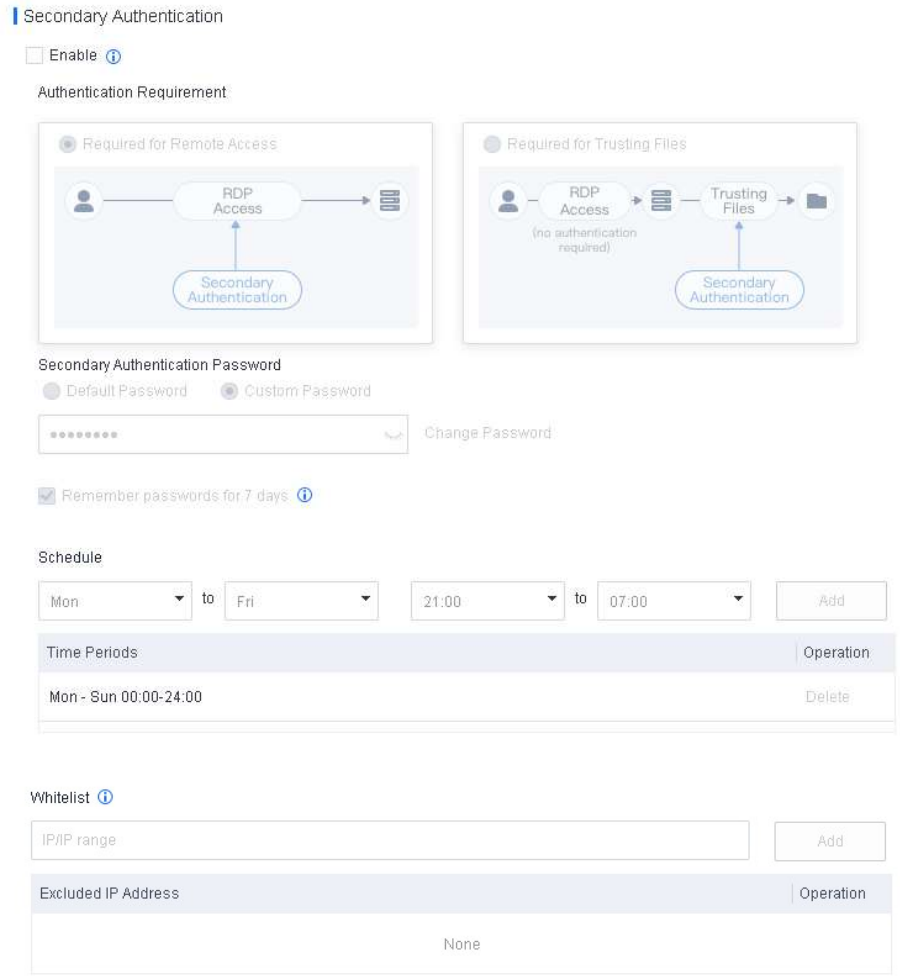
NOTE

This feature is available for Windows Server and Linux endpoints.

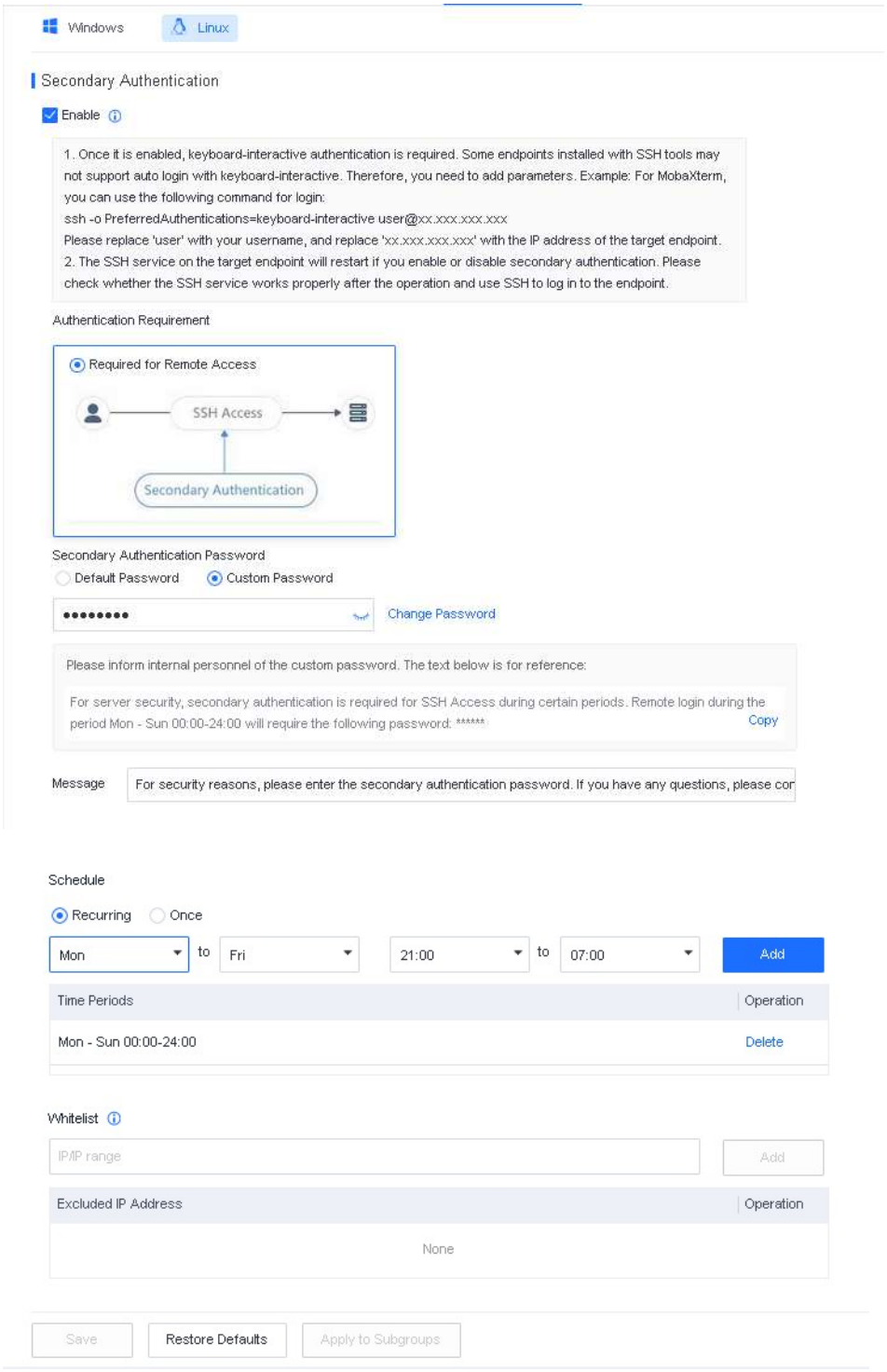
Secondary Authentication

To prevent hackers from accessing a server via RDP and quickly obtaining server permissions, you can enable secondary authentication for RDP access.

Settings for Windows endpoints are shown in the following figure.

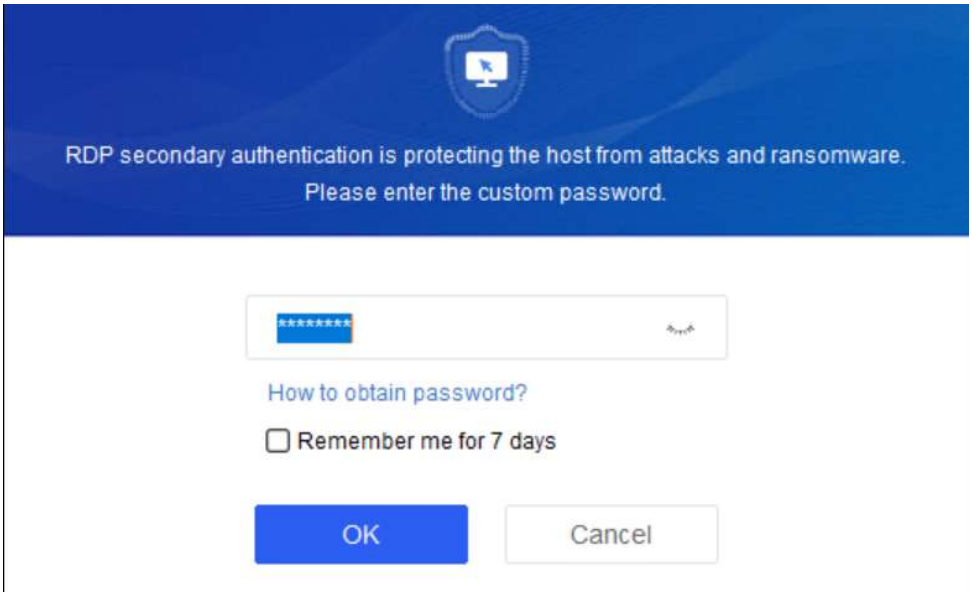


Settings for Linux endpoints are shown in the following figure.



Suppose secondary authentication for RDP access is enabled, and a hacker successfully accesses a server via RDP access. In that case, NovaGuard will lock

the screen to protect the server, as shown in the following figure.

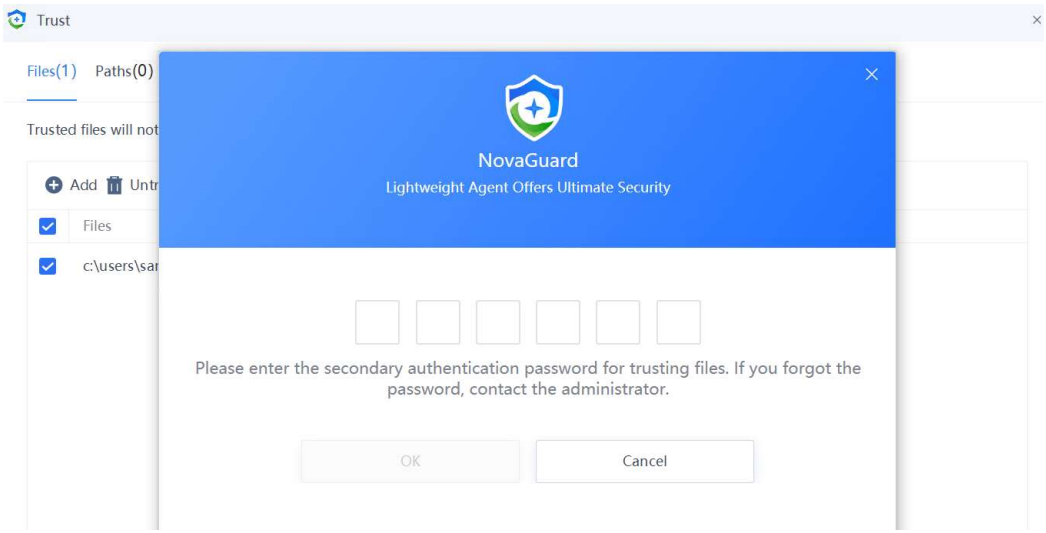


The hacker can obtain server permissions only after completing the secondary authentication process. It effectively ensures server security. It is recommended to enable secondary authentication.

Secondary Authentication for Trusting Files

To prevent hackers from infiltrating the NovaGuard trust list with malicious files and planting ransomware, you can enable secondary authentication for **trusting files**.

When a hacker successfully logs in to a server protected by NovaGuard and attempts to plant ransomware, the ransomware execution will fail as the file is not trusted. Nevertheless, if the hacker manages to include the ransomware in the trust list, the hacker can launch ransomware attacks successfully. If secondary authentication for trusting files is enabled, the hacker must complete the secondary authentication process to execute the file.



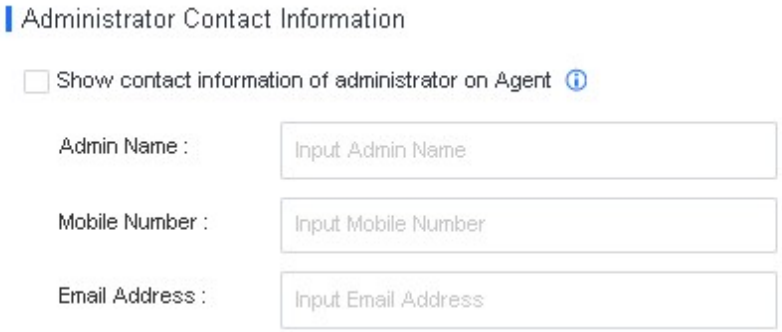
NOTE

This feature is available for Windows and Linux endpoints.

Secondary Authentication Password

1. Default Password

The default password is the last six digits of the administrator's mobile number. For instance, if the administrator's mobile number is 15258227998, the default password is 227998. To configure the administrator's contact information, go to **Policies** > **Basic Config**, as shown in the following figure.



NOTE

The default password is recommended, provided the administrator's mobile number is correctly configured. To obtain the mobile number, the server O&M administrator can check the company contact list or the NovaGuard information.

2. Custom Password

After **Custom Password** is selected and a custom password is configured, the server O&M administrator cannot access the server remotely if the administrator does not know the password. To avoid such remote access failures during critical business periods, it is recommended to inform the administrator of the custom password as soon as possible.

Schedule

You can specify the time during which RDP secondary authentication is applied. By default, secondary authentication is applied at all times.

Whitelist

RDP secondary authentication is not required for remote access to the server from IP addresses in the whitelist during critical business periods. For trusted endpoints that attempt to access the server, you can add their IP addresses to the whitelist.

Trusted Processes

This feature protects the server system or specific directories on the server. When enabled, it allows only trusted processes to run, read, and write. You can also enable RDP access protection.

4.6.1.4.1 Scenario 1: Protect the System

Protect stable systems by preventing untrusted processes (such as unknown ransomware and other viruses) from running, ensuring security.

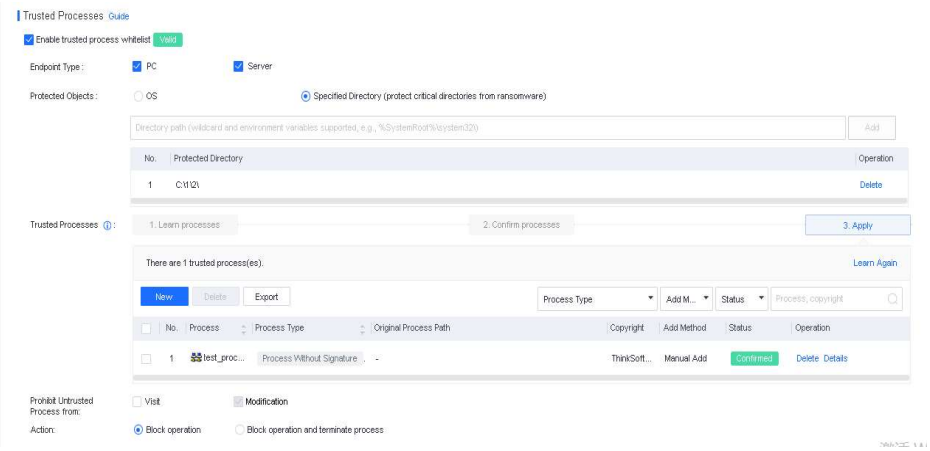
Procedure:

Step 1. Perform a virus scan.

Perform a virus scan on the endpoint to ensure the operating environment is secure.

Step 2. Enable process learning.

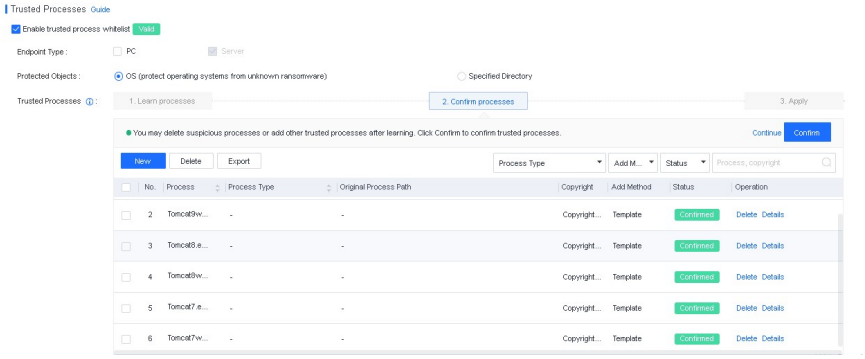
Check **Enable trusted process whitelist** and select **OS** as **Protected Objects**. Specify a time ranging from 1 day to 30 days for process learning and click **Save**, as shown in the following figure.



After the learning is complete, you can check the learned processes on this page and review the status of each process, including whether a process is flagged as suspicious or lacks a digital signature. This information can be a reference for confirming trusted processes in the next step.

Step 3. Confirm trusted processes.

After the learning, you need to confirm trusted processes. By analyzing the results of process learning, you can remove untrusted processes and add trusted processes that were not learned, as shown below.

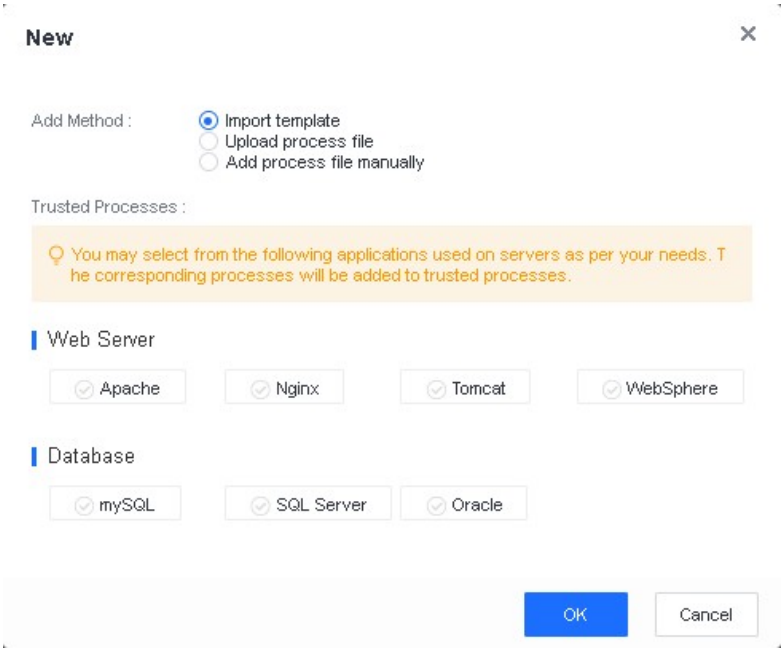


- **Process Type:** NovaGuard identifies a process as a suspicious or system process.
- **Original Process Path:** The path where the process file was initially reported.
- **Add Method:** The method for adding the process, including **Learning**, **Manual Add**, and **Template**.

- **Status:** The current status of the process. **Unconfirmed** means the process has not been confirmed as trusted.
- **Operation:** You can delete, view process details, or analyze the process.

Note:

1. If you find a trusted process not in the learning results, click **New** to add it. The page for adding a process is shown in the following figure.



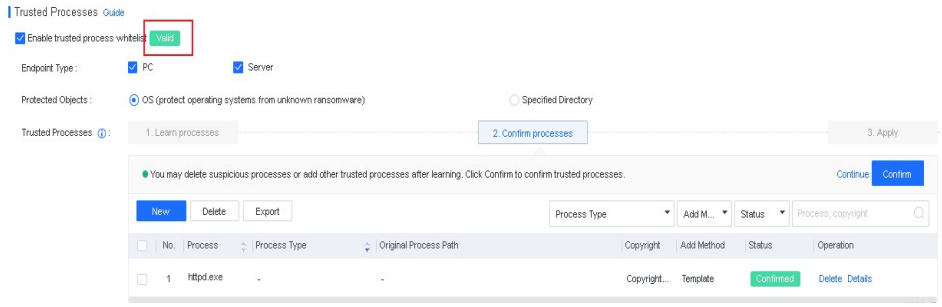
Add Method: Three methods are available for adding a process: **Import template**, **Upload process file**, and **Add process file manually**.

- **Import template:** Applicable to scenarios where the endpoint that needs to be strengthened are the web servers or database servers provided in the template.
- **Upload process file:** Upload a trusted process file to the endpoint.
- **Add process file manually:** Collect the process name, original file name, and copyright of the trusted process, then manually enter the information.

After confirming the information, click **OK** to complete the setting.

Step 4. Apply trusted processes.

Click **Save**. You can find that endpoint protection is in effect, showing **Valid**.



4.6.1.4.2 Scenario 2: Protect the Specified Directories

Protect critical endpoint directories and files from unauthorized access and modification.

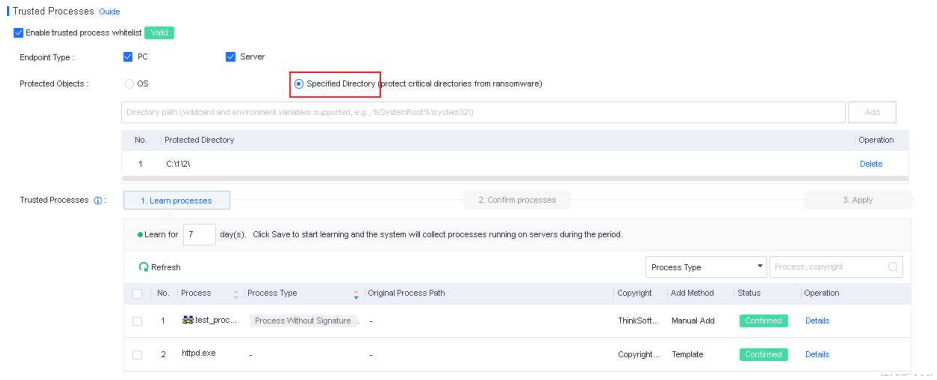
Procedure:

Step 1. Perform an endpoint virus scan.

Perform a virus scan on the endpoint to ensure the operating environment is secure.

Step 2. Add directories.

Check **Enable trusted process whitelist** and select **Specified Directory** as **Protected Objects**. Manually add critical directories of the endpoint. Directories with a wildcard (*) or an environment variable are supported.



Step 3. Enable process learning and confirm trusted processes.

For details about the configurations, see **Chapter 3.5.1.4 Scenario 1: Protect the server system** for references.

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



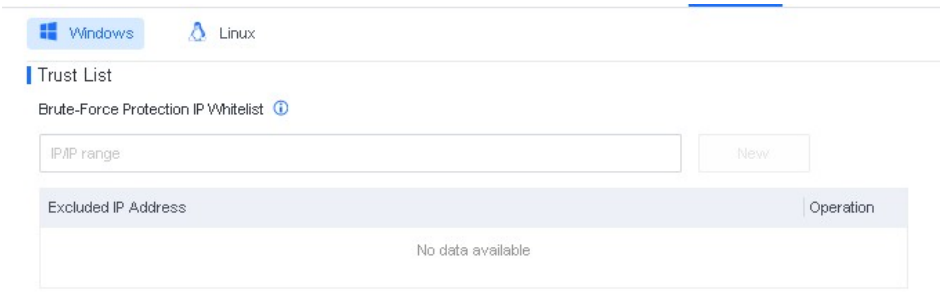
- **Prohibit Untrusted Process from:** Untrusted processes cannot delete or modify protected directories. You can specify whether their access to protected directories is allowed.
- **Action:** You can specify whether to block process operations or block process operations and terminate an untrusted process when the untrusted process performs operations on protected directories.

4.6.1.5 Trust List

This policy covers the **Brute-Force Protection IP Whitelist** and **PowerShell Parameter Whitelist**.

Brute-Force Protection IP Whitelist

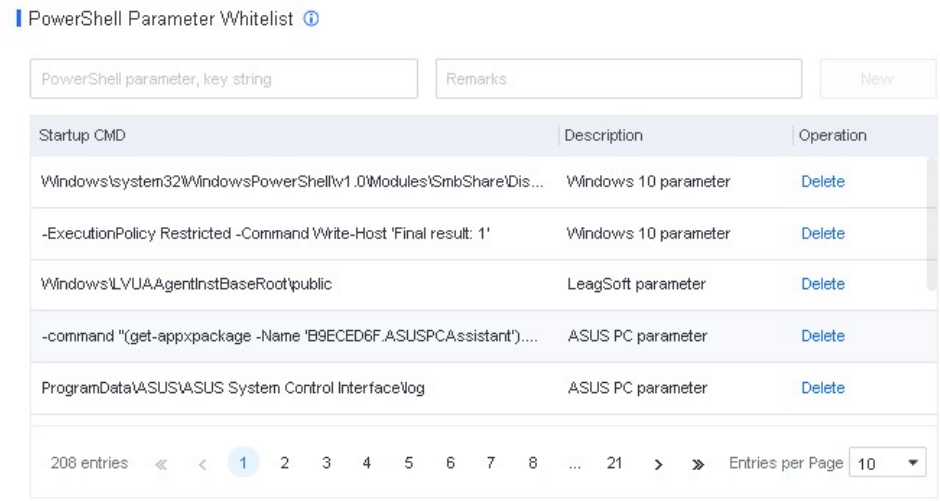
Source IP addresses for brute-force attacks can be added to the whitelist on Windows or Linux endpoints. When false positive brute-force attacks are detected, you can add the source IP addresses to the whitelist. Then, IP addresses in the whitelist are allowed without triggering an alert.



You can specify IP addresses, IP address ranges, or subnets for the **Brute-Force Protection IP Whitelist**. When false positive brute-force attacks are detected, you can add the source IP addresses to this whitelist. Then, IP addresses in the whitelist are allowed without triggering an alert.

PowerShell Parameter Whitelist

When O&M scripts written with PowerShell commands are detected, it is important to add the corresponding PowerShell parameters to the whitelist, as shown in the following figure.



It ensures that false positives do not affect business operations.

Whitelist PowerShell parameters: When detected, PowerShell parameters listed in the whitelist are allowed to run. Partial string match is supported. For instance, the parameter powershell **-ExecutionPolicy Restricted -Command Write-Host 'Final result:1'** can be matched by full name or keywords, such as **Command Write-Host 'Final result:1'**.

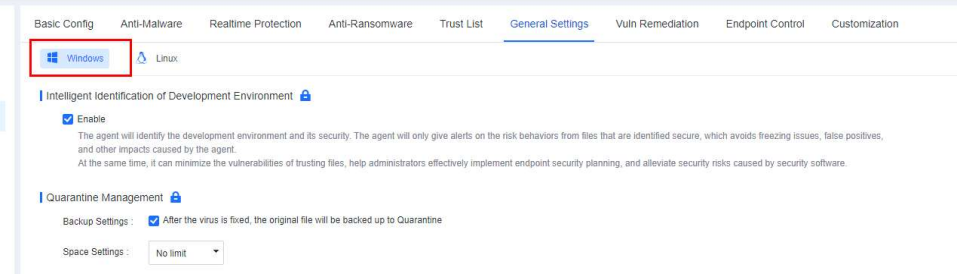
NOTE

It is recommended to enter parameters longer than 10 characters to avoid protection being bypassed by attackers.

4.6.1.6 General Settings

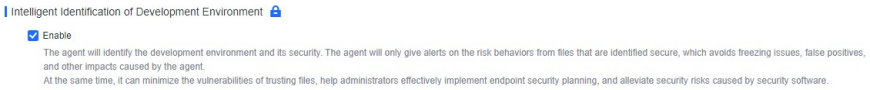
On this tab, you can configure general settings for the following aspects: **Intelligent Identification of Development Environment**, **Quarantine**

Management, **Agent Bypass**, and **Agent Performance Protection**.

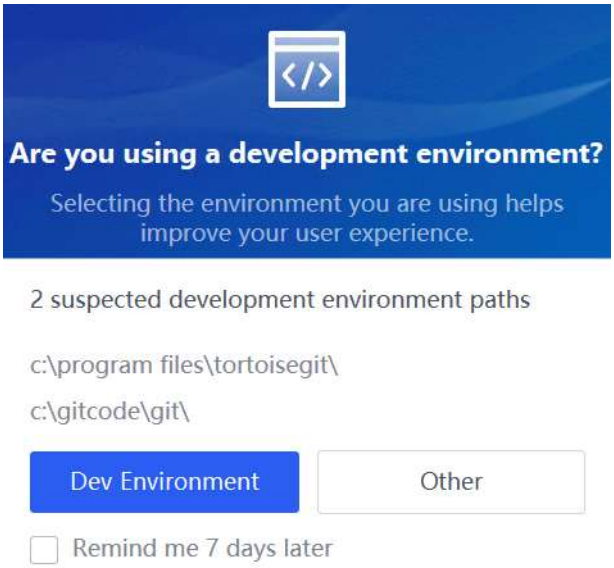


1. Intelligent Identification of Development Environment

The development environment is important, producing numerous unsigned compiled files that antivirus software might flag as false positives. It disrupts developers' work and may even make them hesitant to install antivirus software, posing security risks. This feature intelligently identifies the development environment, reduces false positives, and keeps the development environment secure.



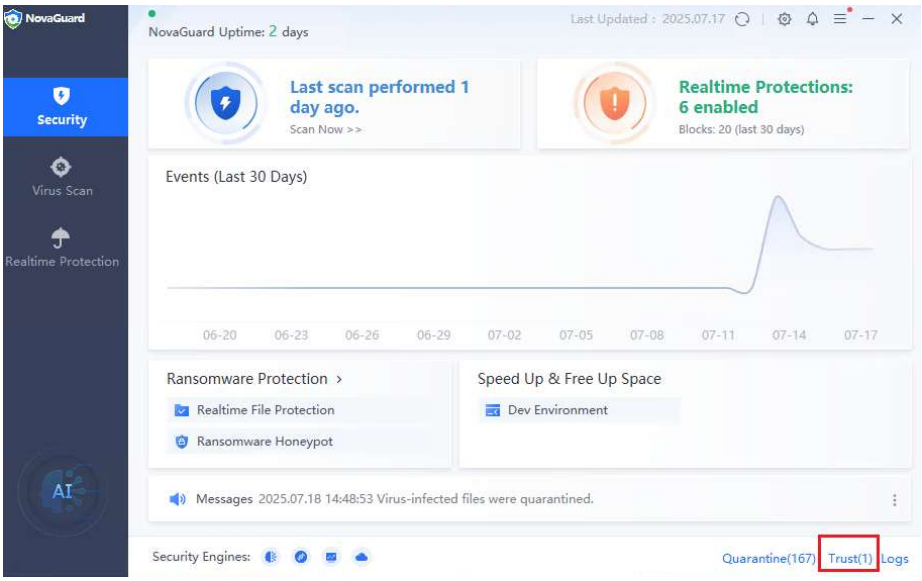
After enabling **Intelligent Identification of Development Environment**, it intelligently scans for the presence of compiling software on endpoints. A pop-up window appears when the compiler is detected, prompting endpoint users to confirm whether they are using a development environment, as shown in the following figure.

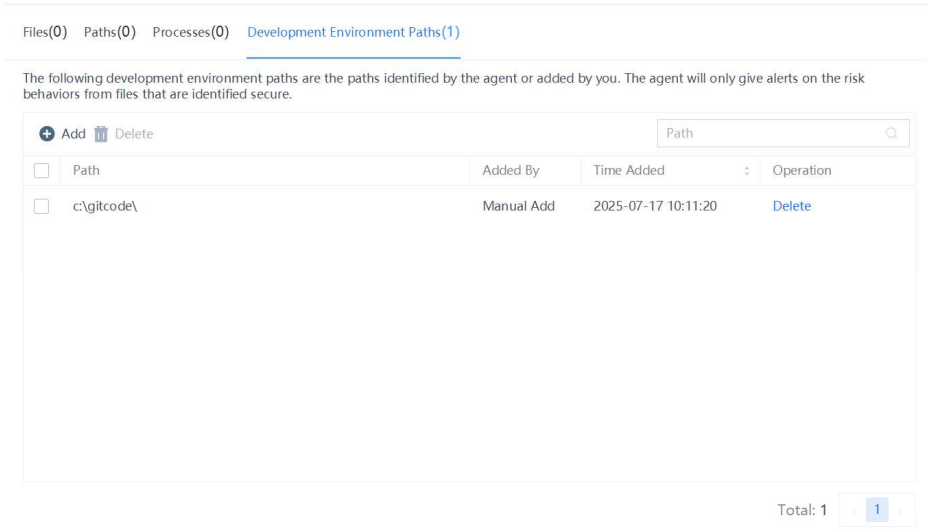


Endpoint users can select **Dev Environment** or **Other**.

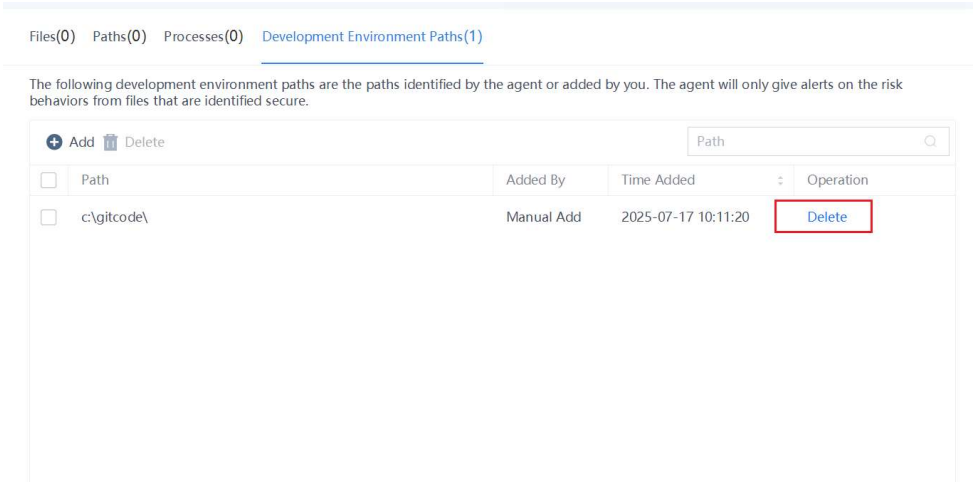
When **Other** is selected, this feature fixes threats according to the antivirus policy.

When **Dev Environment** is selected, intelligently identified paths are automatically added in **Trust** > **Development Environment Paths** on the NovaGuard agent. For compiled files generated during the execution of the compiling software, NovaGuard only reports them without fixing them or giving alerts, as shown in the following figure.

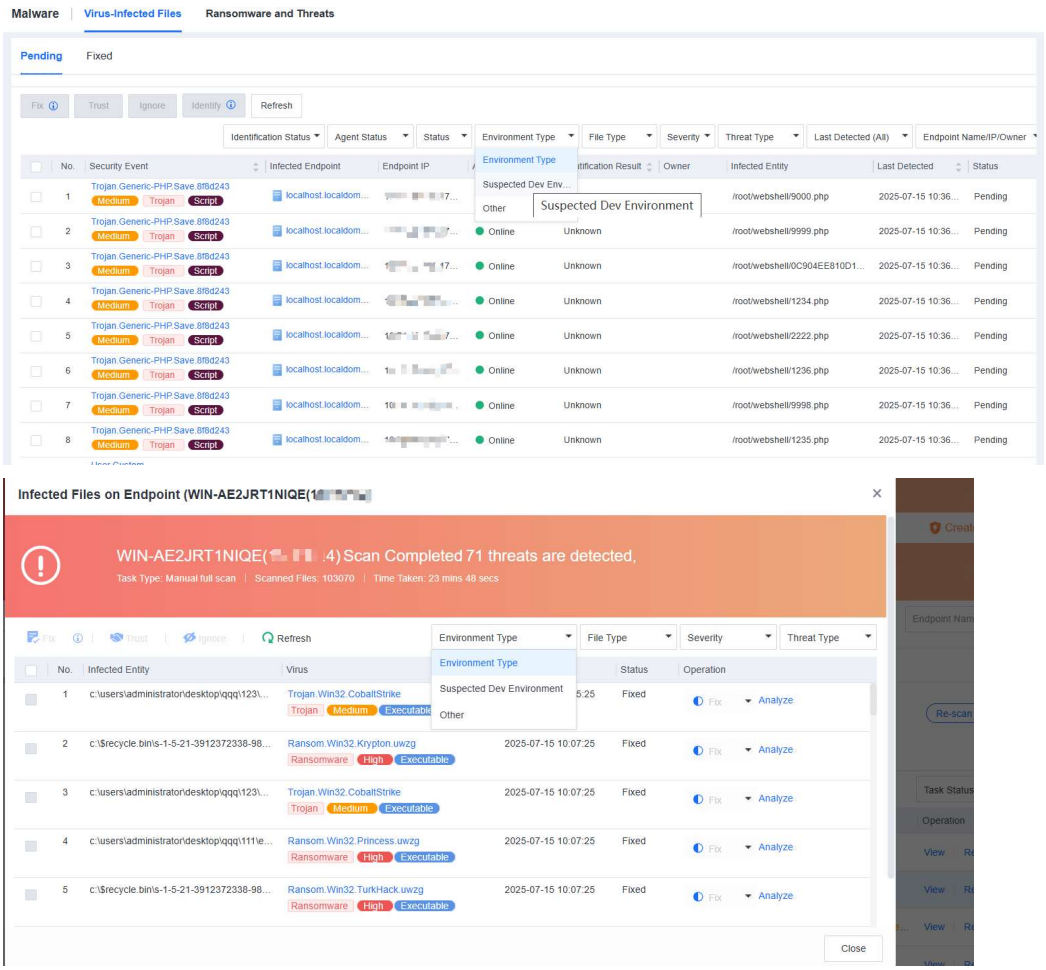




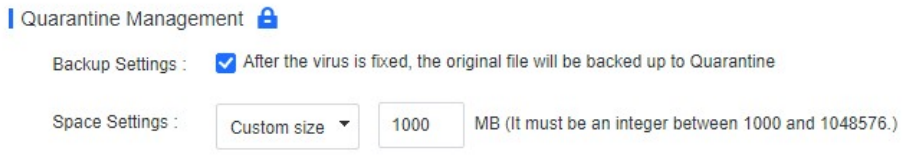
Endpoint users can manually add or delete a development environment path, as shown in the following figure.



For an intelligently identified path, a **Suspected Development Environment** tag is shown on the **Defense > Malware Scan** > **Virus List** page and the **Defense > Malware Scan** >**Tasks** page. When you handle viruses on the NovaGuard manager as an administrator, you can select **Suspected Development** Environment as the **Environment Type** to avoid false positives.



2. Quarantine Management



Backup Settings: If this feature is enabled, the original file will be backed up to Quarantine after the virus is fixed.

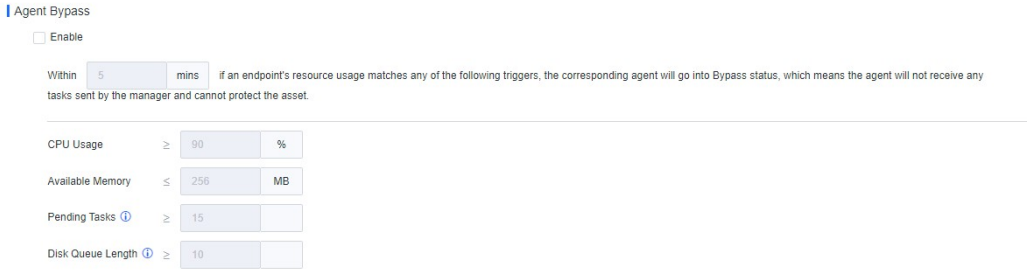
Space Settings: Configure the size of the Quarantine area on an endpoint or set it as **No limit**.

NOTE

Quarantine management is not available for macOS endpoints.

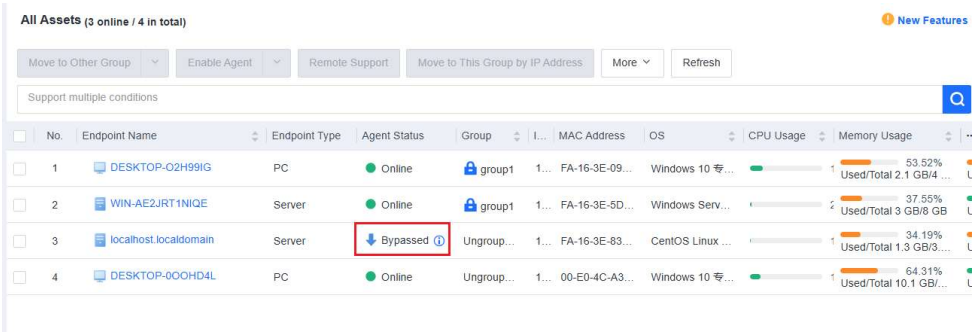
3. Agent Bypass

Agent bypass is available for endpoints running on Windows Server and Linux.



Agent bypass refers to the policy applicable to scenarios where the NovaGuard agent actively monitors resources on an endpoint. Suppose the average usage of any resources (CPU, memory, or load) on the endpoint reaches or exceeds the threshold within a specified period. In that case, the NovaGuard agent automatically enters the Bypass state to release occupied resources, preventing disruptions to business operations from resource contention. On the contrary, suppose the average usage of any resource (CPU, memory, or load) on the endpoint remains below the set threshold. In that case, the endpoint is automatically restored to its normal state.

In the Bypass state, the NovaGuard agent releases occupied resources, the agent will not receive any tasks sent by the manager, and the agent cannot protect the asset.

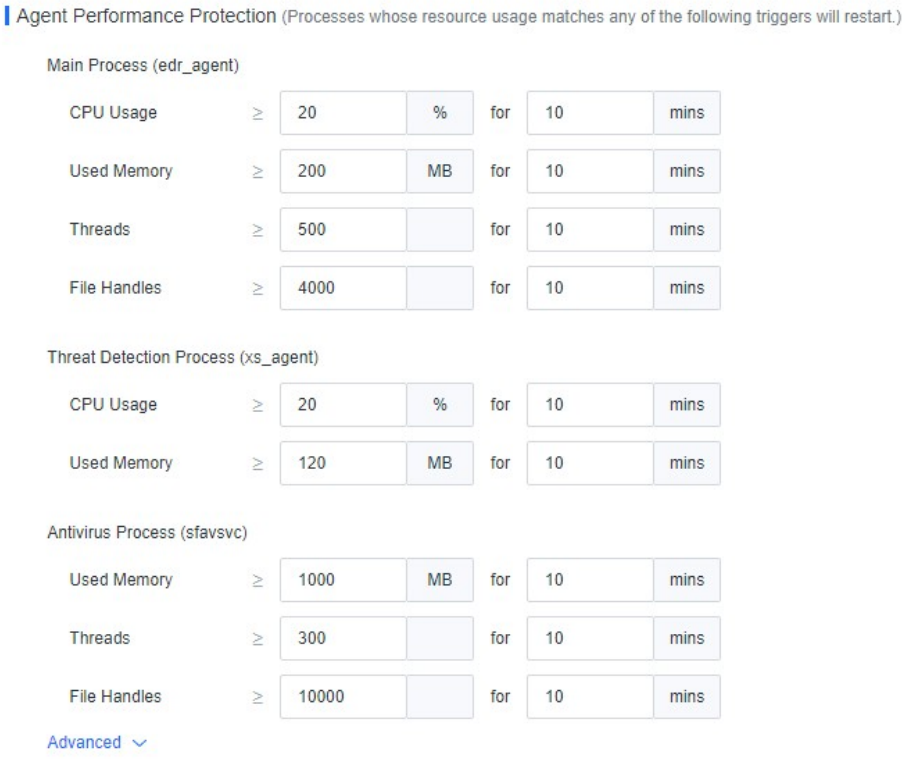


NOTE

Agent bypass is available for Windows Server and Linux endpoints.

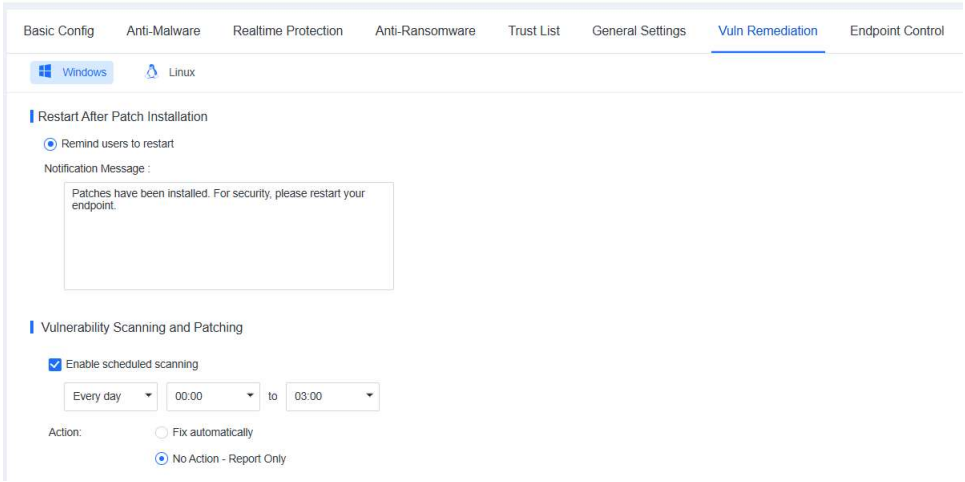
4. Agent Performance Protection

Processes whose resource usage matches any threshold will restart. It aims to constrain the resource usage of the NovaGuard agent processes to prevent them from occupying too many business resources. Thresholds for the resource usage of the processes can only be adjusted to higher values than the default values. In scenarios with adequate server resources, you can increase the thresholds for the resource usage of the NovaGuard agent, enabling faster and more comprehensive detection. This feature is available for Windows Server and Linux endpoints.



4.6.1.7 Vuln Remediation

On this tab, you can customize vulnerability scan settings for Windows and Linux systems separately. Specifically, you can configure scheduled vulnerability scan tasks for endpoints, and select whether to remind users to restart endpoints after patch installation to ensure that the installed patches take effect.



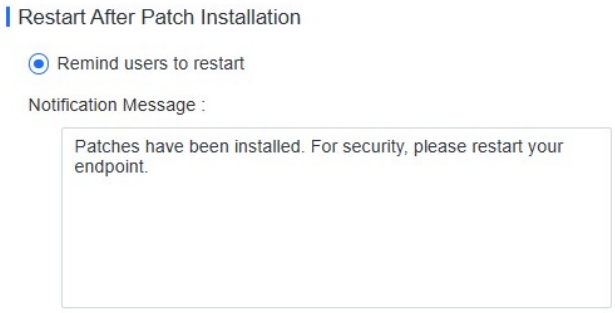
NOTE

1. Patching is available for Windows PCs and Windows Server endpoints.

2. For details about systems that support this feature, see Compatibility Support.

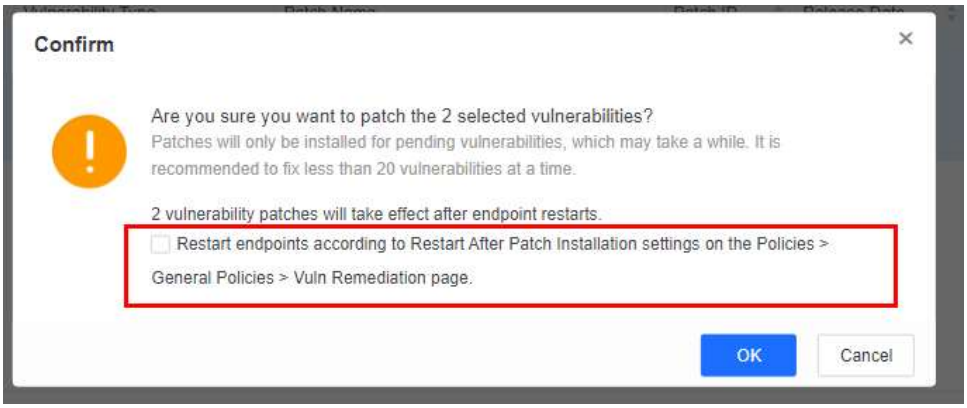
1. Restart After Patch Installation

Certain patches take effect only after the endpoint restarts. You can specify the restart policy by selecting **Remind users to restart** and customize the notification message to send after patch installation.

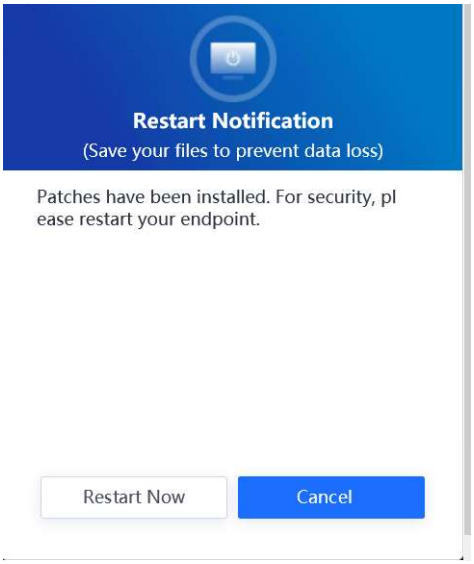


Go to **Risk Assessment** > **Windows Update** or **Risk Assessment > Vulnerabilities** to scan for and fix vulnerabilities. When it is required to restart the endpoint following patch installation, a prompt appears, as shown in the

following figure.

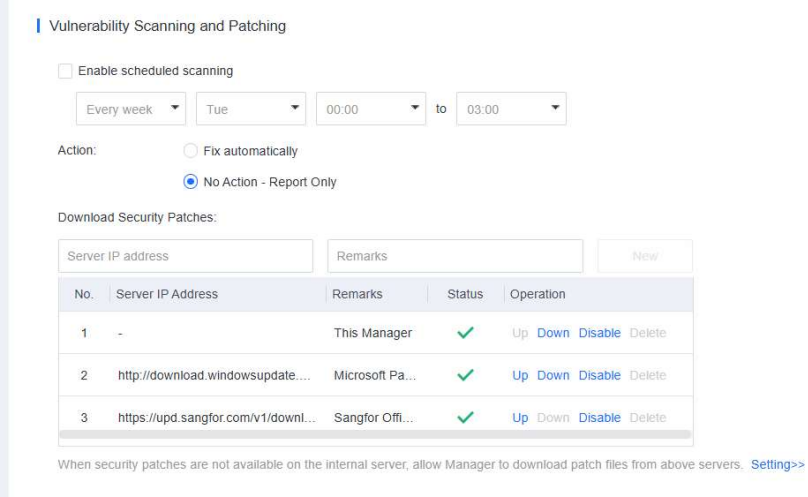


If you select this option and **Remind users to restart** is selected as the restart policy, a pop-up reminder appears on the endpoint, as shown in the following figure.



2. Vulnerability Scanning and Patching

Select **Enable scheduled scanning** to enable scan tasks to run as scheduled.



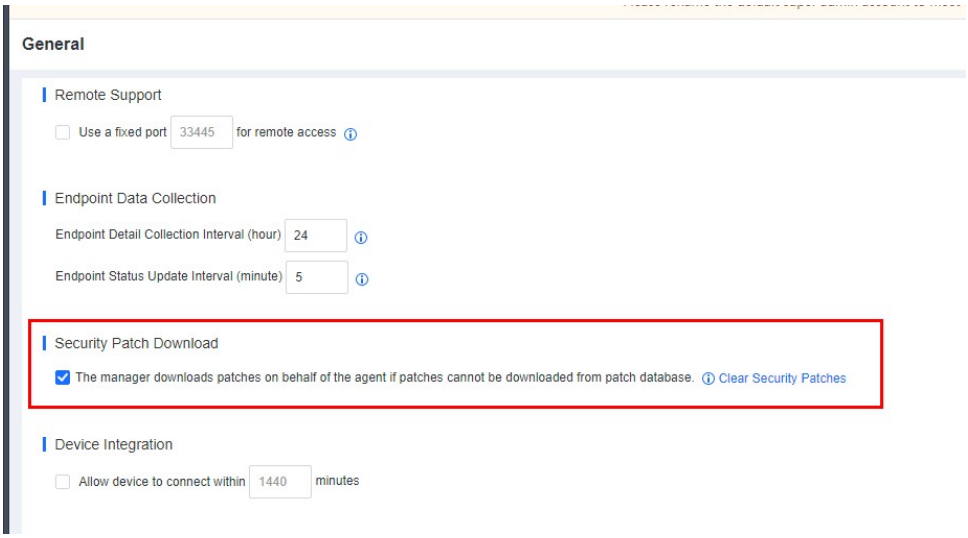
Relevant parameters are described as follows:

- **Scheduled scanning:** Specify the time for the vulnerability scan to run.
- **Action:** Specify the method for fixing vulnerabilities, including **Fix automatically** and **No Action - Report Only** (recommended).
- **Download Security Patches:** Specify the server where vulnerability patches for endpoints can be downloaded. Default options include ForeNova CDN Server, Microsoft Patch Server, and the NovaGuard manager.

Install vulnerability patches when an endpoint is offline

In cases where an endpoint does not have an Internet connection, while the NovaGuard manager is connected to the Internet, the endpoint cannot download vulnerability patches from an online server. To install vulnerability patches, go to **System** > **System** > **General**. Select **The manager downloads patches on behalf of the agent if patches cannot be downloaded from patch database** to enable the NovaGuard manager to download patches on

behalf of the NovaGuard agent, as shown in the following figure.



NOTE

If an endpoint and NovaGuard manager are not connected to the Internet, you can download vulnerability patches using offline tools. For details, see the Section 3.6.9.9 "Tools" in this document.

This feature enables you to identify and install vulnerability patches for Windows endpoints and applications and identify vulnerability patches for Linux endpoints. It does not support the automatic installation of vulnerability patches for Linux endpoints.

4.6.1.8 Endpoint Control

On this tab, you can configure the following settings: USB device control, unauthorized outbound access detection, remote support control, and cleanup. Among them, USB device control is available for both Windows and macOS endpoints, whereas other settings are available only for Windows endpoints.

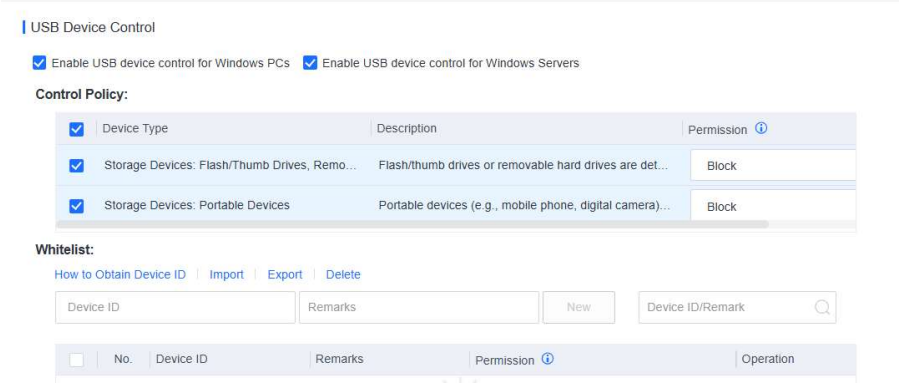
1. USB Device Control

Unauthorized access to USB storage devices can expose endpoints to various threats, such as viruses, Trojans, data leaks, and tampering. By leveraging the USB device control feature, you can deny or allow the usage of mobile devices such as USB flash drives, removable hard disks, and mobile phones.

Furthermore, you can set up notifications to alert endpoint users, mitigating the risks associated with insufficient control over mobile devices.

For Windows endpoints, go to **Policies** > **General Policies** > **Endpoint Control**, and select **Enable USB device control for Windows PCs** and **Enable USB device control for Windows Servers** under **USB Device Control** as needed.

For macOS endpoints, go to **Policies** > **General Policies** > **Endpoint Control**, and select **Enable** under **USB Device Control**.



You can set the control policy for the storage features of USB flash drives, removable hard disks, and portable devices (such as mobile phones and digital cameras).

Control policies include the following:

Block: The device and the files it contains are not visible to users.

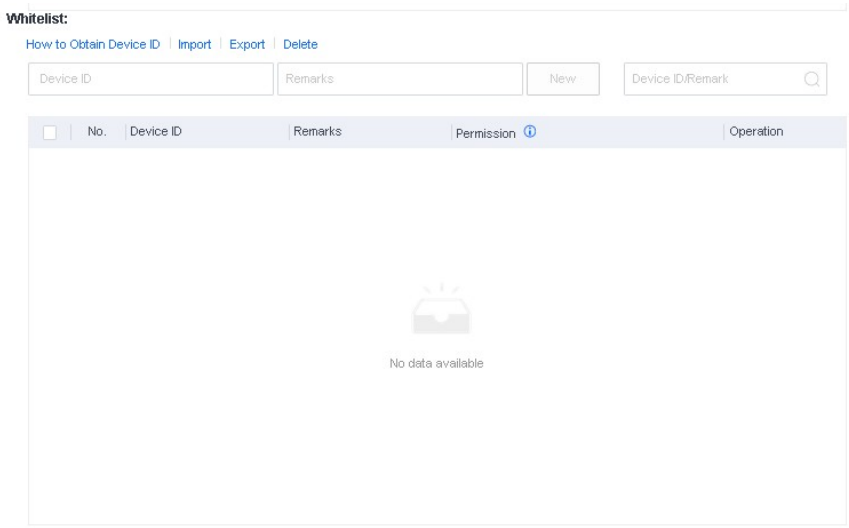
Read & Execute: Data can be read from but cannot be written to the device. The files it contains can be executed.

Read: Data can be read from but cannot be written to the device. The files it contains cannot be executed.

Full Access (With Notification): Data can be read from and written to the device. Pop-up notification will be displayed on the endpoint and related logs will be reported to the manager.

Whitelist

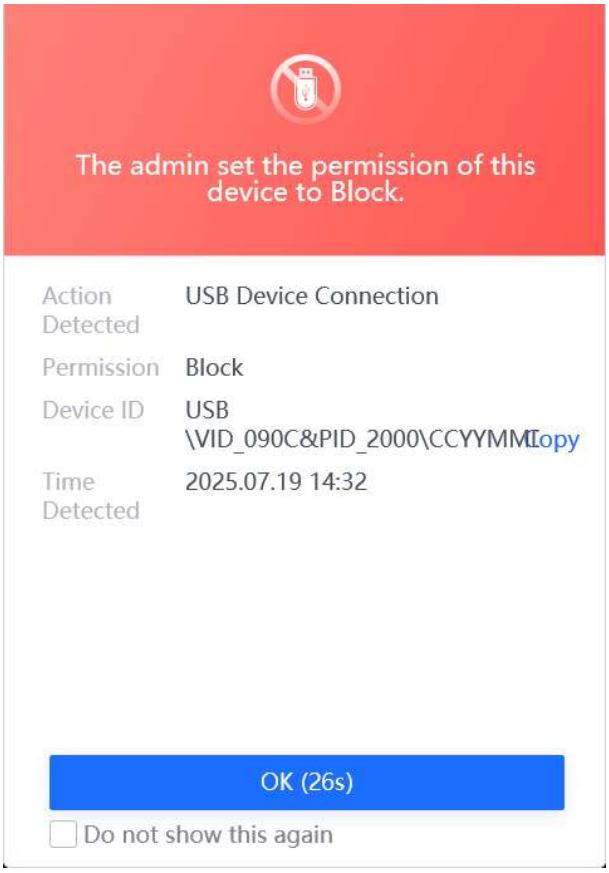
When certain USB devices are allowed, add them to the whitelist and complete the required information settings, as shown in the following figure.



You can import many devices in batches if you need to add them.

Notify

After selecting the **Notify user when a device with permissions other than Full Access is detected**, endpoint users will receive notifications when attempting to use devices blocked on servers or endpoints, as shown in the following figure.



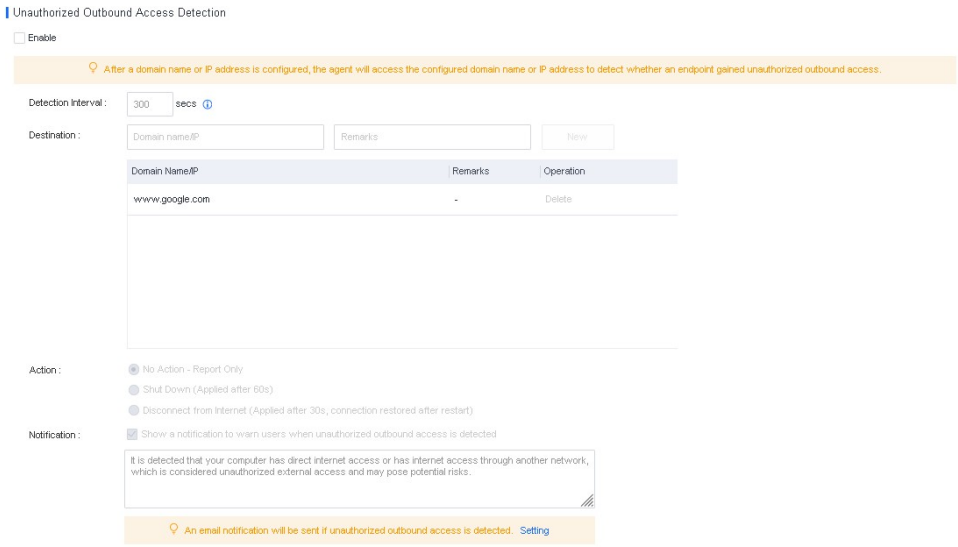
NOTE

The USB device control feature is available for Windows and macOS endpoints. You can block USB devices or set the permissions of the devices to **Read-Only** for macOS endpoints.

2. Unauthorized Outbound Access Detection

Unauthorized outbound access occurs when an endpoint in the internal network connects to an unauthorized target server. NovaGuard can detect unauthorized outbound access by utilizing the ping command and respond with actions like disconnecting the endpoint from the network, shutting down the endpoint, and notifying users if such access is identified, enabling real-time control of endpoints.

Settings for this feature are shown in the following figure.



Detection Interval: The interval for detecting unauthorized outbound access on an endpoint. You can set the detection interval to a value between 60 to 3,600 seconds.

Destination: The destination address for unauthorized outbound access is www.google.com by default. You can add IP addresses or domain names.

Action: The method for handling detected unauthorized outbound access.

- **No Action – Report Only**: Only display a notification.
- **Disconnect from Internet(Applied after 30s, connection restored after restart)**: For Windows Vista and above, the result of this action is similar to endpoint isolation because the endpoint can only communicate with the NovaGuard manager. As an administrator, you can restart the NovaGuard agent on the Endpoint page to restore the Internet connection. For Windows Server 2003 and Windows XP, this action disables the NIC, and the endpoint user must manually enable the NIC or restart the endpoint.
- **Shut Down**: The endpoint will shut down after a 60-second countdown.

Notification: When unauthorized outbound access is detected on an endpoint, a notification appears in the lower right corner of the screen to warn the endpoint user. You can specify the content of the notification in the **Notification** text box.

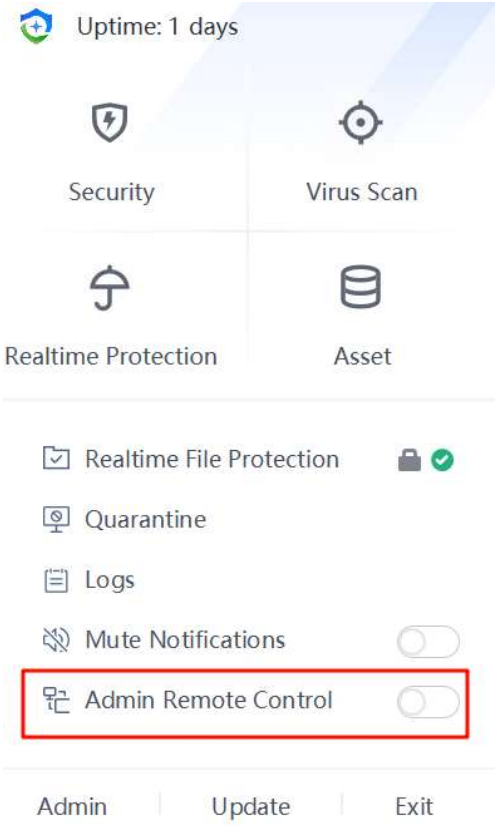
Email notification: When unauthorized outbound access is detected on an endpoint, you can receive an email notification as an administrator.

3. Remote Support Control

When an exception occurs on a managed endpoint, you can remotely control the endpoint as an administrator to help solve the exception quickly and safely.

Prerequisites

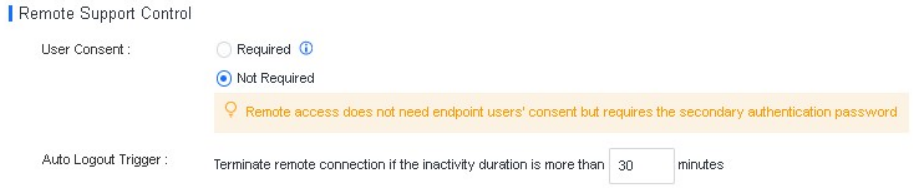
You can remotely control an endpoint if the endpoint user has enabled **Admin Remote Control** on the NovaGuard agent. To set this feature, right-click the tray icon of the NovaGuard agent on the endpoint, as shown in the following figure. This feature is enabled by default.



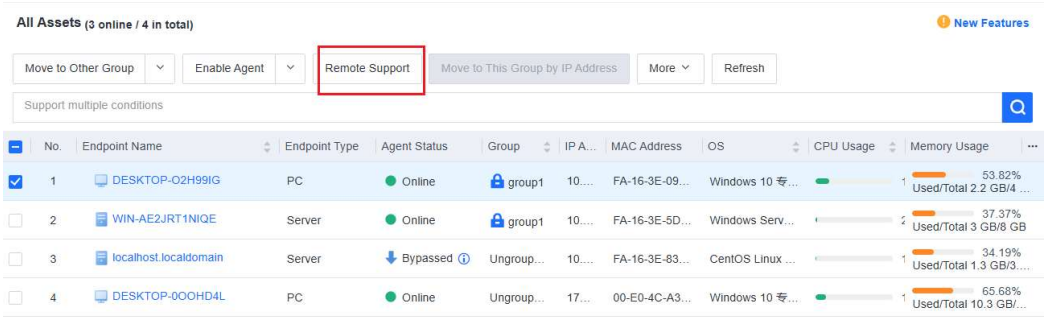
Scenario 1: Remote control of an endpoint without user consent

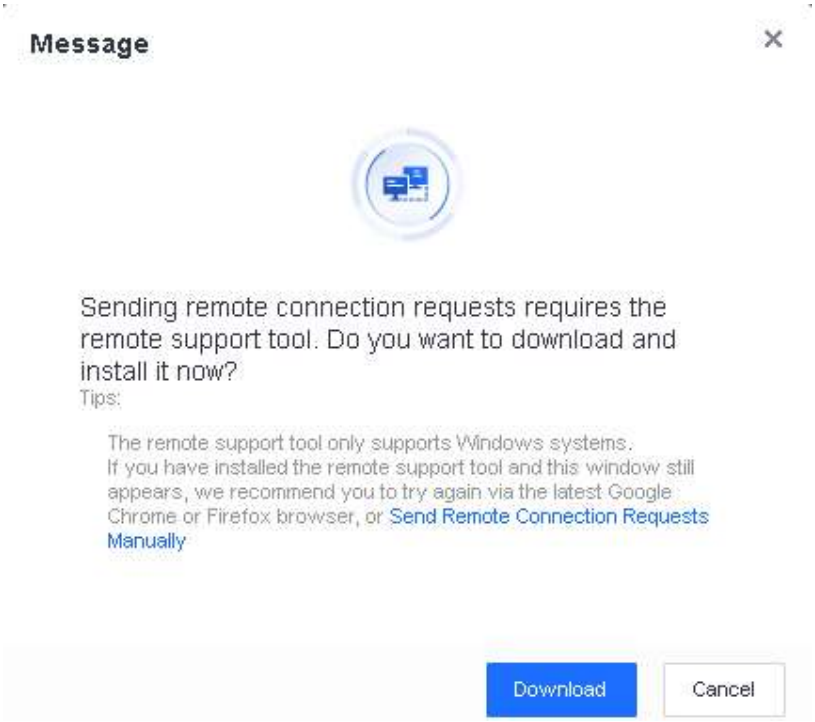
You can remotely control an endpoint without user consent. This configuration applies to an unattended scenario:

Go to **Policies** > **General Policies** > **Endpoint Control** and select **Not Required** for **User Consent** in the **Remote Support Control** section, as shown in the following figure.

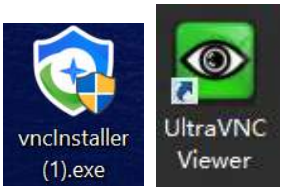


Go to **Endpoint** > **Endpoint Groups**, select the endpoint you want to control, and click **Remote Support**, as shown in the following figure.

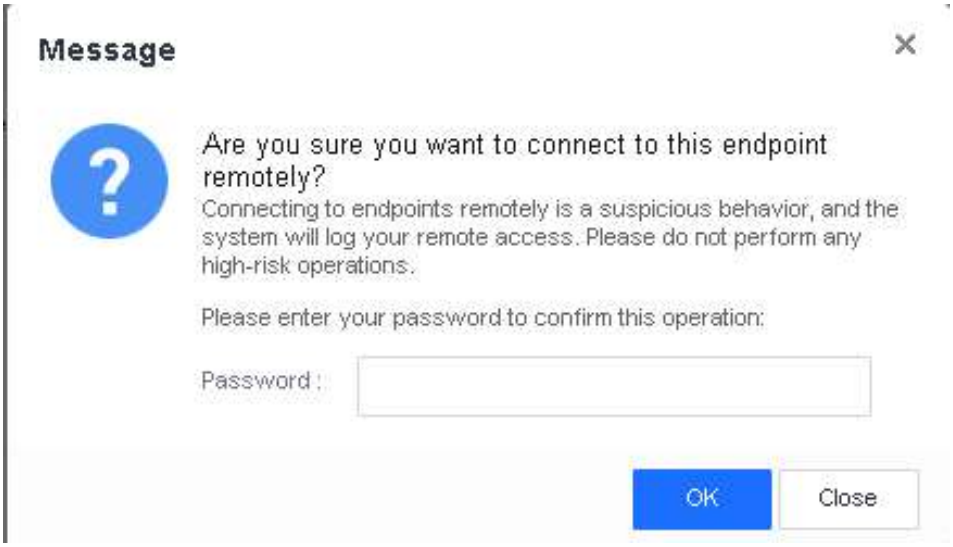




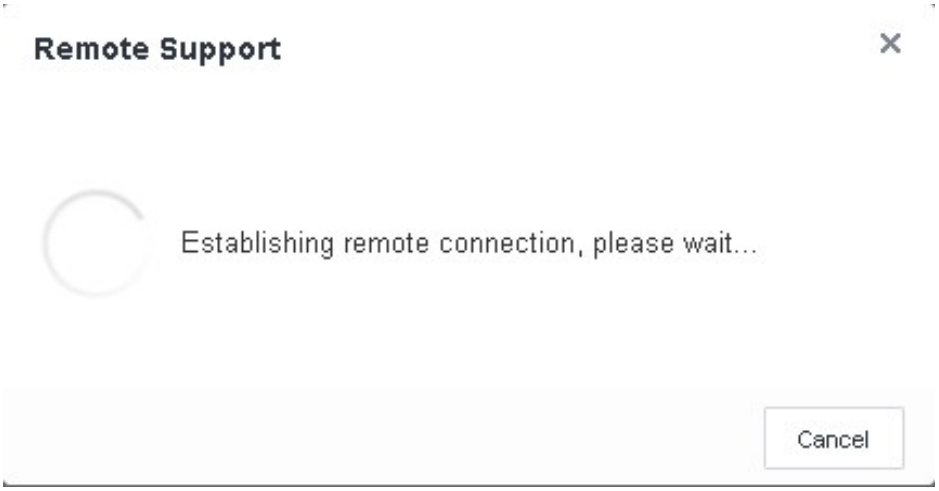
When you initiate the remote control for the first time, a message indicates that you need to download UltraVNC Viewer(the remote control tool). Click **Download** to download and install the tool, as shown in the following figure.

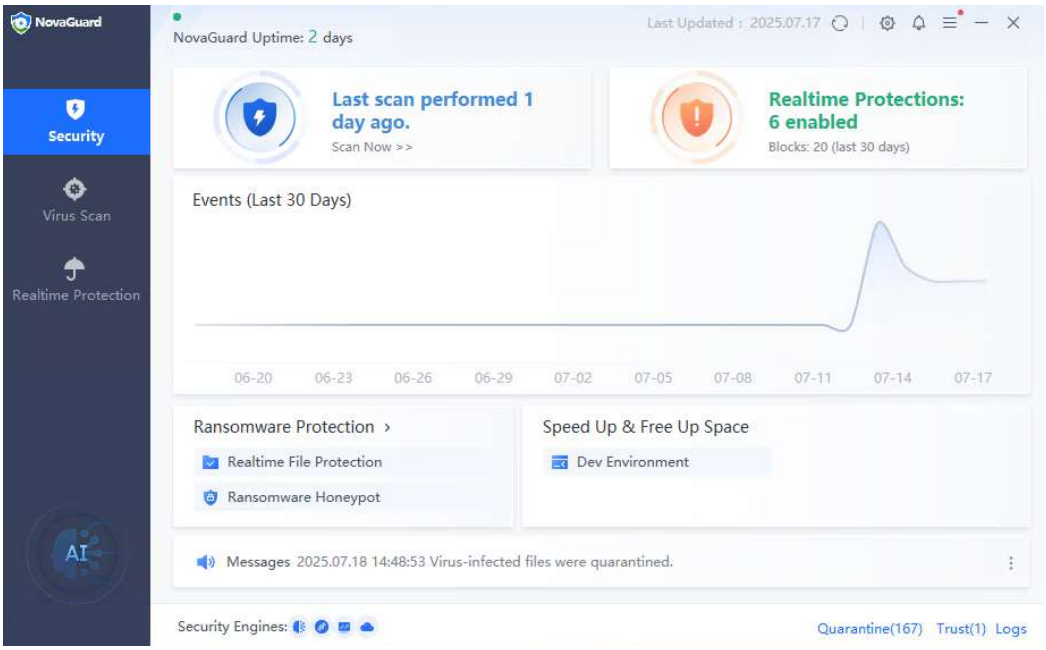


After you install UltraVNC Viewer, initiate remote control again. A message box appears, as shown in the following figure.



To confirm that you are an administrator, you need to enter the password of your administrator account and click **OK** to establish a remote connection to the endpoint, as shown in the following figure.

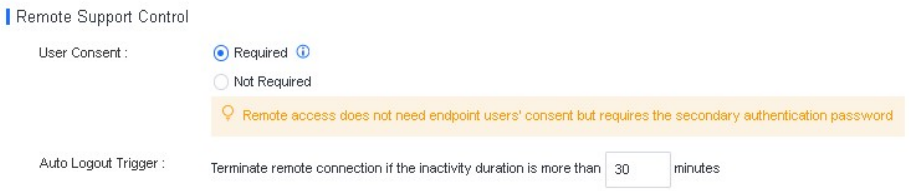




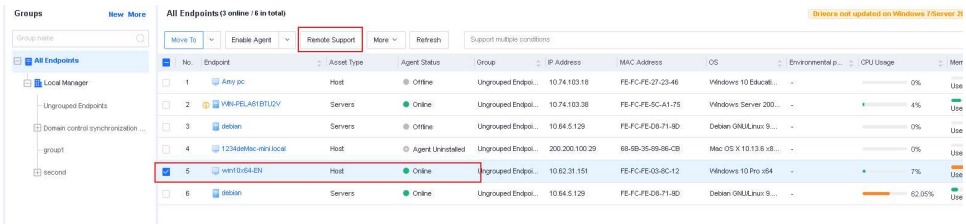
Scenario 2: Remote control of an endpoint with user consent

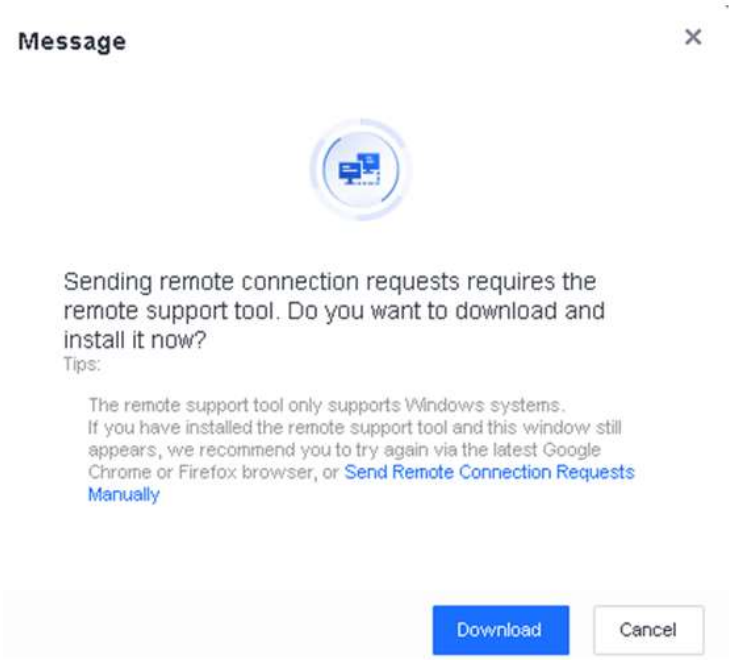
You can also specify that user consent is required to control an endpoint remotely. This configuration applies to a constantly attended endpoint sensitive to remote operations:

Go to **Policies** > **General Policies** > **Endpoint Control** and select **Required** for **User Consent** in the **Remote Support Control** section, as shown in the following figure.

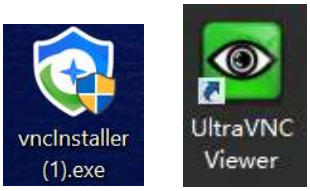


Go to **Endpoint** > **Endpoint Groups**, select the endpoint you want to control, and click **Remote Support**, as shown in the following figure.

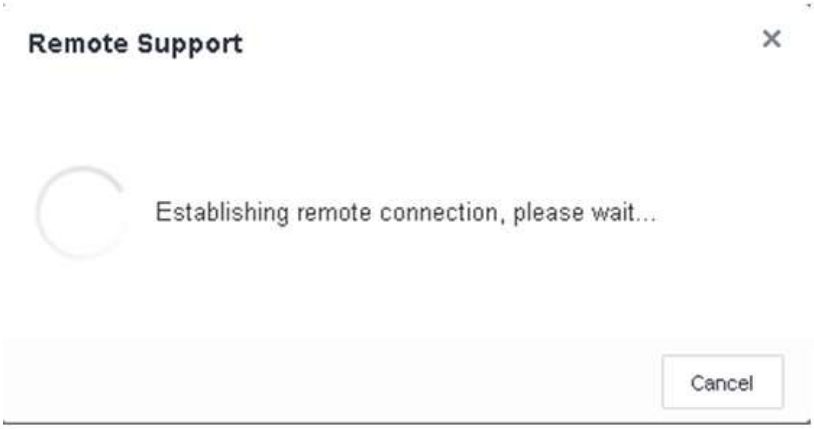




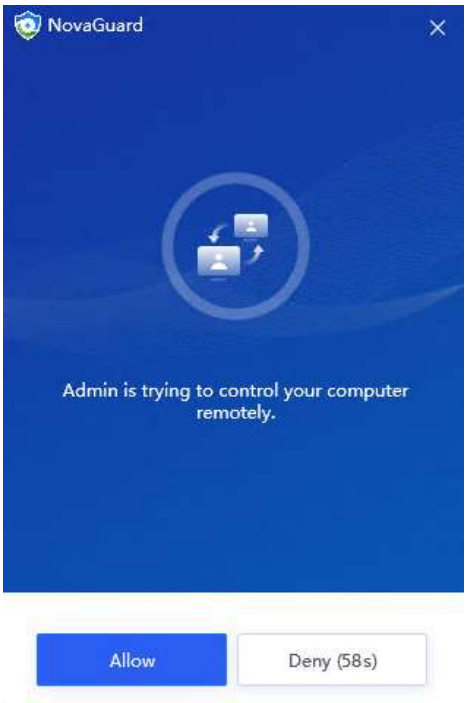
When you initiate the remote control for the first time, a message indicates that you need to download UltraVNC Viewer(the remote control tool). Click **Download** to download and install the tool, as shown in the following figure.



After you install UltraVNC Viewer, initiate remote control again. A message appears, as shown in the following figure.

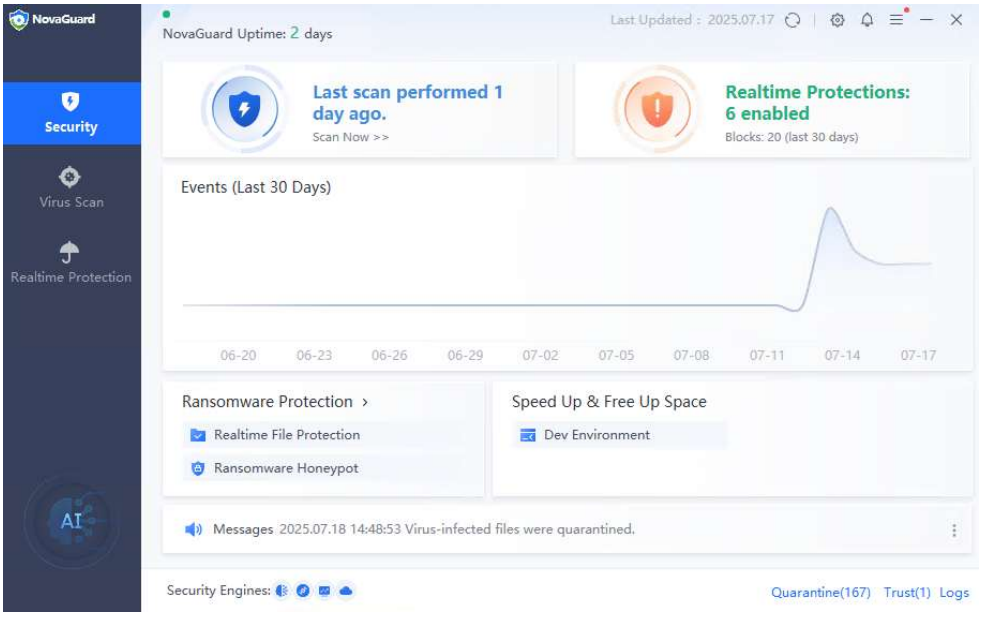


An NovaGuard agent notification will be shown on the endpoint.



Once the endpoint user clicks **Allow**, you can remotely control the endpoint.

To confirm that you are an administrator, you need to enter the password of your administrator account and click **OK** to establish a remote connection to the endpoint, as shown in the following figure.



NOTE

1. Only the Super administrator and security administrator have remote control permissions. The communication is fully encrypted.

2. By default, a random port is used for the remote control of an endpoint. You can go to **System** > **System** > **General** and specify the port for remote control in the **Remote Support** section.

3. Remote control is supported by endpoints running on Windows XP, Windows 7, Windows 8, Windows 8.1, Windows 10, or Windows 11.

---

4. Cleanup

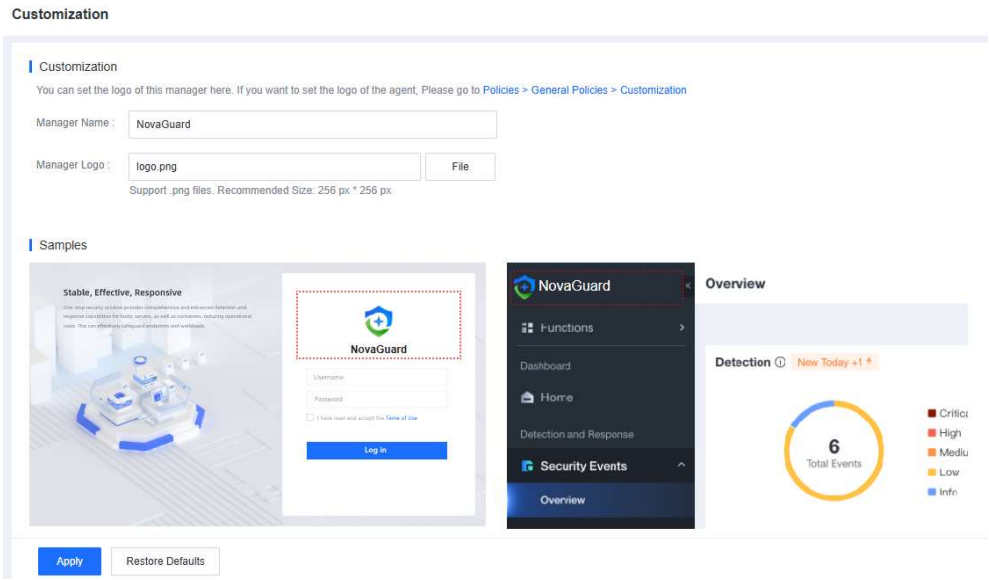
You can enable this feature to free up the storage space to improve the endpoint system performance.

4.6.1.9 Customization

On this tab, you can customize the brand name and logo as needed.

Customize the NovaGuard manager

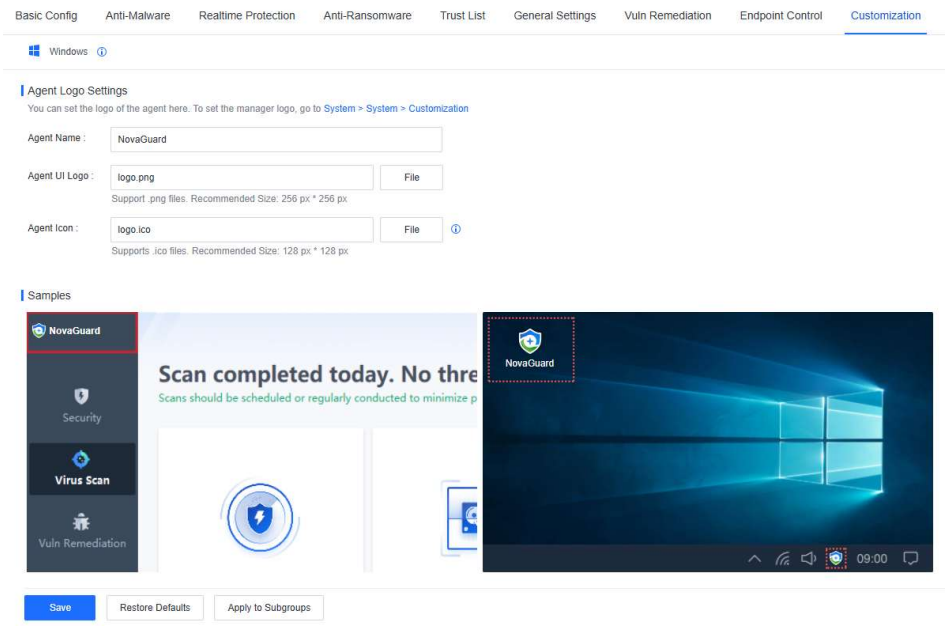
To change the name and logo for the NovaGuard manager, go to **System** > **System** > **Customization**, as shown in the following figure.



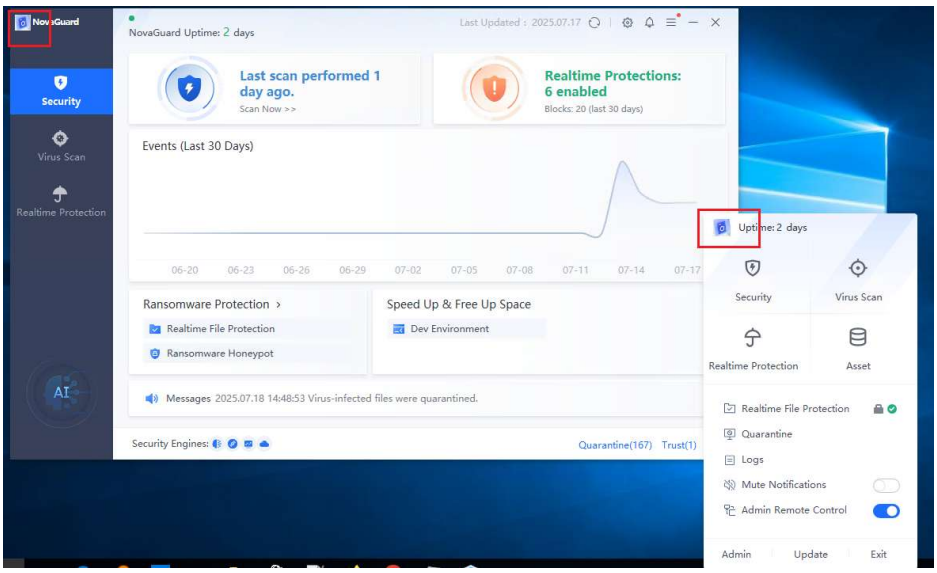
On the **Customization** page, change the **Manager Name** and upload a **Manager logo** image.

Customize the NovaGuard agent

To change the name and logo for the NovaGuard agent, go to **Policies** > **Customization**, as shown in the following figure.



On the **Customization** page, change the **Agent Name, UI Logo,** and **Agent icon.** The following figure shows a sample.

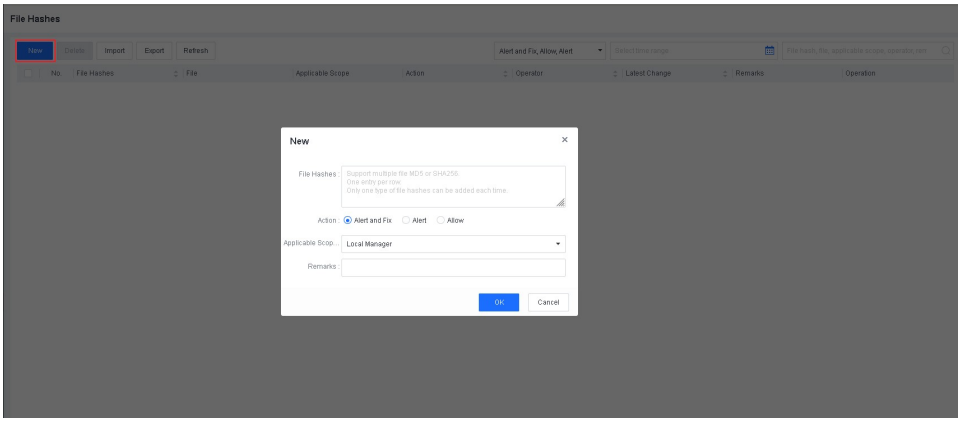


4.6.2 Detection Policies

4.6.2.1 File Hashes

Indicators enable you to quickly respond to false positive and false negative security events and improve O&M efficiency based on **File Hashes**.

Go to **Policies** > **Detection Policies** > **File Hashes**, as shown in the following figure.



You can set the action to take for specified files. Supported actions are **Alert and Fix**, **Alert**, and **Allow**.

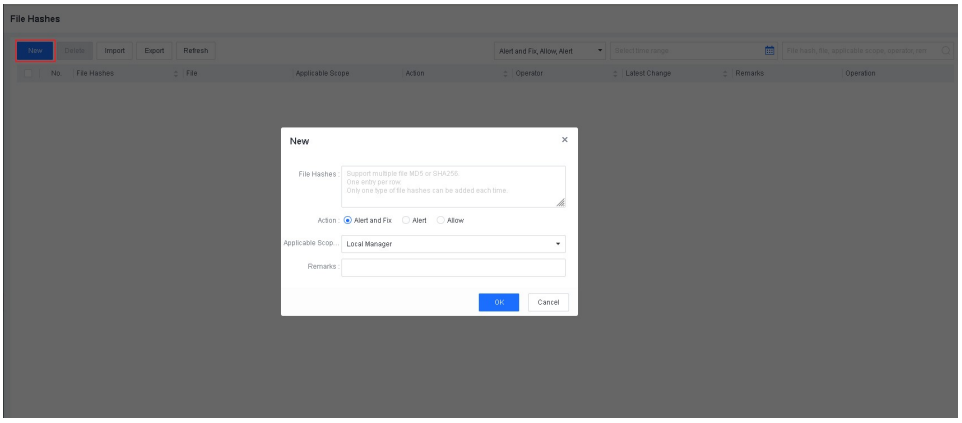
Alert and Fix: A false negative threat will be fixed and an alert will be given for the threat.

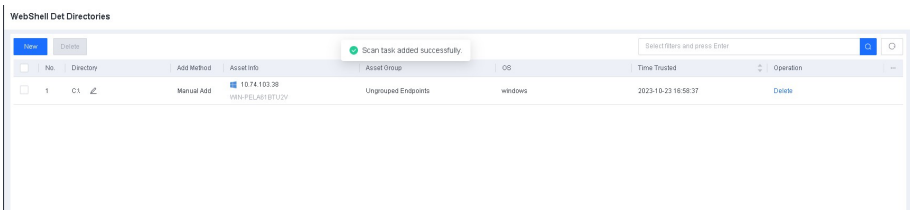
Alert: Only an alert is given for the threat.

Allow: A false positive threat is allowed.

4.6.2.2 WebShell Directories

You can specify the web servers' web directories to detect web shells.



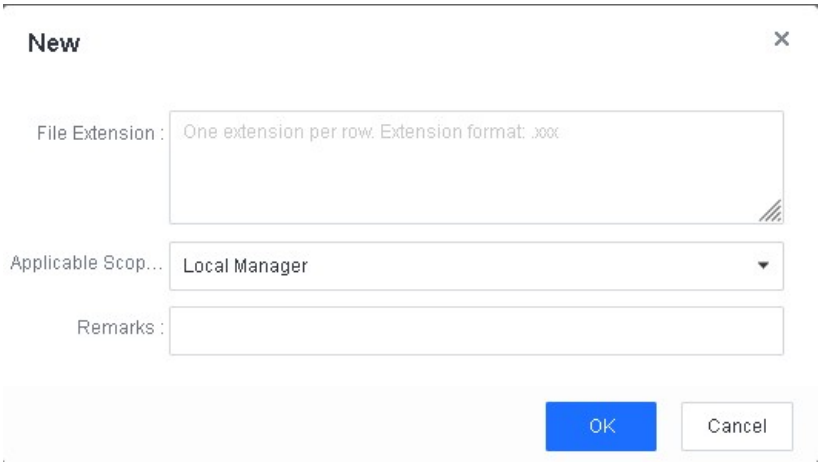


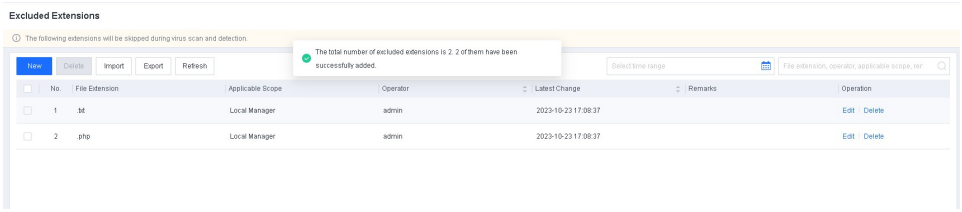
4.6.3 Exclusions

When you find a false positive security event, you can exclude it by file name, file path, or file extension. Excluded files and directories will not be checked in virus scanning, real-time monitoring, or web shell detection.

4.6.3.1 Excluded Extensions

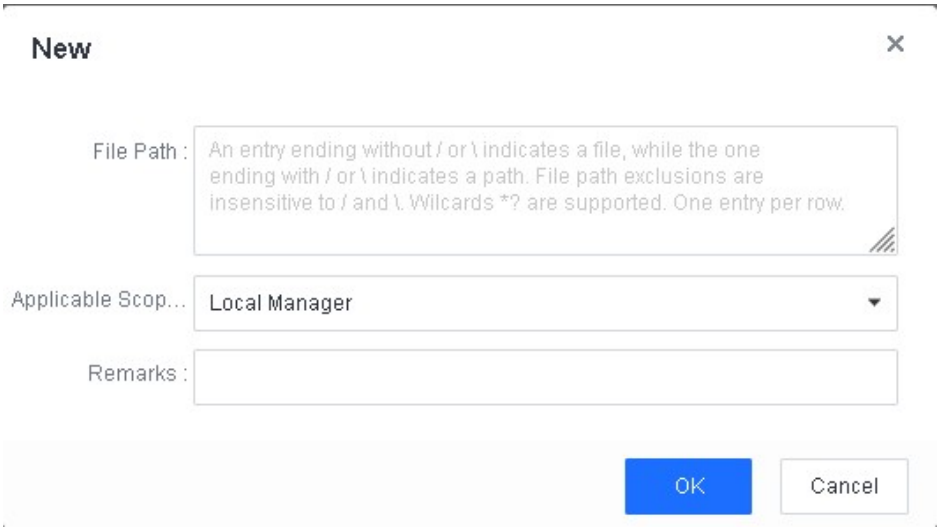
The virus detection module does not scan or detect files with the specified extensions.





4.6.3.2 Excluded Paths

The virus detection module does not scan or detect files in the specified excluded paths.



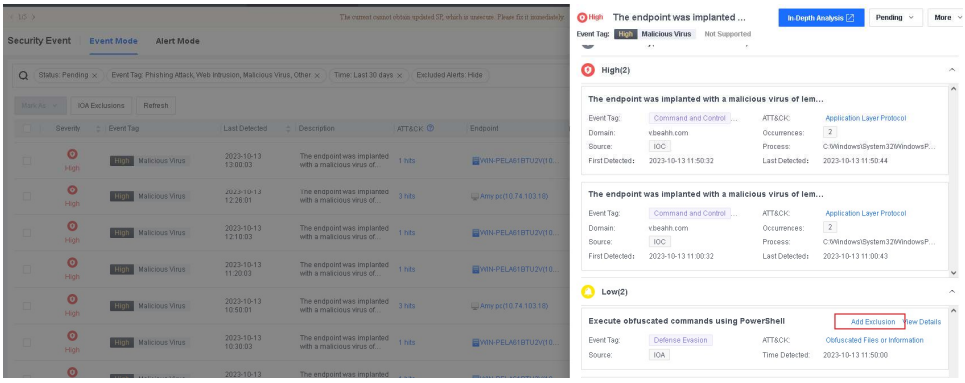


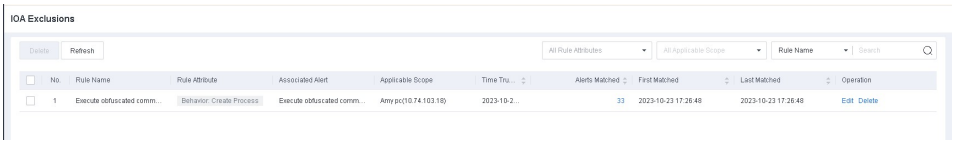
File exclusion: To exclude a file, specify the path to the file. The path string ends with the file name rather than a backslash (\), for example, D:\2022\10 tools\test.

Directory exclusion: To exclude a directory, specify the path to the directory. The path string ends with the directory name and a backslash (\), for example, D:\2022\10 tools\test\.

4.6.3.3 Excluded IOAs

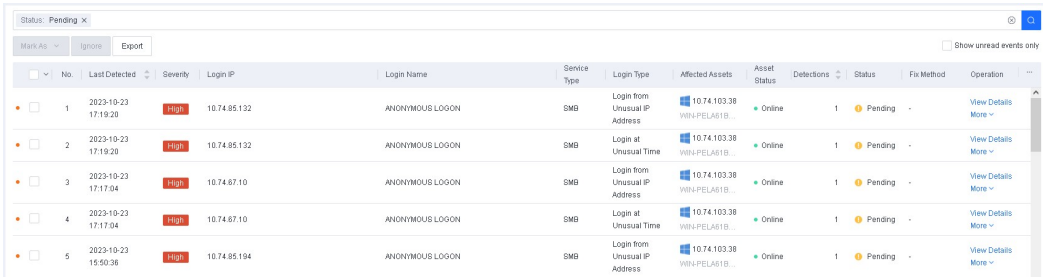
When the IOA engine detects an advanced threat event, you can add it to IOA Exclusions. You can also edit or delete an exclusion rule.

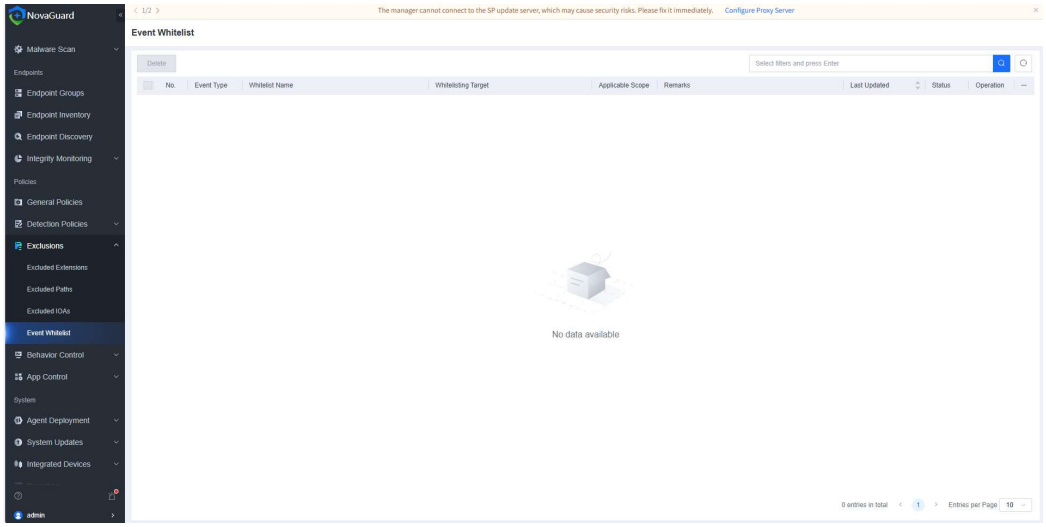




4.6.3.4 Event Whitelists

You can add security events identified in intrusion detection, such as brute-force attacks, suspicious scans, application vulnerabilities, and memory backdoors, to the event whitelist.



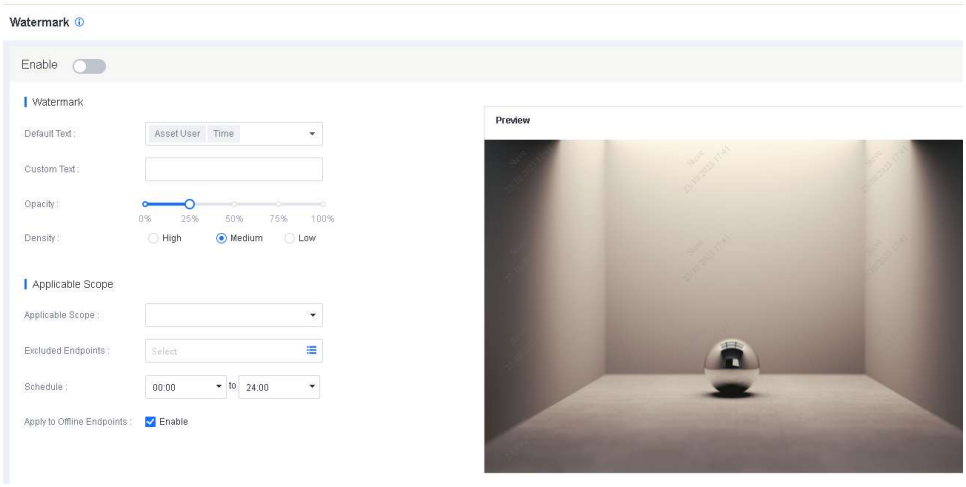


4.6.4 Behavior Control

4.6.4.1 Watermark

The watermark feature prevents information leakage. You can specify the watermark text to trace the source based on the screenshots.

To configure watermark settings, go to **Policies** > **Behavior Control** > **Watermark**, as shown in the following figure.



Watermark: Select one or more default text options or specify custom text for the watermark and set its opacity and density.

Applicable Scope: Specify the endpoints on which the watermark is displayed, the period when the watermark takes effect, and whether to apply the watermark to offline endpoints.

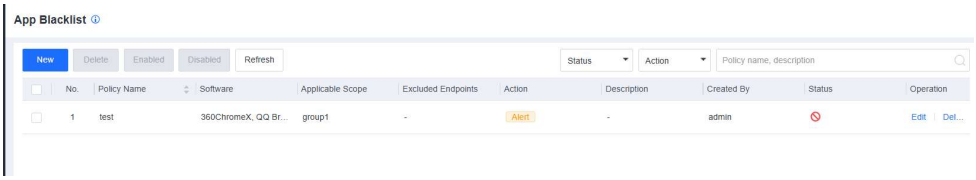
After you set a watermark parameter, you can view the result in real time in the **Preview** section on the right.

4.6.5 App Control

Application control helps you manage the use of software on an endpoint based on built-in and custom rules. You can prevent blacklisted software from running and record software operation logs.

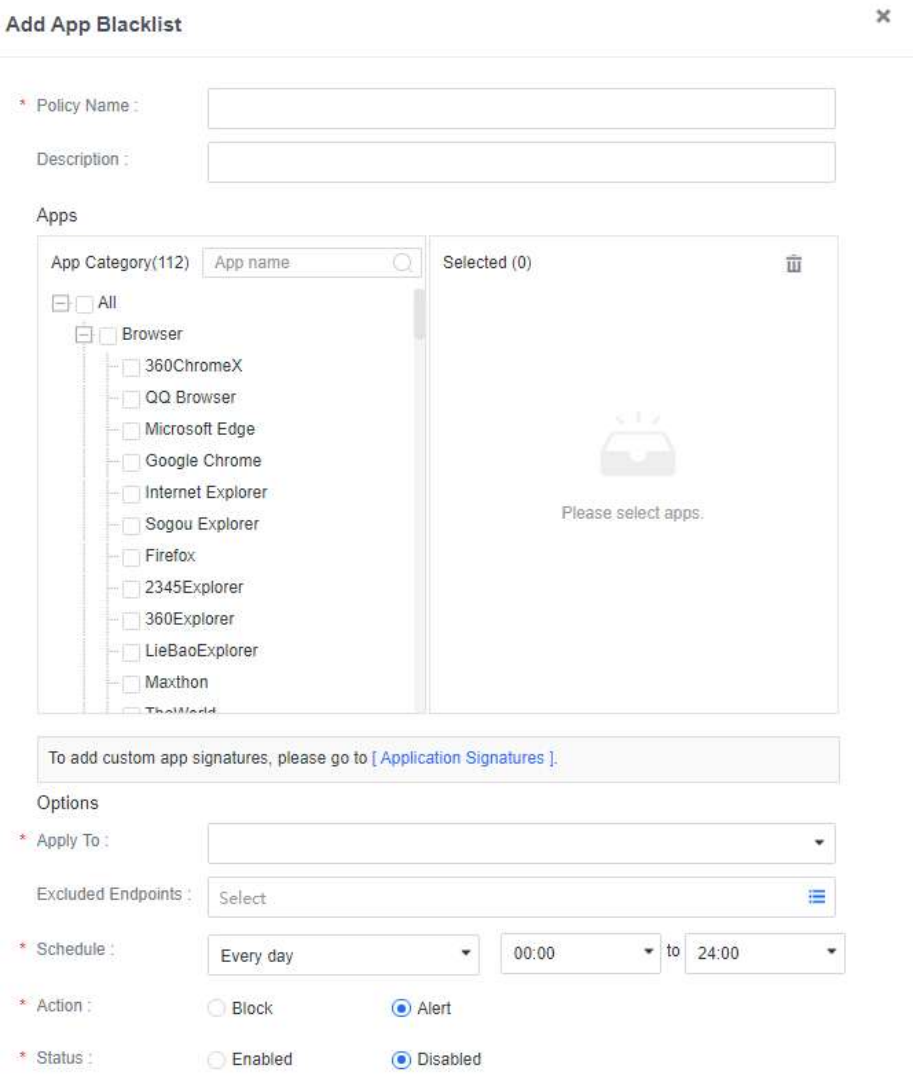
4.6.5.1 Application Blacklists

To manage application blacklists, go to **Policies** > **App Control** > **Application Blacklists**, as shown in the following figure.



Click **New** to create an application blacklist. You can add applications to the blacklist, and specify endpoints to which the blacklist applies, the schedule of the blacklist takes effect, and the action to take when a blacklisted application

is detected, as shown in the following figure.

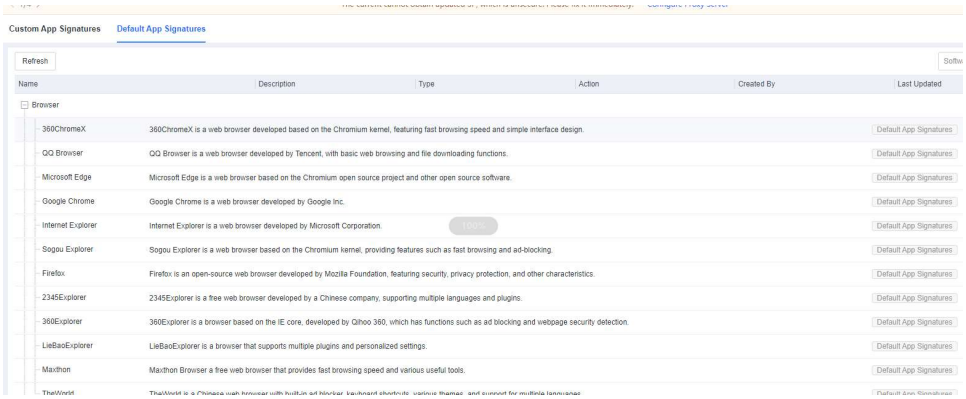


NOTE

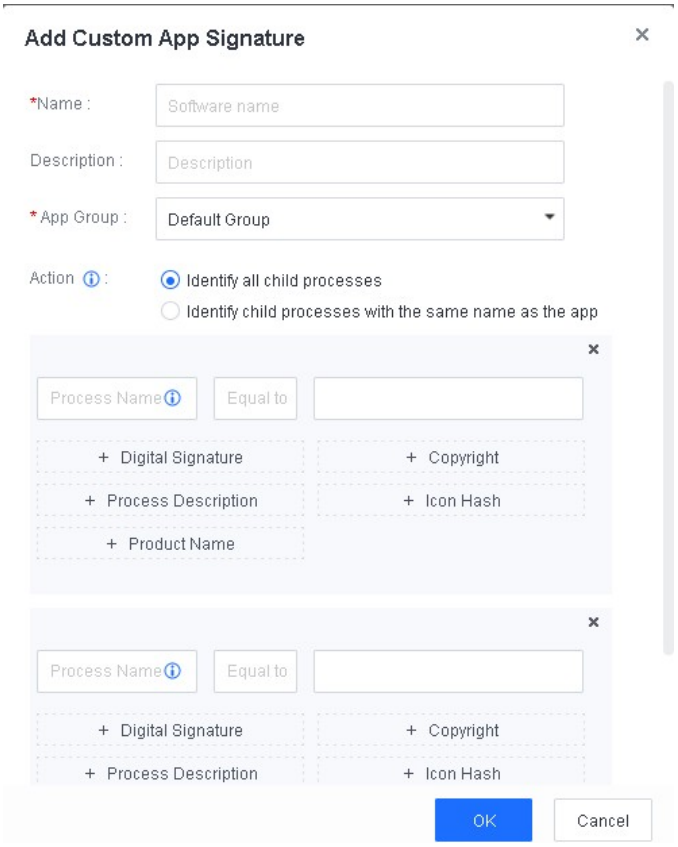
Software uninstallation is supported only for endpoints that run Windows 7 and later or Windows Server 2012 and later.

4.6.5.2 Application Signature Database

The application signature database provides default application signatures and supports custom application signatures.



Suppose a required application signature is not included in the default application signature database. In that case, you can go to **Policies** > **App Control** > **Application Signature Database** and add the application signature, as shown in the following figure.



App Group: The group to which the custom application belongs.

Action: The scope of child processes identification. An application may have child processes whose names differ from the application name. We

recommend that you select **Identify all child processes** so that you can identify and terminate all child processes of an application.

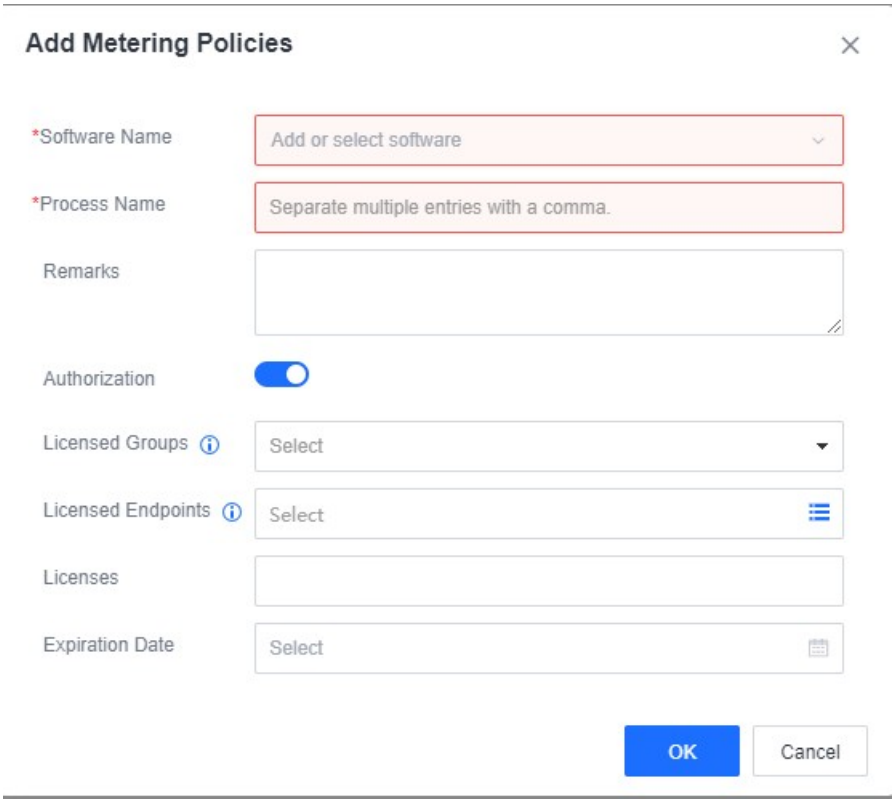
You can identify a custom application using one or more application information groups. Each application information group consists of multiple fields, including **Digital Signature**, **Copyright**, **Process Description**, **Icon Hash**, and **Product Name**. You can click the corresponding button to add an information field. To add an application information group, click **Add Another Group**.

If the application has only one child process, you need to add only one application information group. Otherwise, you need to add multiple application information groups. Multiple information fields or an application information group must match to identify an application uniquely.

4.6.5.3 Metering Policies

You can specify software metering policies. NovaGuard automatically collects the operation statistics of metered software on all managed endpoints. If you have configured an email notification, NovaGuard sends you an email in case

of insufficient license, unauthorized software use, or license expiration.



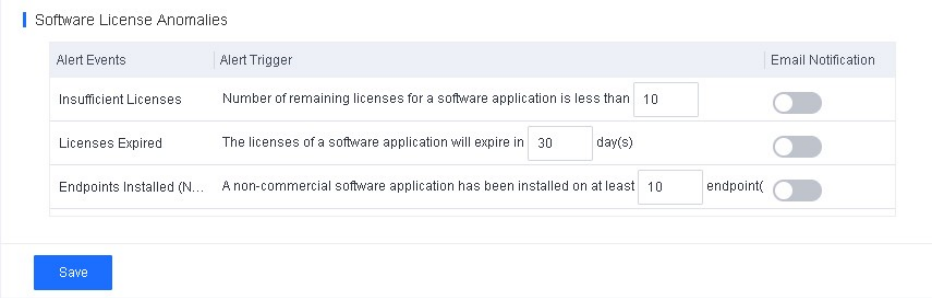
You can click **New** and set the following parameters to create a metering policy:

Software Name: The name of the software.

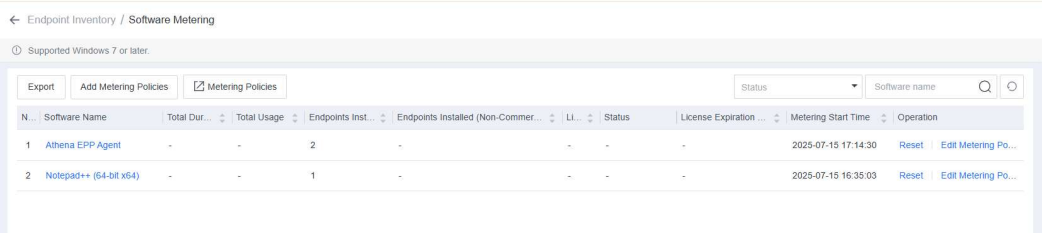
Process Name: The name of the process file. If two process names are the same, the number of executions and usage duration of the corresponding software are repeatedly metered.

Authorization: Enable it to trigger license-related alerts rather than limiting the software usage on endpoints. You can fill in the information as needed. Enable this on specific endpoints only.

You can click **License Alert Settings** to configure alert settings on events such as insufficient license, license expiration, and use of non-commercial software.



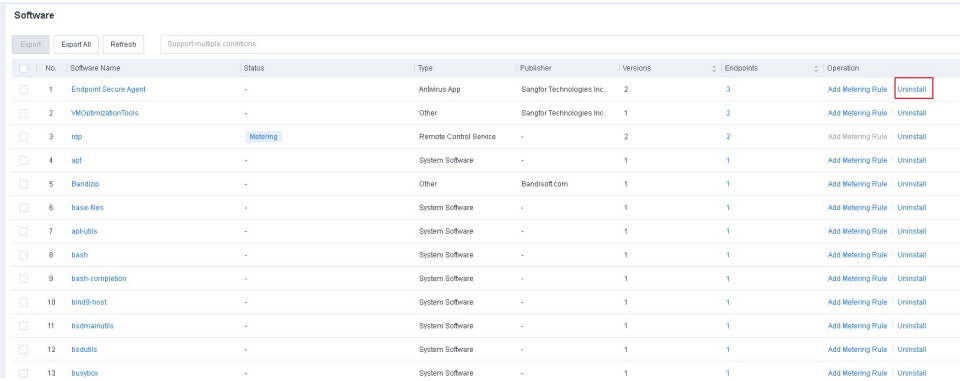
After you save the settings, you can go to **Endpoints** > **Endpoint Inventory** > **Office PCs** > **Software Metering** to view the software metering information in columns such as **Total Duration**, **Total Usages**, **Endpoints Installed**, **Endpoints Installed (Non-Commercial)**, **Licenses**, **Status**, **License Expiration Date**, and **Metering Start Time**.



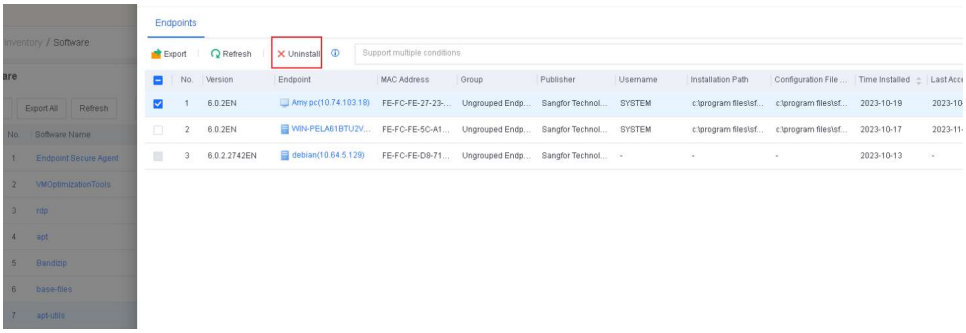
4.6.5.4 Software Uninstallation

Once you find a piece of non-compliant software on a managed endpoint, you can remotely uninstall the software. This is the last action in the software lifecycle management.

To uninstall the non-compliant software from all managed endpoints, go to **Endpoint** > **Endpoint Inventory** > **Software** and click **Uninstall** under the **Operation** column.



You can also click the software name to go to the details page, select an endpoint, and uninstall the software from only the selected endpoint.



After you click **Uninstall**, you need to create an uninstallation task.

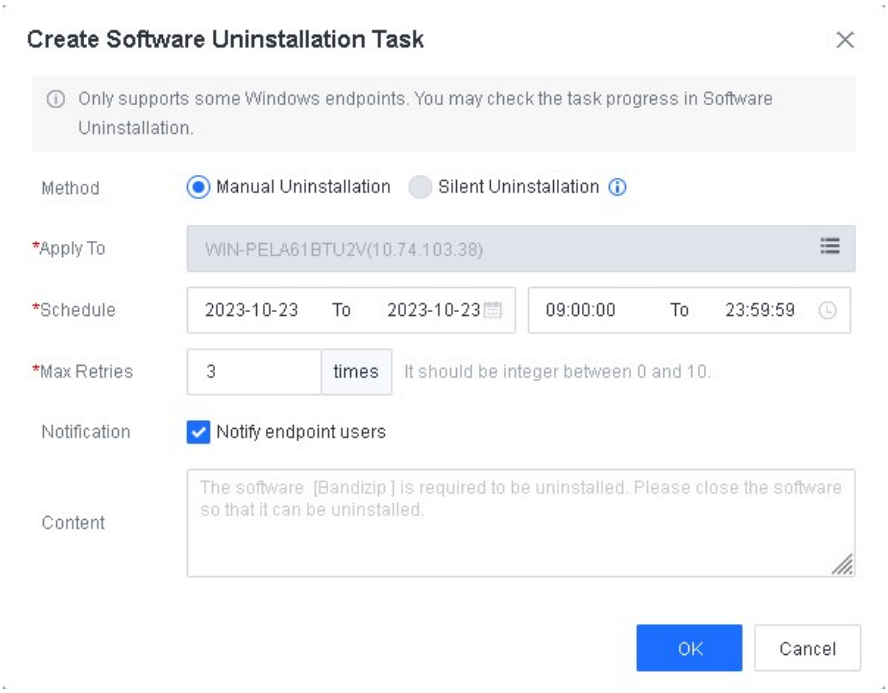
Manual Uninstallation: You can select this method to uninstall any software.

Silent Uninstallation: You can select this method to uninstall software that supports silent uninstallation.

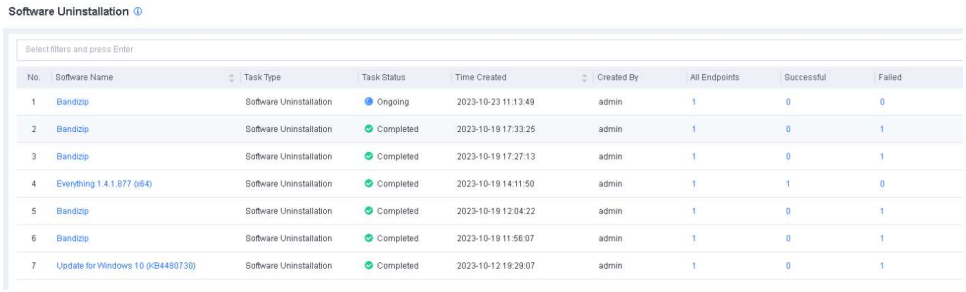
Schedule: The task will be executed during the specified period.

Max Retries: If the task fails on the first try, it retries until the software is uninstalled from the endpoint or it meets the **Max Retries**, whichever comes first.

Notification: If you check this option, the endpoint user will be notified 5 minutes before and when the uninstallation starts.



After you create an uninstallation task, you can go to **Policies** > **App Control** > **Software Uninstallation** to check the task progress.



NOTE

Software uninstallation is supported only for Windows 7 and above endpoints or Windows Server version 2012 and above.

4.7 System

On the **System** page, you can perform operations such as NovaGuard agent deployment, system update, integrated device management, branch management, account management, license management, data synchronization, object definition, and system setting.

4.7.1 Agent Deployment

4.7.1.1 Agent Download

NOTE

For more information about NovaGuard agent deployment, refer to **Chapter 2 Installation and Deployment.**

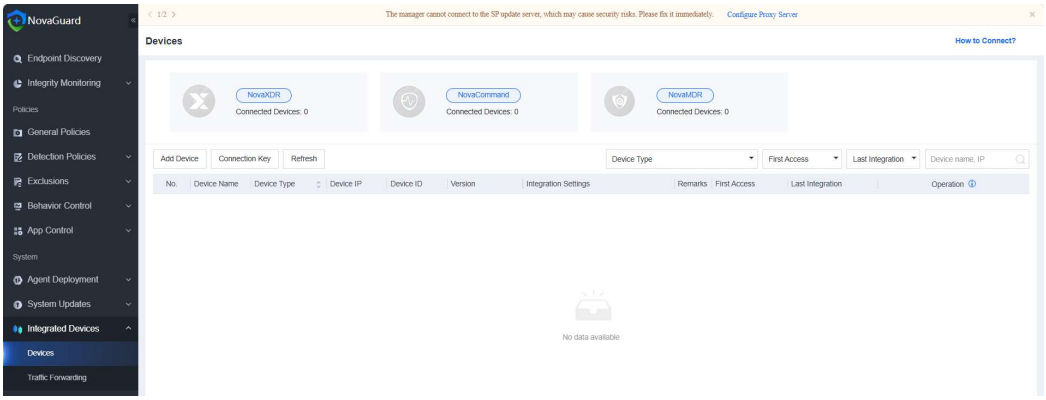
4.7.2 System Updates

NOTE

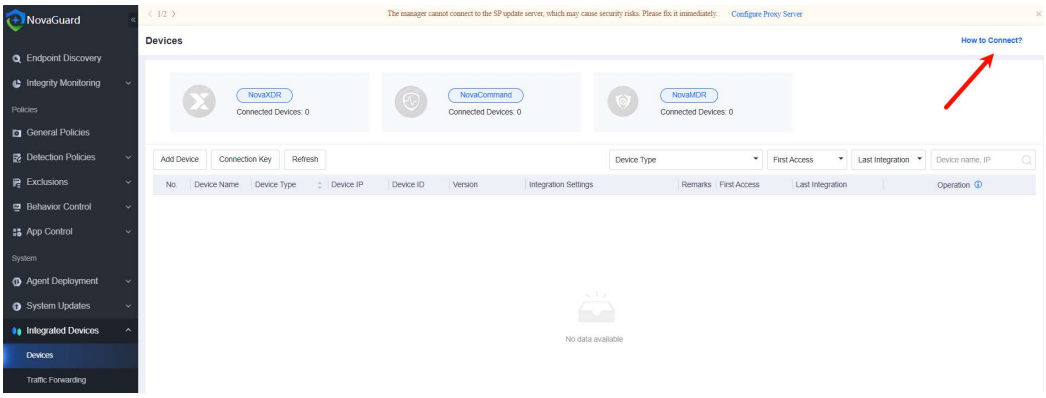
For more information about system updates, refer to **Chapter 4 Product Upgrade**.

4.7.3 Integrated Devices

This feature enables NovaGuard to be integrated with NovaXDR, NovaCommand, and NovaMDR, providing customers with a closed-loop solution from threat discovery to threat fix. To manage integrated devices, go to **System** > **Integrated Devices** > **Devices**, as shown in the following figure.



To view the integration configurations of different products, click **How to Connect?** in the upper right corner of the **Devices** page.



Features supported by integrated devices

The following table describes the features supported by devices integrated with NovaGuard.

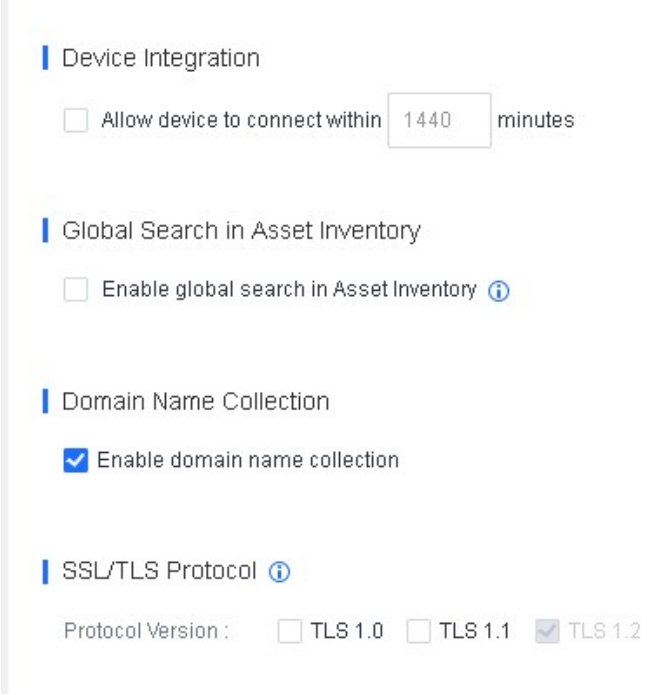
Device	Agent Deployment	Endpoint Isolation	Log Reporting	Access Control	Virus Scan	Threat Fix	IOC Forensics	Risk Assessment

NovaXDR	N	Y	Y	Y	Y	Y	Y	Y
NovaMDR	N	Y	Y	Y	Y	Y	N	Y
NovaCommand	N	Y	Y	Y	Y	Y	Y	Y

Table 4: Features Supported by Integrated Devices

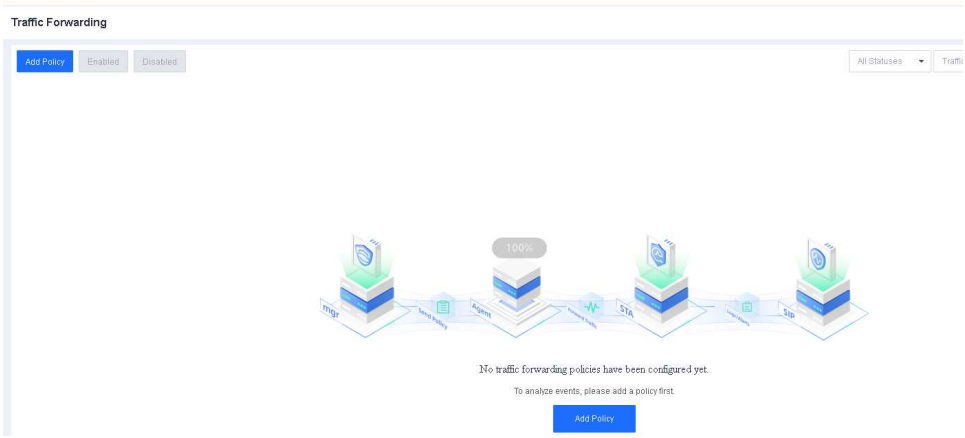
Device integration configuration

To integrate NovaGuard with any other products, go to **System** > **System** > **General**, enable **Device Integration**, specify the duration a device can be connected, and select **TLS1.0** and **TLS1.1** in the **SSL/TLS Protocol** section.

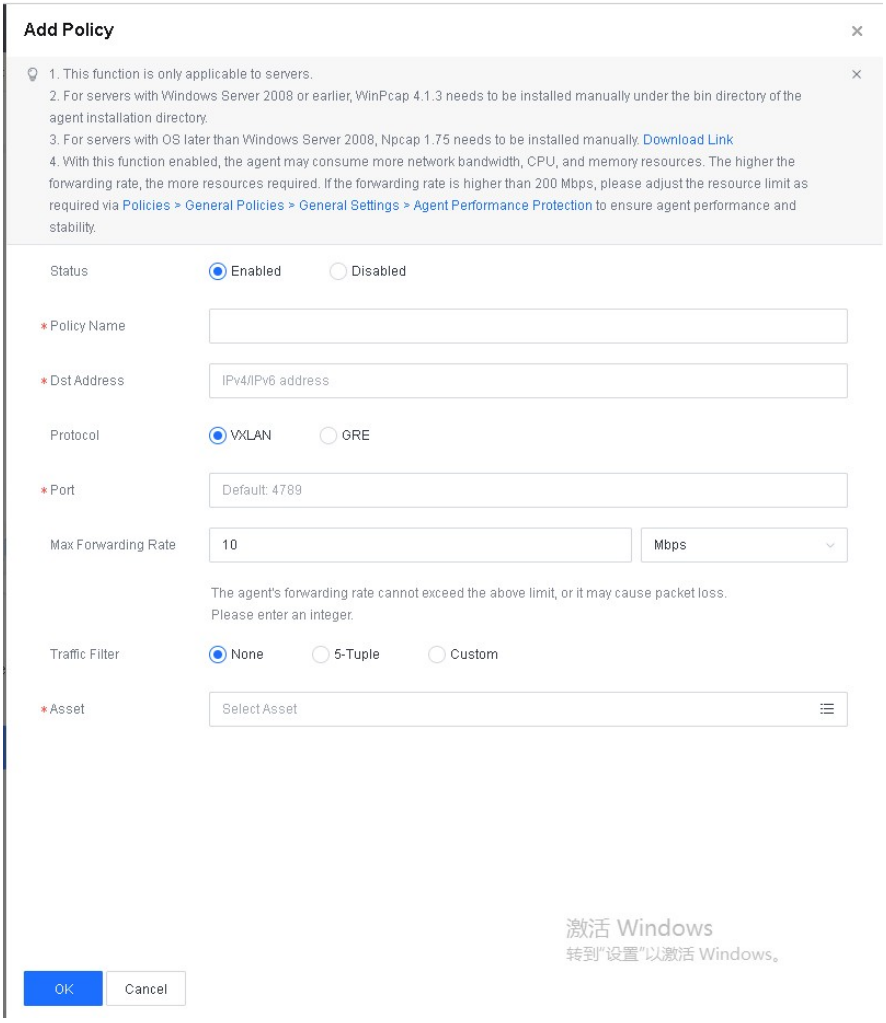


4.7.3.1 Traffic Forwarding

NovaGuard uses the traffic forwarding feature to collect the original traffic from a host's NIC and forward it to the NovaCommand device for threat analysis. To enable this feature, you must integrate NovaGuard with NovaCommand.



To configure a forwarding policy, click **Add Policy** and set the following parameters.



Specify the IP address of the STA device for **Dst Address**; select **VXLAN** or **GRE** for **Protocol**; set the value of **Max Forwarding Rate** below 1 Gbit/s; and specify a value for **Traffic Filter**, where **None** indicates that the traffic is

collected without filtering and **5-Tuple** indicates that the 5-tuple attributes are collected.

4.7.4 Branches

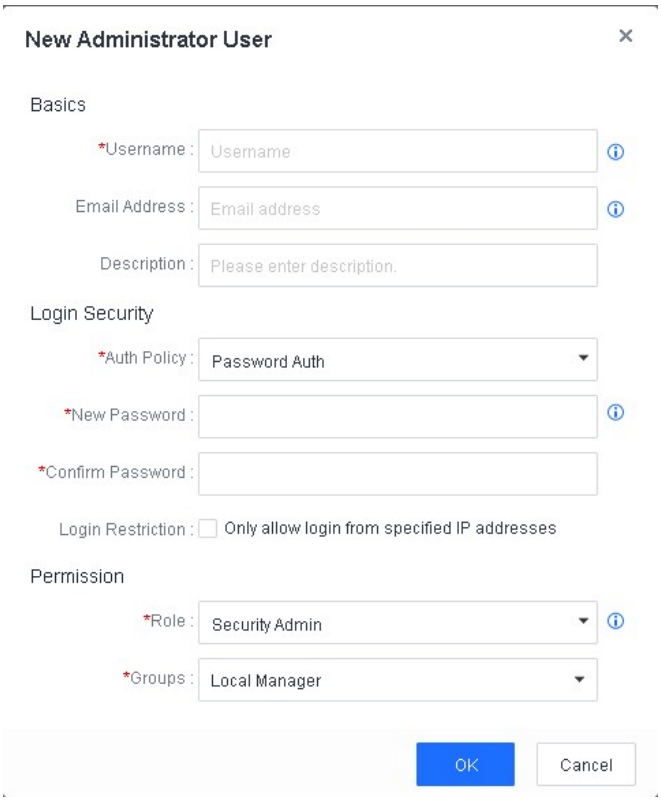
NOTE

For details about branch management, see **Chapter 2.2.2 Cascade Deployment**.

4.7.5 Administrators

4.7.5.1 Administrator Roles

You can create administrator accounts with different roles as needed. To create an administrator account, go to **System** > **Administrators** and click **New > Local Account**, as shown in the following figure.



In the **Role** field, select one of the following roles as needed:

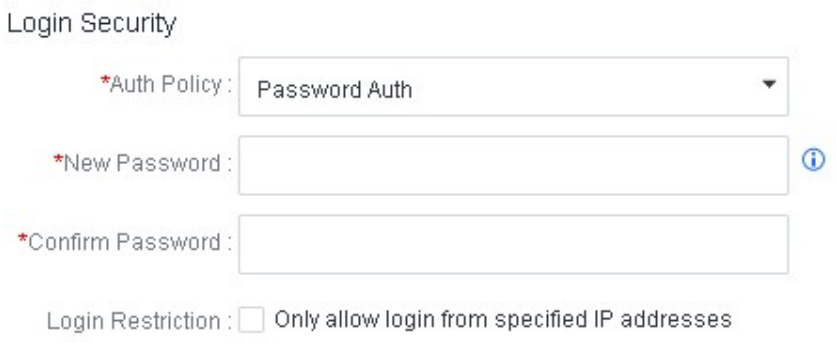
System Admin: Allowed to view the home page and configure system settings (excluding log settings).

Security Admin: Allowed to view and configure administrators, security policies, and security events. This role cannot perform operations on micro-segmentation, integrated devices, reports, account management, system updates, licensing, branches, and system settings.

Audit Admin: Can only view system information. This role cannot perform any operations to edit, add, or delete information.

4.7.5.2 Manager Login Authentication

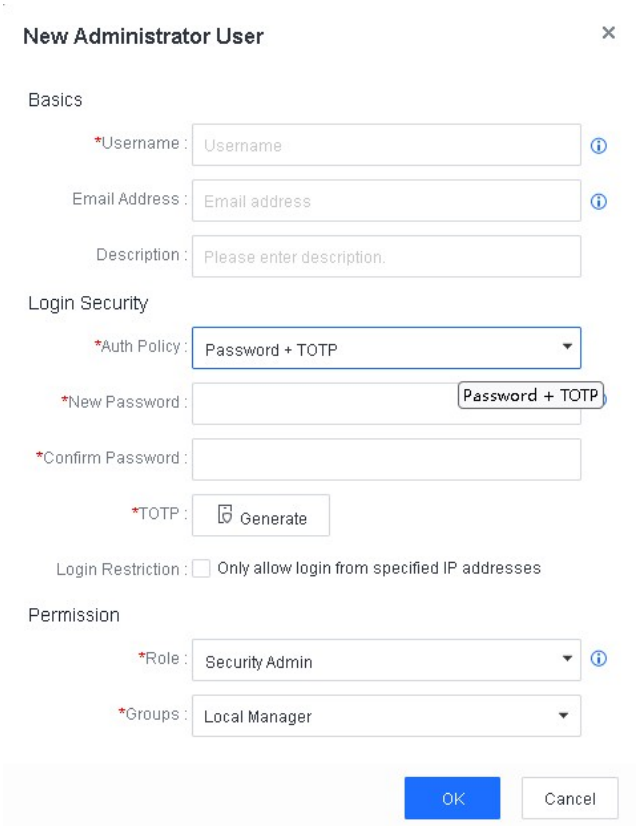
You can select the NovaGuard manager **Auth Policy** from **Password Auth** or **Password + TOTP**. Go to **System** > **Administrators**, click **New > Local Account** to create an administrator account and select **Password Auth** as the Auth Policy, as shown in the following figure.



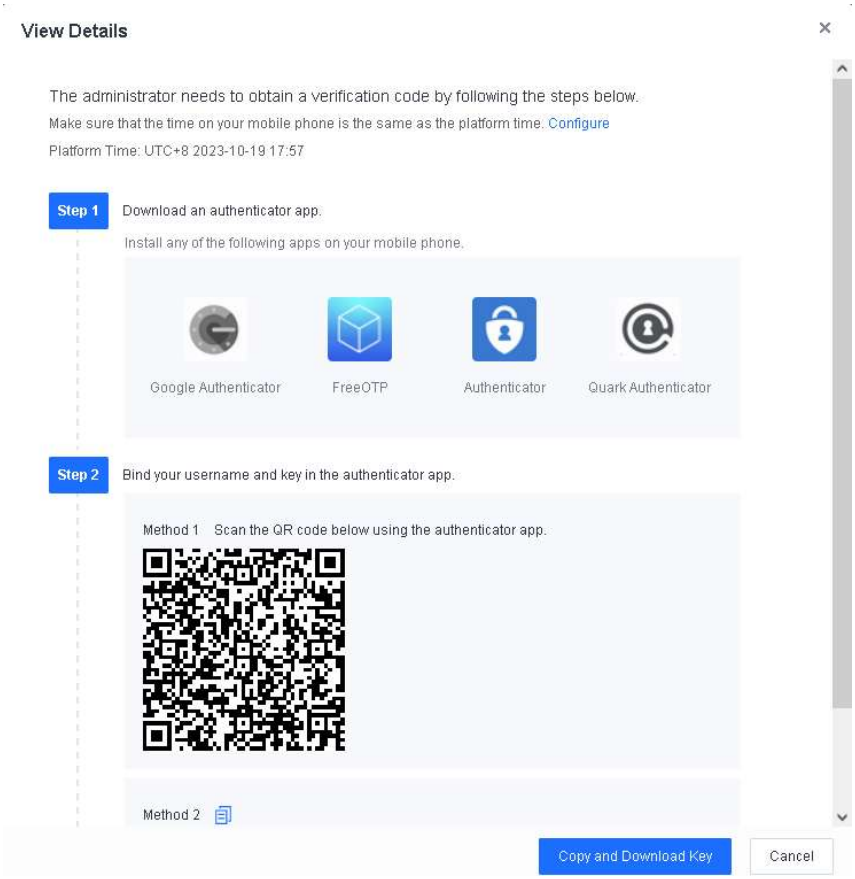
Password + TOTP

This two-factor authentication method requires administrators to log in to the NovaGuard manager using their account passwords and TOTPs sent to their mobile devices. The configuration procedure is as follows:

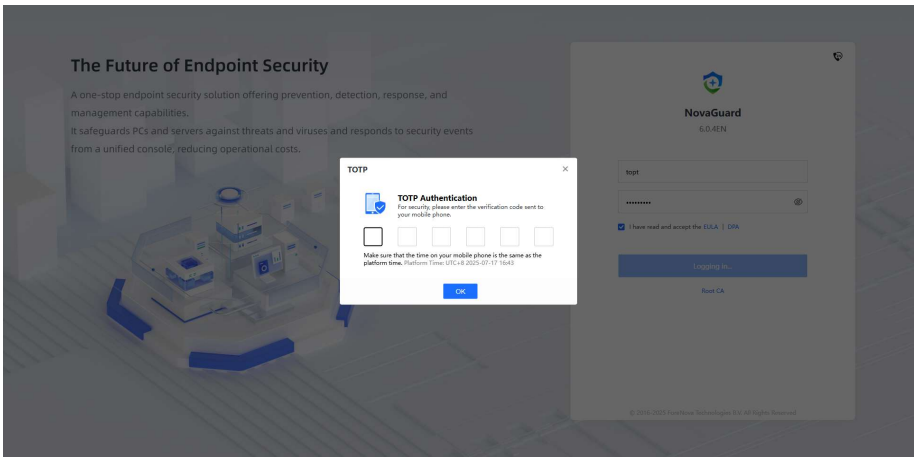
Go to **System** > **Administrators**. Click **New** in the upper right corner or **Edit** in the **Operation** column of an existing account. Then, select **Password + TOTP** for **Auth Policy**, as shown in the following figure.


New Administrator User
Basics
*Username :
Username
Email Address :
Email address
Description :
Please enter description.
Login Security
*Auth Policy :
Password + TOTP
*New Password :
Password + TOTP
*Confirm Password :
*TOTP :
Generate
Login Restriction :
Only allow login from specified IP addresses
Permission
*Role :
Security Admin
*Groups :
Local Manager
OK
Cancel

Click **Generate** and add authentication information as prompted, as shown in the following figure.

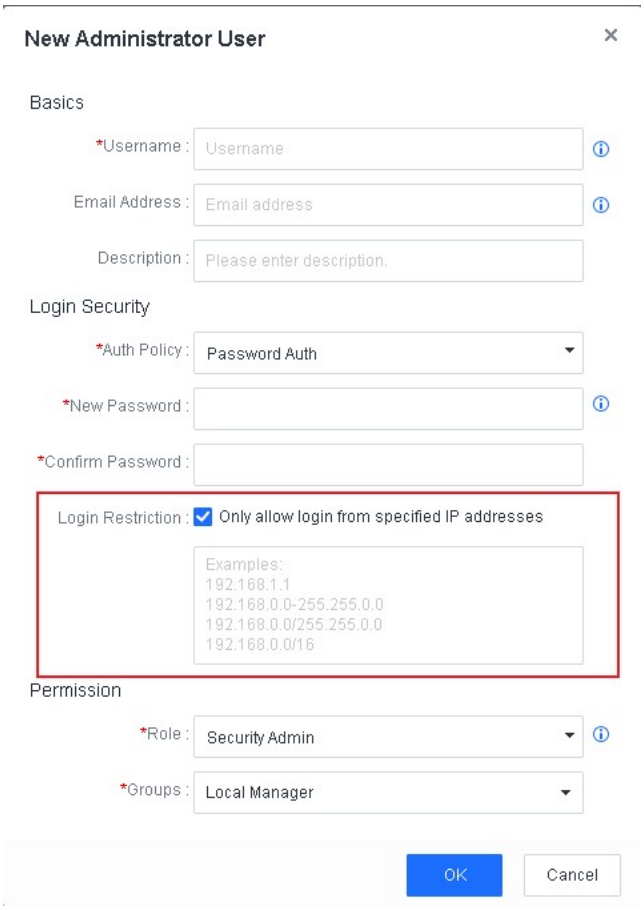


After the configuration, administrators must enter their account passwords and TOTPs sent to their mobile devices when they log in to the NovaGuard manager, as shown in the following figure.



4.7.5.3 Login Restriction Based on IP Addresses

The NovaGuard manager supports login from specified IP addresses only. On the **New Administrator User** page, you can enable **Only allow login from specified IP addresses**, and set IP addresses for endpoints that are allowed to log in to the NovaGuard manager, as shown in the following figure.



4.7.6 Licensing

4.7.6.1 License Types

NovaGuard provides essential and ultimate licenses, as shown in the following figure.

Sangfor Endpoint Secure Capabilities		Windows workstation		Windows Server		Linux		macOS	
		essential	ultimate	essential	ultimate	essential	ultimate	essential	ultimate
Prevention	Vulnerability Scan	√	√	√	√	√	√		
	Remediation	√	√	√	√	√	√		
	Security Compliance	√	√	√	√	√	√		
	Asset Inventory	√	√	√	√	√	√		
	Asset Discovery	√	√	√	√	√	√		
	Micro-Segmentation	0	√	0	√	0	√		
	Hot Patching	0	√	0	√	0	0		
	TOTP Authentication	√	√	√	√	√	√	√	√
	Endpoint Behavior Data & Log Collection	√	√	√	√	√	√		
Protection	Realtime File Monitoring	√	√	√	√	√	√		
	Ransomware Honeypot	√	√	√	√	0	0		
	Ransomware Protection	√	√	√	√	0	0		
	Ransomware Backup Recovery	√	√	√	√	0	0		
	Ransomware Defense	√	√	√	√	0	0		
	Fileless Attack Protection	0	√	0	√	0	0		
	End-of-Support Windows System Protection	√	√	√	√	0	0		
	RDP Secondary Authentication (Anti-Ransomware)	0	√	0	√	0	√		
	Trusted Processes (Anti-Ransomware)	0	√	0	√	0	0		
	Key Directory Protection (Anti-Ransomware)	0	√	0	√	0	0		
Detection	Malicious File Detection	√	√	√	√	√	√	√	√
	APT Detection	√	√	√	√	√	√		
	Brute-Force Attack Detection	√	√	√	√	√	√		
	Improved Phishing and Web Intrusion Detection	√	√	√	√	0	0		
	Coordinated Malware Response with XDDR	0	√	0	√	0	√		
	WebShell Detection	0	0	0	√	0	√		
	Advanced Threat Detection	0	√	0	√	0	√		
	Suspicious Login Detection	√	√	√	√	√	√		
	Suspicious Scan Detection	√	√	√	√	√	√		
	Memory Backdoor Detection	0	√	0	√	√	√		
	Reverse Shell Detection	0	√	0	√	√	√		
	Local Privilege Escalation Detection	0	√	0	√	√	√		
	Remote Command Execution Detection	0	√	0	√	√	√		
Response	File Quarantine	√	√	√	√	√	√	√	√
	Endpoint Isolation	√	√	√	√	√	√	√	√
	File Remediation	√	√	√	√	√	√		
	Virus Mitigation	√	√	√	√	√	√	√	√
	Automated Response to Phishing and Web Intrusion events	√	√	√	√	0	0		
	Extended Detection, Defense and Response (XDDR)	0	√	0	√	0	√		
	Threat Hunting	0	√	0	√	0	√		
	Domain Isolation	√	√	√	√	0	0		
	Process Blocking	√	√	√	√	√	√		
Maintenance	Script File Upload	√	√	√	√	√	√		
	USB Control	√	√	√	√	0	0	√	√
	Unauthorized Outbound Access Detection	0	0	√	√	0	0		
	Remote Support	√	√	0	0	0	0		
IT Governance	Application Blacklist	0	√	0	√	0	0		
	Software Metering	0	√	0	√	0	0		
	Software Uninstallation	0	√	0	√	0	0		

New deployment

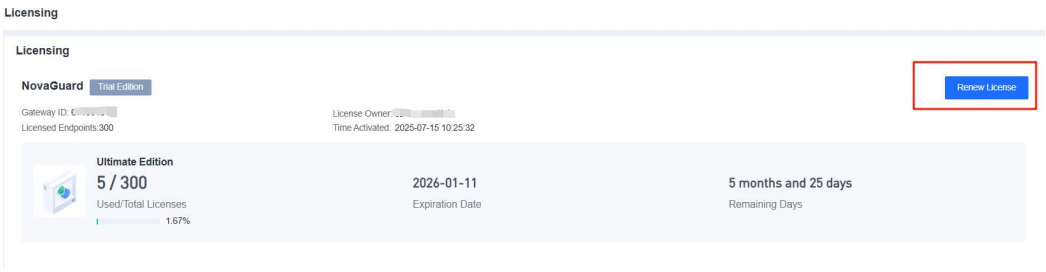
An official license is activated through the ForeNova Licensing Server. To activate a trial license, contact the local sales team. For license activation methods, see **Chapter 2.2 Product Activation**.

Update/Renew License

A license can be activated twice. If a license is lost after the first activation, it can be activated again. The license information is related to the NovaGuard manager hardware. A change in the hardware information invalidates a license. License update/renewal is required in the following two scenarios:

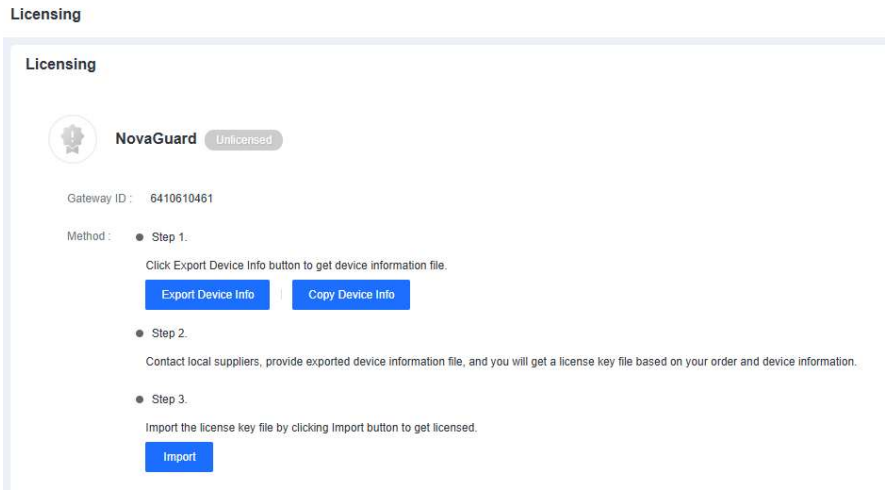
1. **A change in the NovaGuard manager hardware information**

Go to **System** > **Licensing** and click **Renew License**, as shown in the following figure.



1. **Migrate to a new server due to an NovaGuard manager fault**

In this case, go to **System** > **Licensing** and import a new license, as shown in the following figure.



NOTE

License expiration leads to the following results:

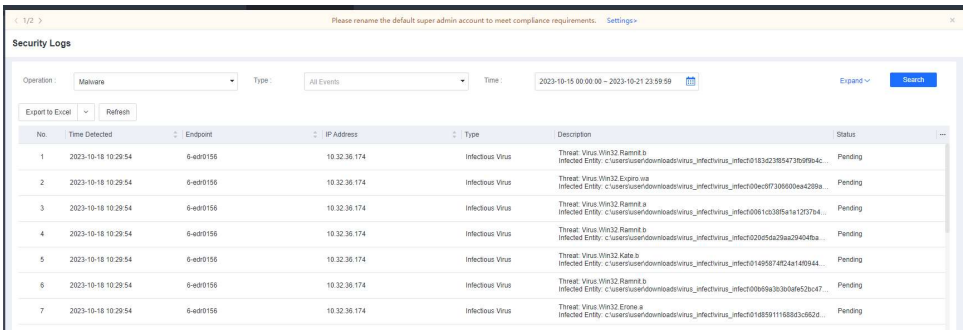
1. NovaGuard cannot be installed on a new endpoint.
2. NovaGuard and its databases cannot be updated.
3. Neural-X and Threat Analytics are disabled.

4.7.7 Logs

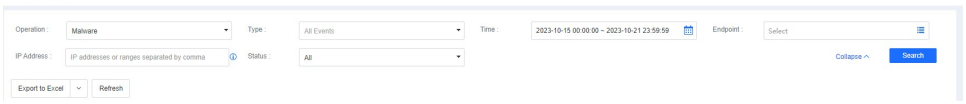
You can view logs on pages such as **Coordinated Action**, **Operations Logs**, and **Admin Logs**, and manually export and subscribe to reports of risks.

4.7.7.1 Security log

You can query security logs by going to **System > Logs > Security Logs**. These logs mainly include security-related information, such as anti-malware, vulnerability scan, security compliance check, intrusion detection, micro-segmentation, server protection, USB device control, and USB device blocking, and hacktool protection, as shown in the following figure.

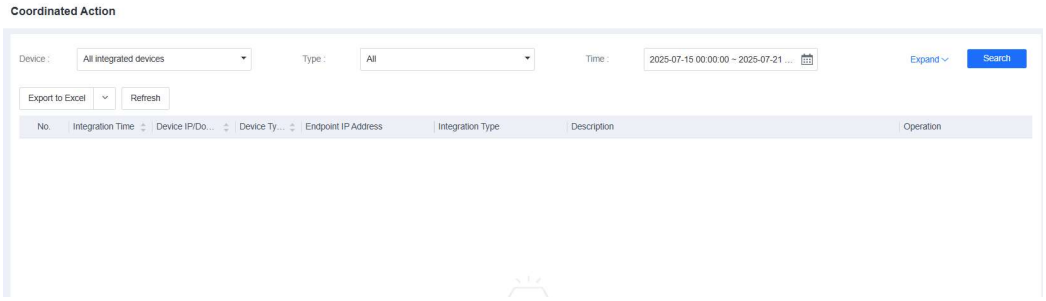


You can first filter these logs by operation and time, and then click **Expand** to filter logs by endpoint name and IP address. The filtering results can be exported.



4.7.7.2 Coordinated Action

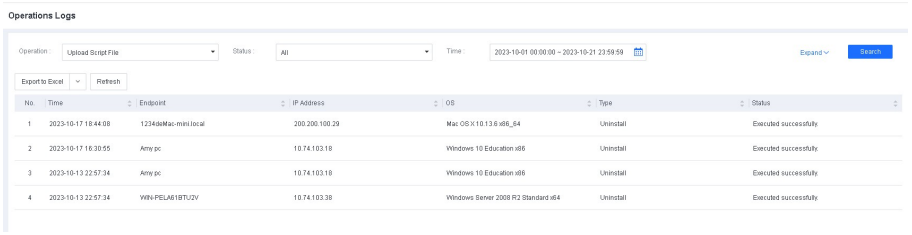
On the **Coordinated Action** page, as shown in the following figure, you can view logs that record the coordinated actions between NovaGuard and other ForeNova products, such as action overview, integration time, device IP address, device type, integration type, and integration description. NovaGuard can be integrated with NovaXDR, NovaCommand, and NovaMDR.



You can filter logs by device name, integration type, and time, then click **Expand** to filter logs by endpoint name and IP address. Once you have applied your filters, you can export the filtering results.

4.7.7.3 Operations Logs

On the **Operations Logs** page, you can select **Upload Script File**, **Remote Support**, and **LDAP Sync History** from the **Operation** drop-down list to view three types of operations logs. The log information is displayed in columns such as **Time**, **Endpoint Name**, **IP Address**, **OS**, **Type**, and **Status**, as shown in the following figure.



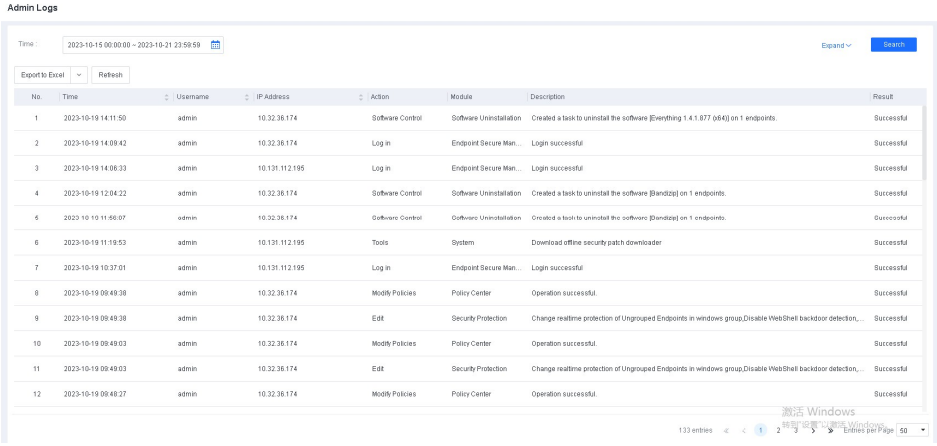
If you select **Upload Script File**, for example, you can filter logs by status and time, then click **Expand** to filter logs by script file name, endpoint name, and IP address. Once you have applied your filters, you can export the filtering results.

4.7.7.4 Control Logs

In the control log, you can view what control operations have been issued to the agent, such as: Hardware Changes, Unauthorized Outbound Access, USB Device Control, Software Uninstallation, App Control.

4.7.7.5 Admin Logs

On the **Admin Logs** page, you can view information about administrative operations performed on the NovaGuard manager in columns such as **Time**, **Username**, **IP Address**, **Action**, **Module**, **Description**, and **Result**, as shown in the following figure.



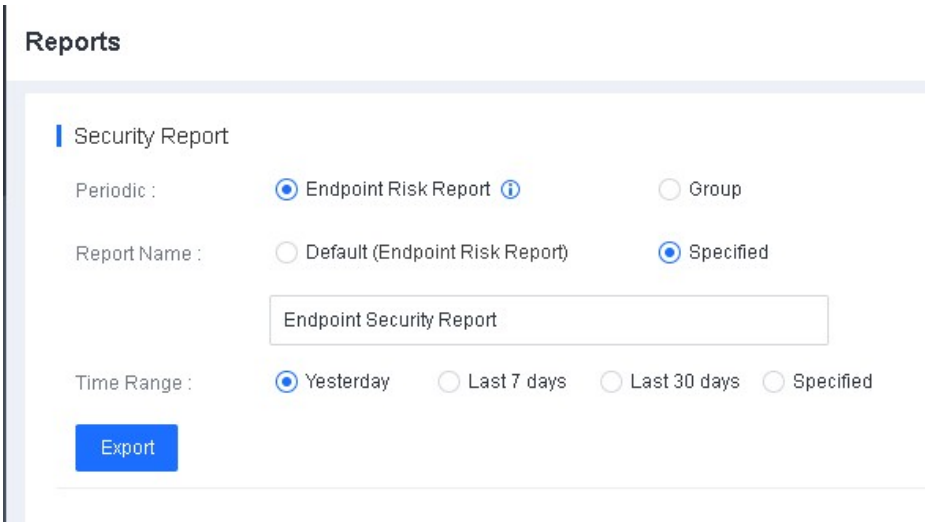
You can filter logs by time, then click **Expand** to filter logs by username and IP address. Once you have applied your filters, you can export the filtering results.

4.7.7.6 Reports

Export a report

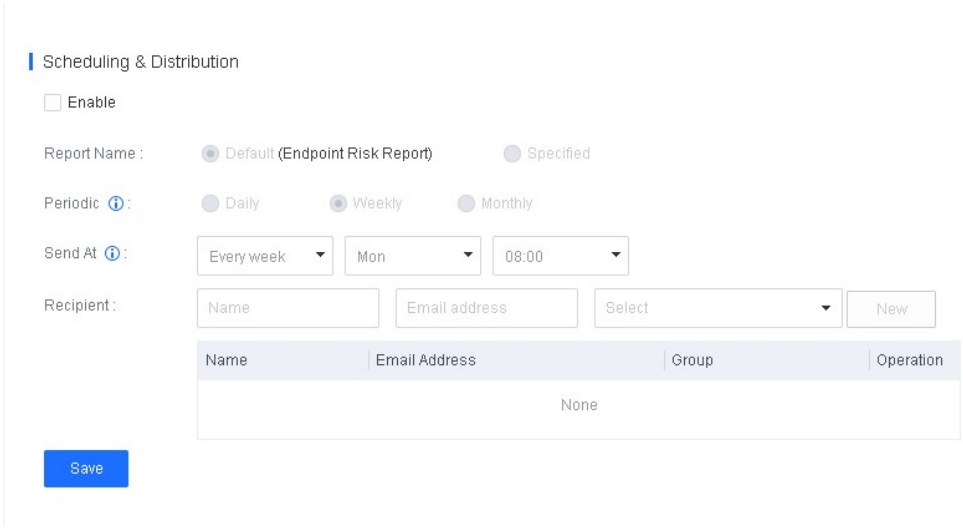
You can export risk reports of all managed endpoints from the NovaGuard manager for quick analysis and assessment of business and network security risks. When you export a report, you can specify its name and time range, as

shown in the following figure.



Subscribe to reports

You can subscribe to risk reports. In the **Scheduling & Distribution** section, specify the report name, report type, sending time, and recipients, as shown in the following figure.



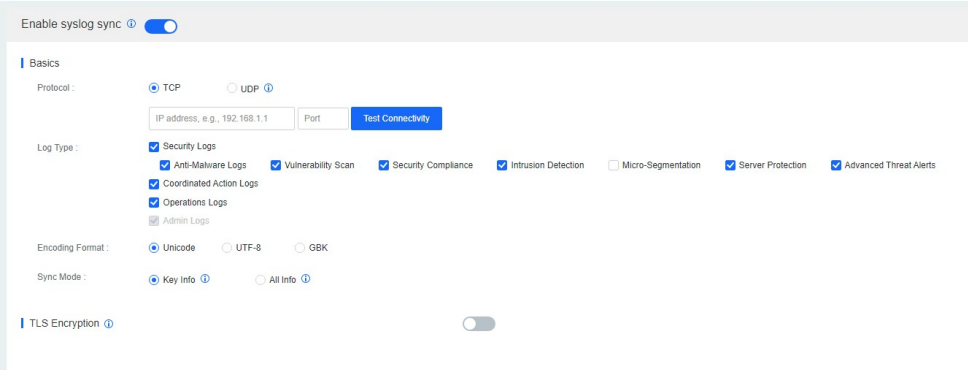
- **Periodic**: Valid values are **Daily**, **Weekly**, and **Monthly**, which refer to reports during one calendar day (00:00 - 24:00), calendar week (Monday - Sunday), or calendar month (1st day to the end date of the month).
- **Send At**: Specify the time when a security report will be sent to the recipients.

4.7.8 Data Sync

In the **Data Sync** module, you can configure the NovaGuard manager to send data such as logs and asset information to a third-party syslog server or Kafka server.

4.7.8.1 Syslog Reporting

On this page, you can sync the logs of NovaGuard to a syslog server over the syslog protocol, as shown in the following figure.



Protocol: First, select the protocol supported by the syslog server. Most syslog servers support the UDP protocol. Then, specify the IP address and port of the syslog server.

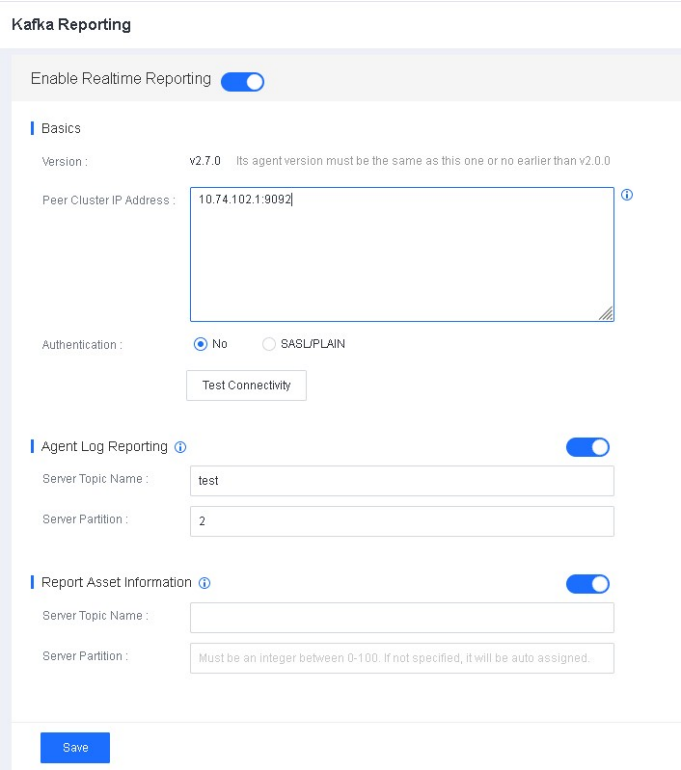
Log Type: Select the types of logs to be synced to the syslog server.

Encoding Format: The **Unicode**, **UTF-8**, and **GBK** formats are supported.

Sync Mode: If you select **Key Info**, only a few log fields will be synced. This mode is suitable for log retention of the Multi-Level Protection Scheme (MLPS). If you select **All Info**, all log fields will be synced. This mode is suitable for a comprehensive security log analysis after synchronization.

4.7.8.2 Kafka Reporting

On this page, you can sync the logs of NovaGuard to a third-party Kafka server, as shown in the following figure.



Peer Cluster IP Address: Specify the IP address and port of the Kafka server. Example: 2.2.2.2:9092.

Authentication: Specify the Kafka server authentication method.

Agent Log Reporting: Specify the topic name and partition for storing the NovaGuard agent logs on the Kafka server.

Asset Info Reporting: Specify the topic name and partition for storing asset information on the Kafka server.

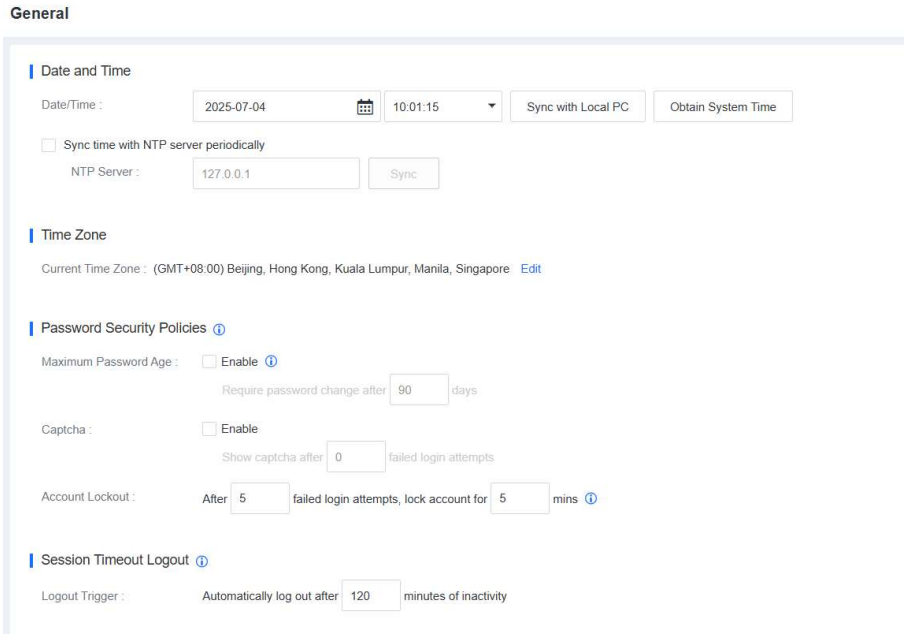
4.7.9 System

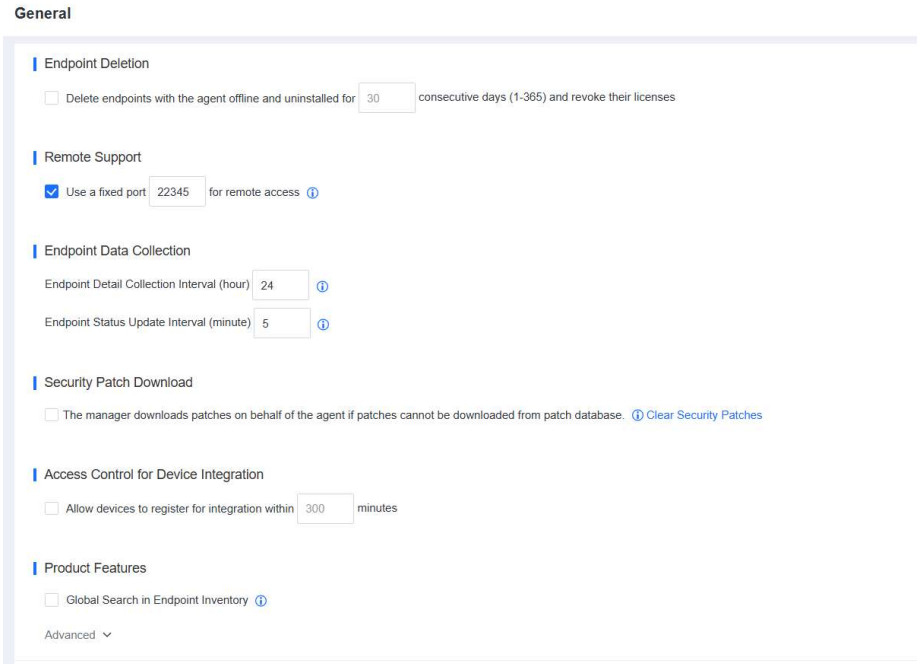
In this module, you can configure system settings on the following pages: **General**, **Data Backup**, **Network**, **Logging Options**, **Deployment and Upgrade**, **Alert Options**, **LDAP Sync**, **Customization**, and **Tools**.

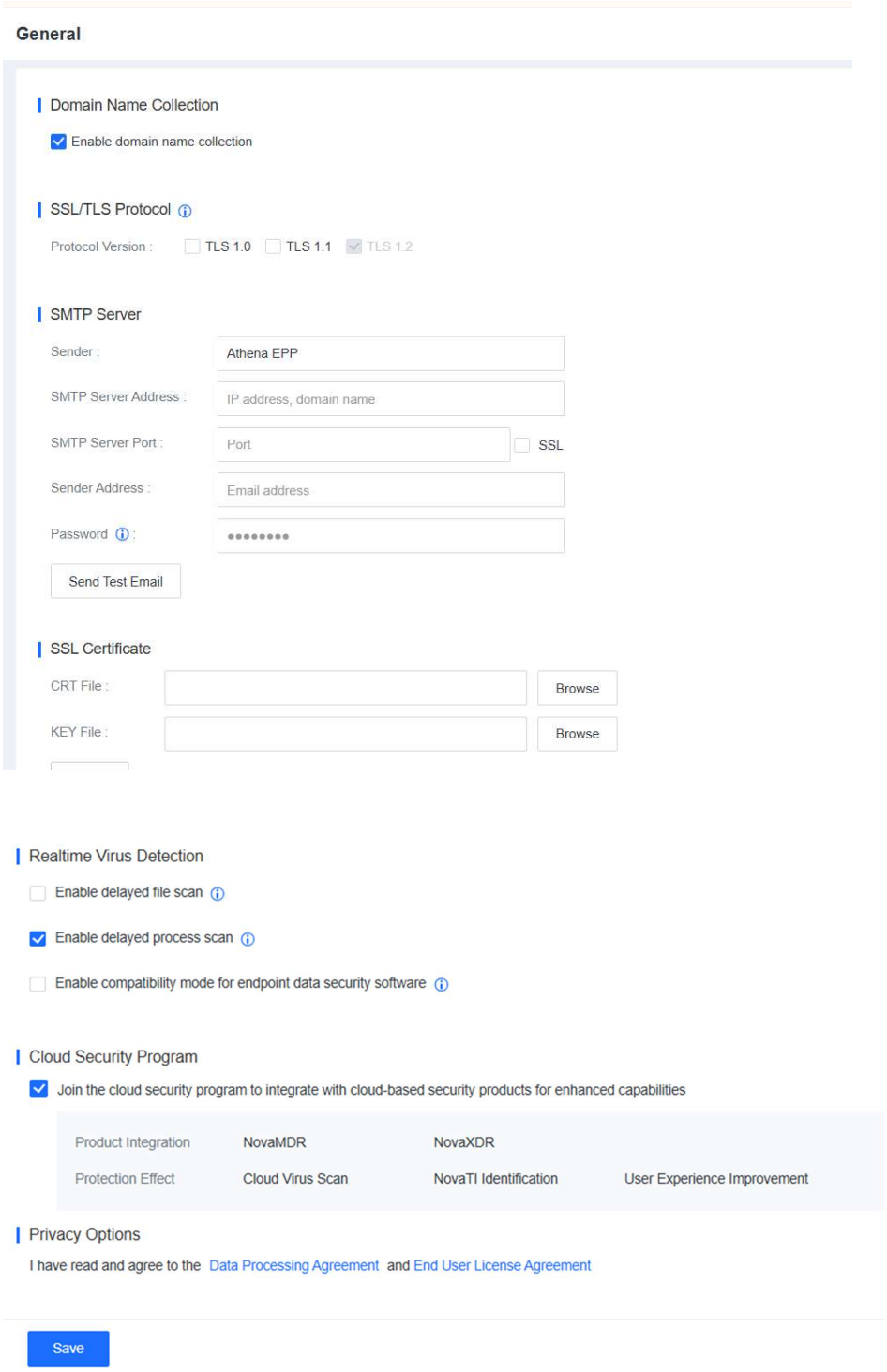
4.7.9.1 General

On the **General** page, you can configure basic system settings, including **Date and Time**, **Time Zone**, **Password Security Policies**, **Session Timeout Logout**, **Endpoint Deletion**, **Remote Support**, **Endpoint Data Collection**, **Security**

Patch Download, **Access Control for Device Integration**, **Product Features**, **Domain Name Collection**, **SSL/TLS Protocol**, **SMTP Server**, **SSL Certificate**, **Realtime Virus Detection**, **Cloud Security Program**, and **Privacy Options**, as shown in the following figures.







1. **Date and Time**: Customize the time of the NovaGuard manager. You can click **Sync with Local PC** to synchronize the time from the local computer, or click **Obtain System Time** to obtain the time of the server where the NovaGuard manager is installed. If the NovaGuard manager can access the Internet, you can select **Sync time with NTP server periodically** to

synchronize the time of the NovaGuard manager with the specified NTP server.

2. **Time Zone**: Click **Edit** to modify the time zone of the NovaGuard manager. The time zone of the Chinese mainland is GMT+08:00.
3. **Password Security Policies**: Configure password security policies, including password expiration period, CAPTCHA verification, and automatic account lockout after a specific number of failed login attempts within a specified time period.
4. **Session Timeout Logout**: Automatically log out a user if the user stays inactive for a specific number of minutes without performing any operations on the NovaGuard manager.
5. **Endpoint Deletion**: Select whether to automatically delete an endpoint from the NovaGuard manager and revoke its license if the endpoint stays offline for a specific number of consecutive days.
6. **Remote Support**: Specify the fixed port for remote access in NovaGuard. Through the fixed port, remote control can be implemented.
7. **Endpoint Data Collection**: Specify the time interval for endpoint data collection for the **Endpoint Inventory** module, with a value range from 4 to 168 hours, as well as the time interval for endpoint status updates, with a value range from 3 to 10 minutes.
8. **Security Patch Download**: If the NovaGuard 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.
9. **Access Control for Device Integration**: Specify 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 NovaXDR, and NovaMDR, the integrated devices can access the NovaGuard manager only within the specified period when this check box is selected.
10. **Product Features**: Select whether to enable or disable specific product features, including **Global Search in Endpoint Inventory**, **Snapshot-Based Ransomware Recovery**, **Advanced Threat Detection and Response**, **App Blacklist**, **Software Uninstallation**, **Unauthorized**

Outbound Access Detection, and **Cleanup**. If you enable these features, business continuity on endpoints may be affected. By default, these features are disabled.

11. **Domain Name Collection**: If you enable this feature, the NovaGuard manager records the processes that access malicious domain names. This feature can be used with botnet and malicious domain name forensics and global threat identification.
12. **SSL/TLS Protocol**: Protocol versions include TLS 1.0, TLS 1.1, and TLS 1.2. By default, TLS 1.2 is enabled because it is more secure than TLS 1.0 and TLS 1.1. To integrate NovaGuard with other devices, you must select TLS 1.0 and TLS 1.1.
13. **SMTP Server**: Configure the SMTP server to send subscription and alert emails. Click **Send Test Email** to check whether the SMTP server is properly configured. If the configuration is successful, the specified administrator will receive a test email, as shown in the following figure.

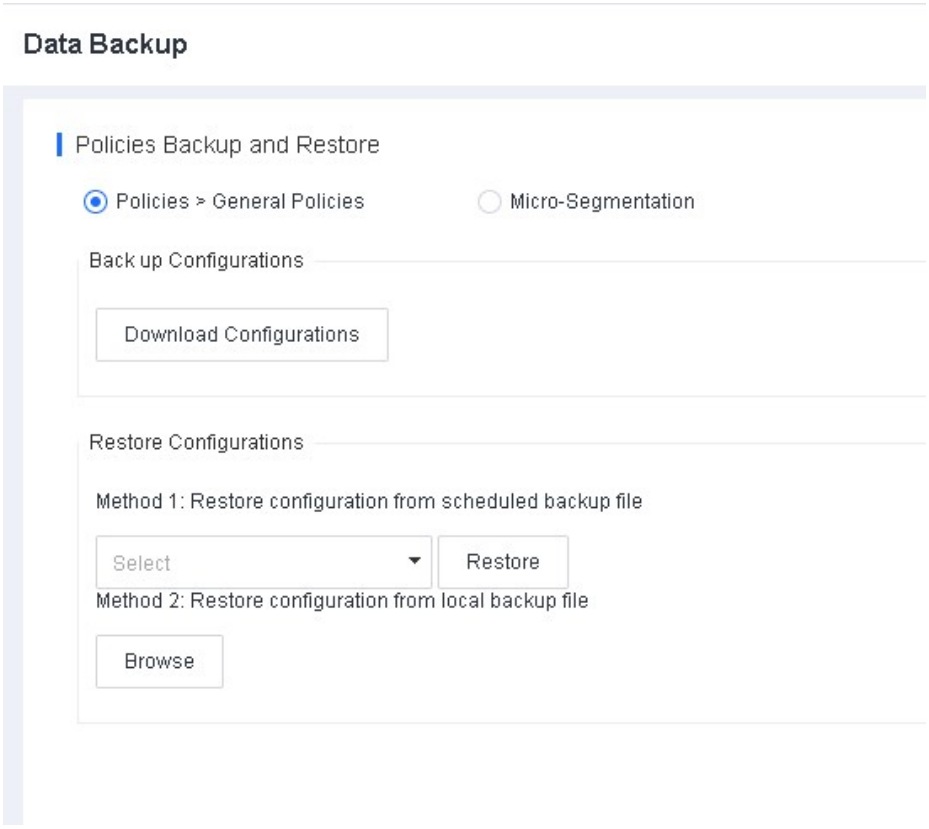


14. **SSL Certificate**: Support exporting custom SSL certificates to NovaGuard to achieve more secure access.
15. **Realtime Virus Detection**: Select whether to enable delayed file scan and delayed process scan. We recommend that you enable delayed file scan if NovaGuard conflicts with other software in terms of file exclusivity. After it is enabled, the virus scan on a file will be delayed by 2 seconds when it is detected that the file is being written to the disk. We recommend that you enable delayed process scan if encryption software exists. After it is enabled, the virus scan on the files associated with a process will be delayed by 2 seconds when it is detected that the process is being started.
16. **Cloud Security Program**: If **Join the cloud security program to integrate with cloud-based security products for enhanced capabilities** and **Allow internet-connected endpoints to upload virus-infected files to the cloud for improved detection of threats such as**

ransomware are 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.

4.7.9.2 Data Backup

On the **Data Backup** page, you can back up and restore configurations of the **General Policies** and **Micro-Segmentation** modules.



To export the current configurations of a module, select the module and click **Download Configurations**.

You can restore configurations from scheduled backup files or local backup files.

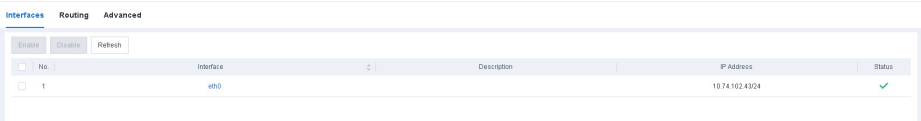
- To use Method 1, select a scheduled backup file from the drop-down list and click **Restore**.
- To use Method 2, click **Browse** and select a local backup file as needed.

4.7.9.3 Network

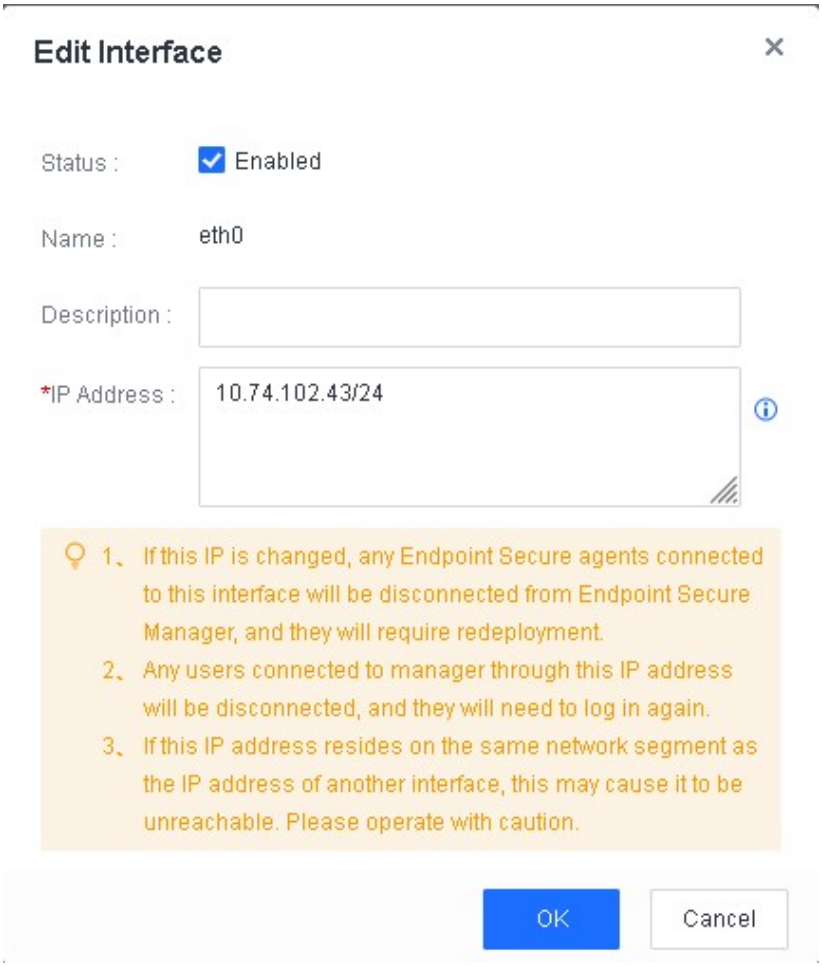
In the **Network** module, you can configure settings for the network interfaces, routing, DNS, SSH service, and NovaGuard manager ports.

Interfaces

You need to specify an IP address for the communication between the NovaGuard manager and NovaGuard agent and access to the NovaGuard manager. To specify the IP address, go to **System** > **System** > **Network** > **Interfaces**, as shown in the following figure.



Click the name of the interface that you want to configure, as shown in the following figure.



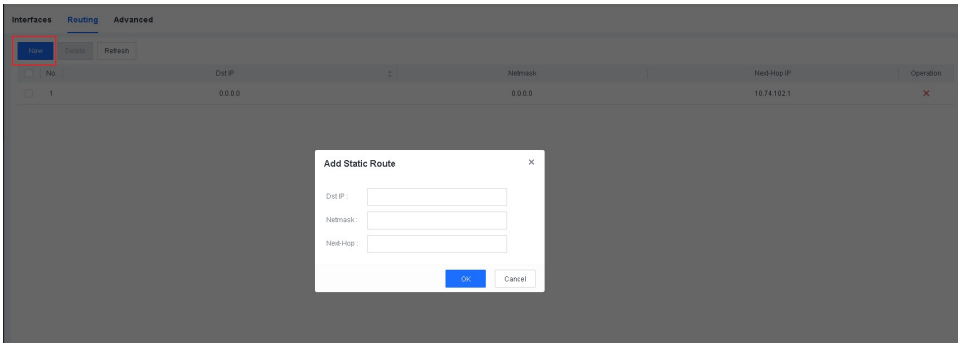
WARNING

1. If the specified IP address is changed, endpoints installed with the NovaGuard agent and connected to the interface will be disconnected from the NovaGuard manager and must be redeployed. Proceed with caution.

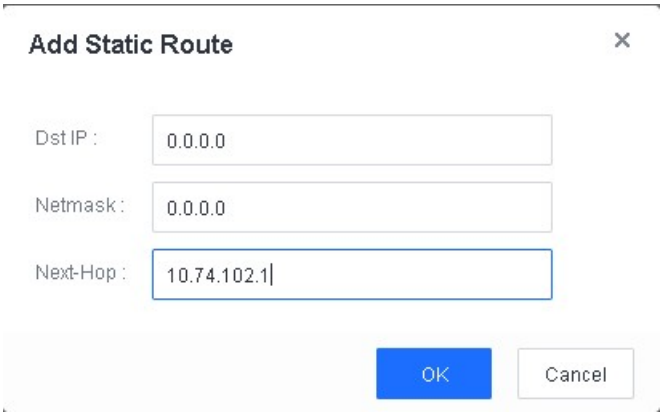
2. The **Routing** and **Advanced** tabs are displayed if you use an ISO or OVA image for the deployment but are not displayed if you use an offline installation package and script.

Routing

You must configure route settings for the NovaGuard manager to connect to the Internet and communicate with endpoints. To configure a route, go to **System** > **System** > **Network** > **Routing**, and click **New**, as shown in the following figure.

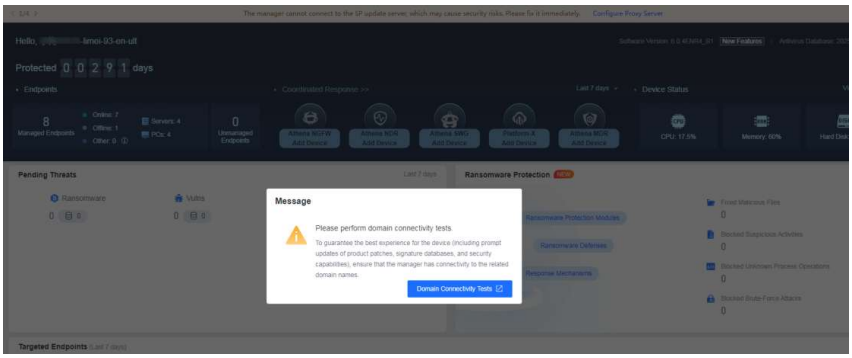


In the dialog box that appears, configure parameters as required, and click **OK**.

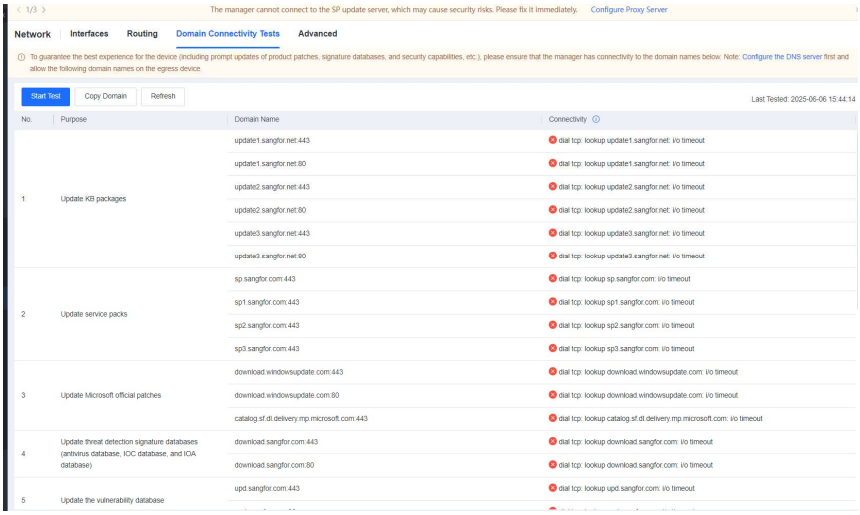


Domain Connectivity Tests

After the administrator logs in to the manager, a pop-up window prompts the administrator to perform domain connectivity tests.

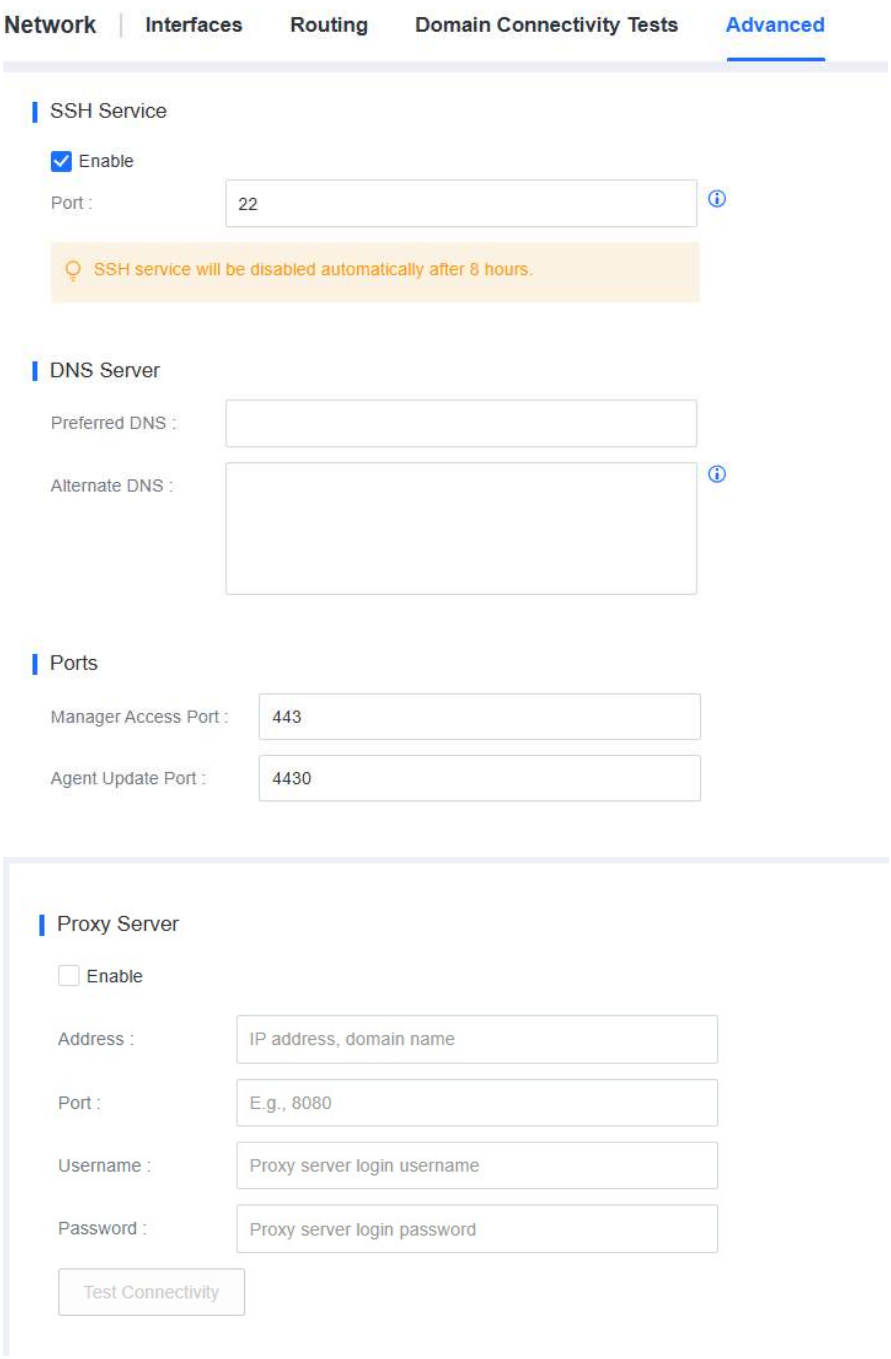


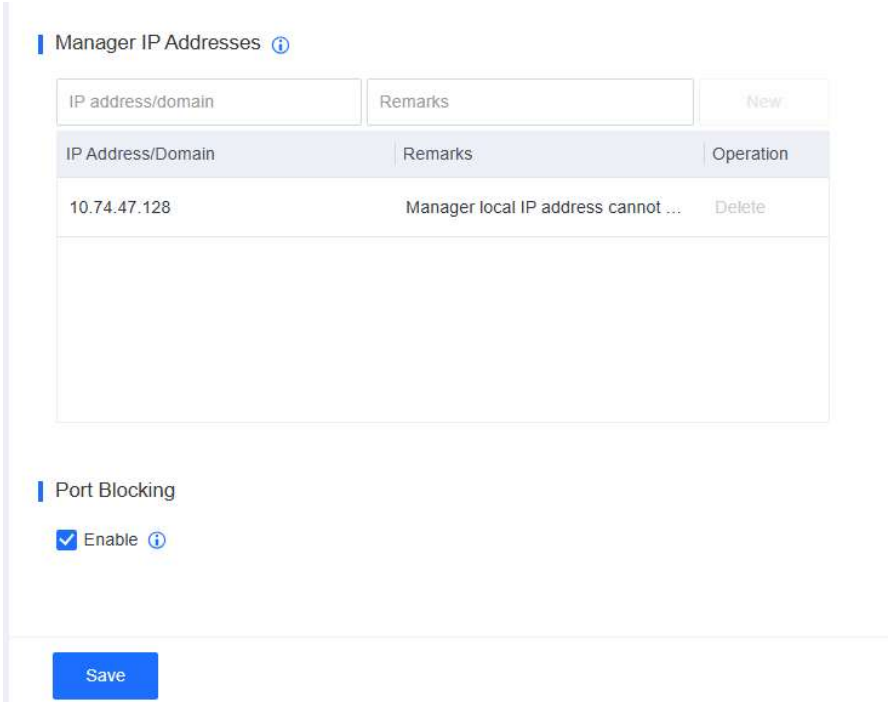
Go to the **System** > **Network** > **Domain Connectivity Tests** page as promoted to start domain connectivity tests.



Advanced

To configure settings for the SSH service, DNS, NovaGuard manager access port, proxy, and NovaGuard manager access IP addresses, go to **System** > **System** > **Network** > **Advanced**, as shown in the following figures.


Network
Interfaces
Routing
Domain Connectivity Tests
Advanced
SSH Service
Enable
Port :
22
SSH service will be disabled automatically after 8 hours.
DNS Server
Preferred DNS :
Alternate DNS :
Ports
Manager Access Port :
443
Agent Update Port :
4430
Proxy Server
Enable
Address :
IP address, domain name
Port :
E.g., 8080
Username :
Proxy server login username
Password :
Proxy server login password
Test Connectivity



SSH Service: Specify whether to enable the SSH service. By default, the SSH service is disabled and will use port 22345 if you enable it. The service is automatically disabled after eight hours. If you are not using cascade deployment, we recommend that you do not enable the SSH service.

DNS Server: Specify the IP addresses of the DNS server for the NovaGuard manager. The DNS service is required for the NovaGuard manager to connect to the Internet and update the antivirus database.

Ports: Specify the port for NovaGuard manager access and for NovaGuard agent updates.

Proxy Server: If the NovaGuard manager cannot directly connect to the Internet and you have deployed a proxy server, you can configure the proxy server's settings for purposes such as updating databases and using a Cloud-Based Engine. HTTP and HTTPS proxies are supported.

Manager IP Addresses: Specify multiple NovaGuard manager IP addresses or domain names. The NovaGuard agent will test the connectivity of the specified IP addresses from top to bottom and connect to the first accessible IP address. This feature solves issues in the following scenarios:

1. Remote working

When endpoint users work in the office, the NovaGuard agent connects to the NovaGuard manager through internal IP addresses. When endpoint users are on a business trip or work remotely, the NovaGuard agent connects to the NovaGuard manager through external IP addresses. This switchover ensures continuous communication.

In this scenario, you must specify internal and external IP addresses in the **Manager IP Addresses** section.

2. NovaGuard manager migration

Assume that a customer has deployed the NovaGuard agent on many endpoints and needs to migrate the NovaGuard manager with a single IP address to a host of new IP address ranges due to network transformation. To connect the NovaGuard agent to the NovaGuard manager after the migration, the customer must redeploy the NovaGuard agent on those endpoints. To avoid that issue, the NovaGuard manager supports multiple IP addresses. You can specify the destination IP address before the NovaGuard manager migration so that endpoints installed with the NovaGuard agent can connect to the NovaGuard manager after migration.

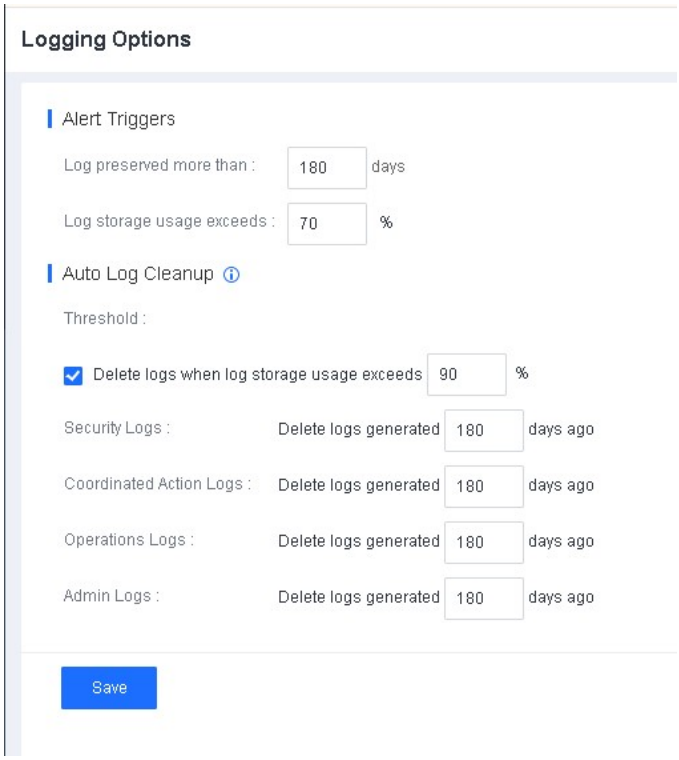
In this scenario, you must specify both the source and destination IP addresses in the **Manager IP Addresses** section.

Port Blocking: If you enable port blocking, the host where the NovaGuard manager is located only enables the ports used by NovaGuard, such as ports 443, 4430, 8083, and 54120.

4.7.9.4 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 1,095 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. To set the rules, go to **System** > **System** > **Logging Options**, as shown in the following figure.



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.

4.7.9.5 Deployment and Upgrade

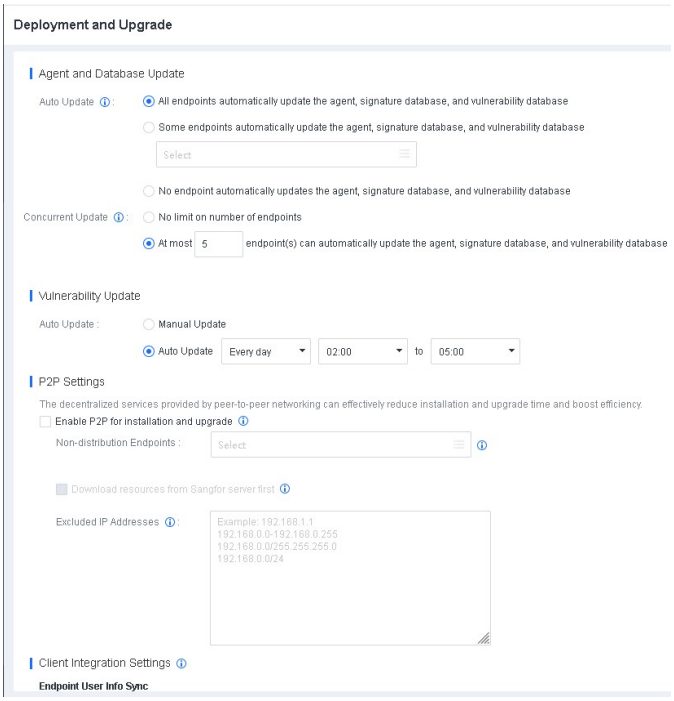
NovaGuard supports auto update, concurrent update, and P2P upgrade of the NovaGuard agent and databases.

1. **Auto update**: Only one agent is updated first when agents on some servers need to be updated. Other agents are updated only after it is confirmed that the first updated agent is normal.
2. **Concurrent 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.

3. **P2P update**: In this upgrade mode, the NovaGuard agent is downloaded from multiple seed nodes (endpoints that have installed the NovaGuard agent). Compared to the previous single-channel NovaGuard agent download from the NovaGuard manager, this mode accelerates the upgrade and reduces bandwidth usage. P2P upgrade is supported for the NovaGuard agent installation, NovaGuard agent upgrade, and antivirus database update.

To configure the upgrade settings, go to **System** > **System** > **Deployment and Upgrade**, as shown in the following figure.



- **Agent and Database Update**: Specify the NovaGuard agent upgrade method and the number of endpoints for concurrent upgrade.
- **Auto Update**: Specify the auto upgrade policy.
- **Concurrent Update**: Specify the concurrent upgrade policy to limit the number of concurrent upgrade endpoints and reduce the upgrade's impact on bandwidth.

- **P2P Settings**: If you enable P2P for installation and upgrade, NovaGuard agent installation, NovaGuard agent upgrade, and antivirus database update are executed in P2P mode. The endpoints serving as P2P seed nodes will enable the HTTP service for download in pieces. To exclude an endpoint from serving as a seed node, select it from **Non-distribution Endpoints**.
- **Vulnerability Update**: Specify the time for the automatic update of the vulnerability database of the NovaGuard manager.

NOTE

1. The P2P upgrade is not supported in scenarios where the NovaGuard manager is exposed to the Internet through port mapping.

2. The P2P upgrade is supported for NovaGuard agent installation, upgrade, and antivirus database update.

3. The P2P upgrade is applicable only to Windows PC endpoints, and is inapplicable to Windows XP, Windows Server, macOS, and Linux.

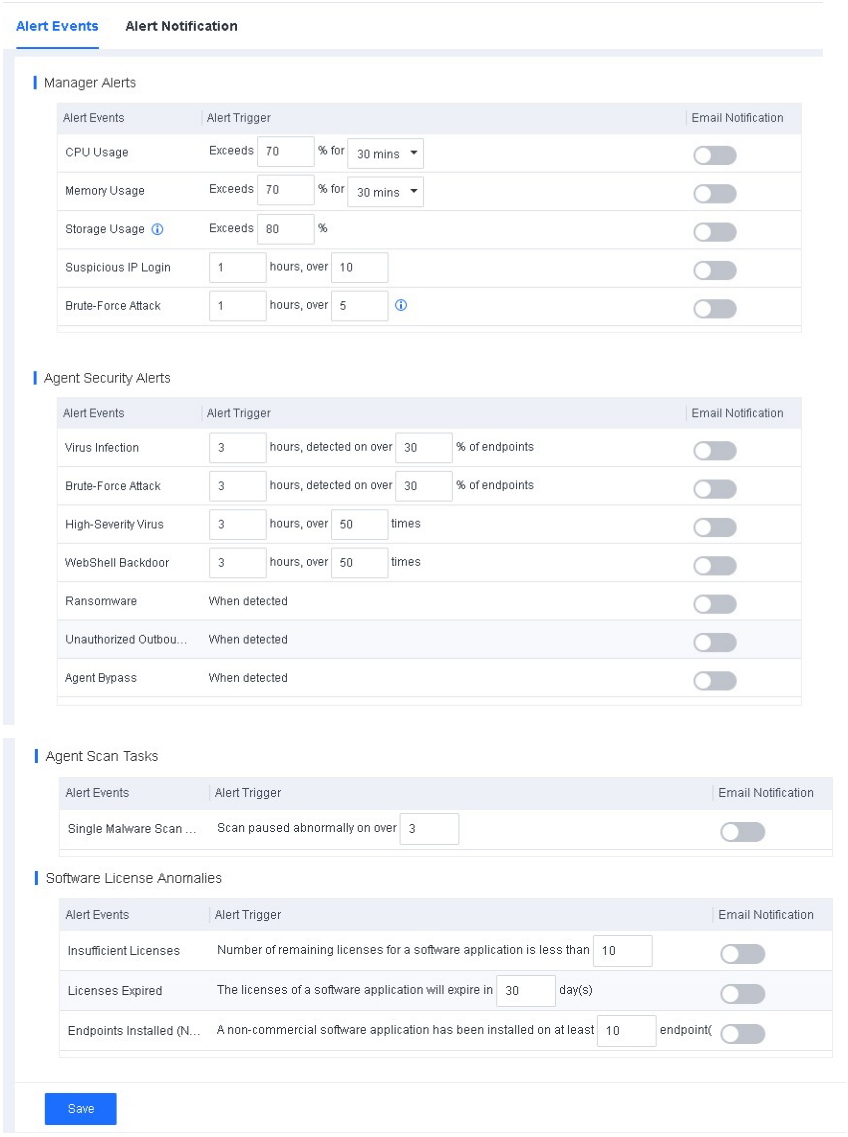
4.7.9.6 Alert Options

Security event alerts can be sent to specified email addresses.

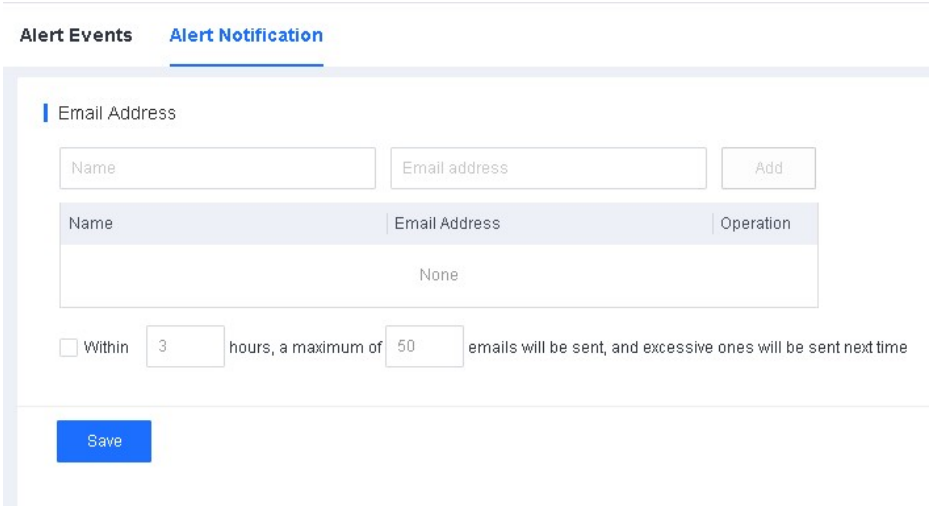
Email alerts

The NovaGuard manager supports the monitoring of CPU, memory, and disk usage. If the usage exceeds the threshold for the specified period, you are alerted by email. This feature keeps you informed of the operation status of NovaGuard and the global security.

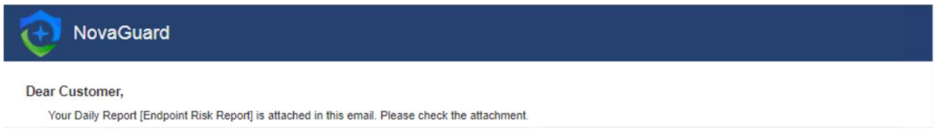
To configure alert events, go to **System** > **System** > **Alert Options** > **Alert Events**, as shown in the following figure.



To configure an alert notification, go to **System** > **System** > **Alert Options** > **Alert Notification**, as shown in the following figure.



The following figure shows a sample alert email sent to the specified email addresses when a specified event triggers an alert.



NOTE

To use email alerts, you must first configure the SMTP server in the **General** module.

4.7.9.7 LDAP Sync

NOTE

For details about LDAP synchronization, see **Chapter 3.2.1.3 Synchronize the LDAP Information.**

4.7.9.8 Customization

NOTE

For more information about customization, see **Chapter 3.5.1.9 Customization**.

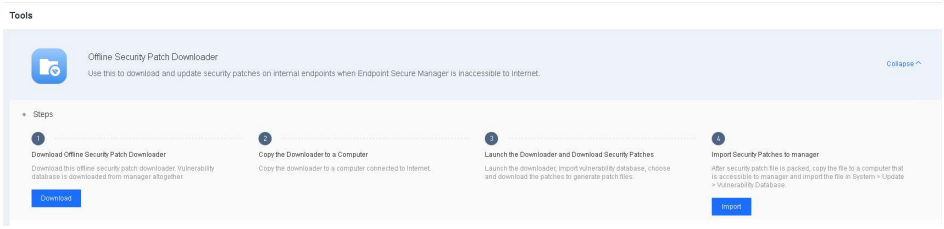
4.7.9.9 Tools

On the **Tools** page, you can use **Offline Security Patch Downloader** and **Agent Uninstaller**.

Offline Security Patch Downloader

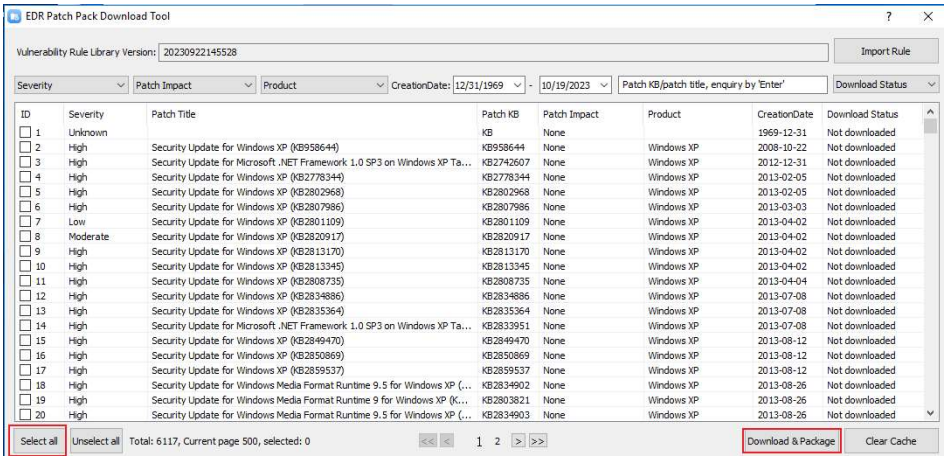
This tool can be used with NovaGuard's vulnerability detection and repair feature. When the NovaGuard manager and the managed endpoints of a customer cannot access the Internet, they can use this tool to download vulnerability patches and then import the patches to the NovaGuard manager and fix vulnerabilities of endpoints.

To download **Offline Security Patch Downloader**, go to **System** > **System** > **Tools**, as shown in the following figure.

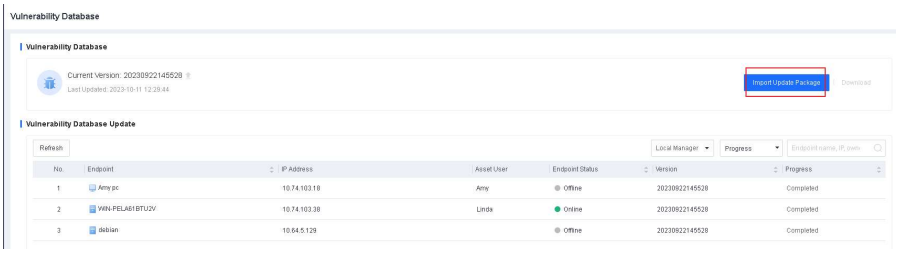


Step 1. After downloading the tool, copy it to an endpoint with Internet access.

Step 1. Run the tool to download a vulnerability patch package, as shown in the following figure.



Step 2. Import the downloaded vulnerability patch package into the NovaGuard manager, as shown in the following figure.



Step 3. Run an NovaGuard manager vulnerability scan and fix the detected vulnerabilities.

NOTE

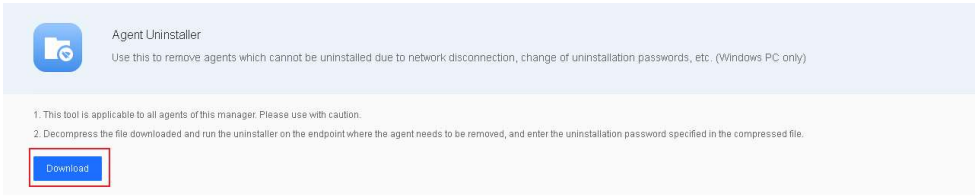
We recommend that you download vulnerability patches as needed. The downloaded patch package can be huge if you download all patches simultaneously. As a result, the import may fail.

Agent Uninstaller

When the NovaGuard agent is disconnected from the Internet, and the uninstallation password cannot be used, you can download Agent Uninstaller from the NovaGuard manager and share it with endpoint users who want to uninstall the NovaGuard agent from their endpoints.

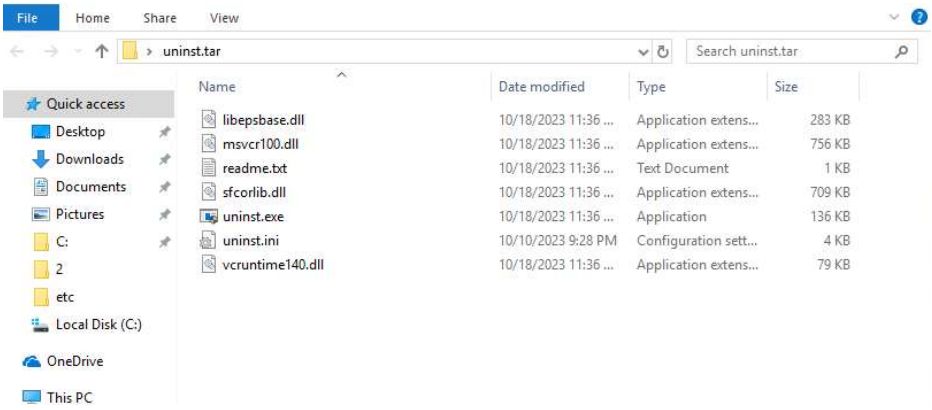
1. **Download Agent Uninstaller from the NovaGuard manager**

The downloaded Agent Uninstaller package contains the uninst.exe file, configuration files, and the uninstallation password in plain text.

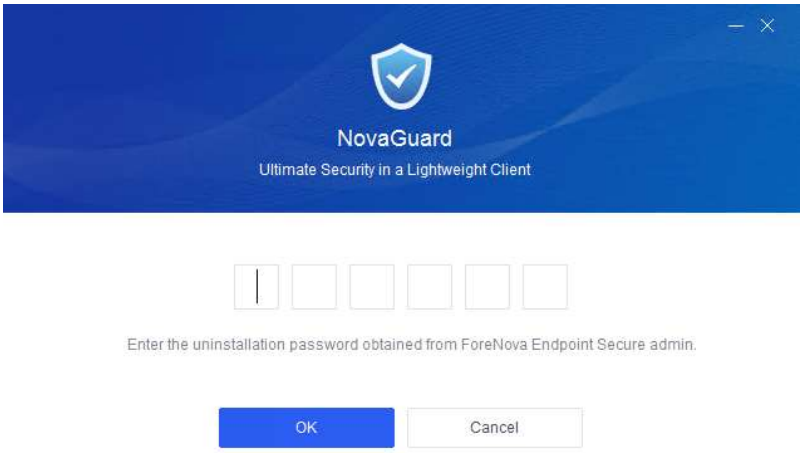


2. Run Agent Uninstaller on a Windows endpoint

The endpoint user receives the Agent Uninstaller package, decompresses it, and runs uninst.exe.



On the UI of Agent Uninstaller, the endpoint user enters the uninstallation password in the readme.txt file to start the uninstallation.

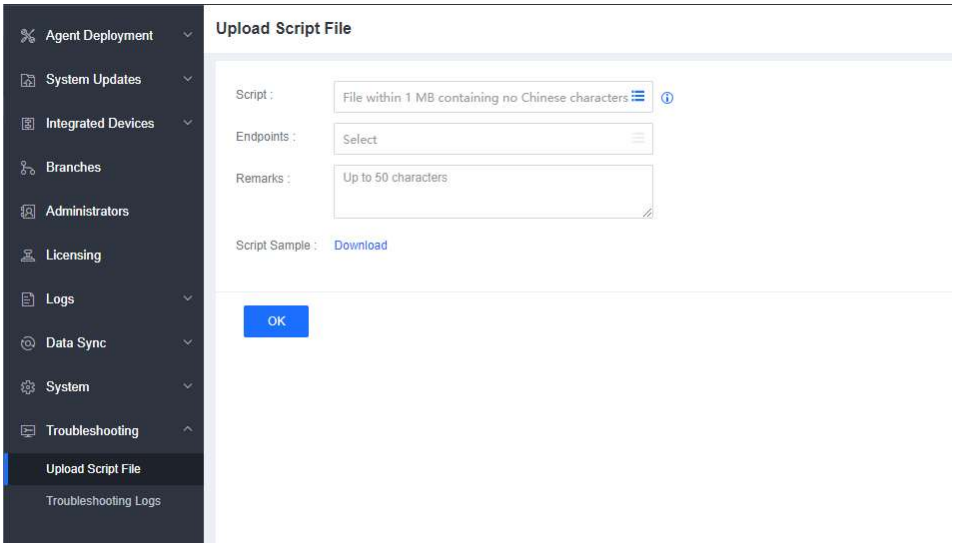




4.7.10 Troubleshooting

4.7.10.1 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; and the file size cannot exceed 1MB.

Endpoints: Select the endpoints to receive the scripts.

NOTE

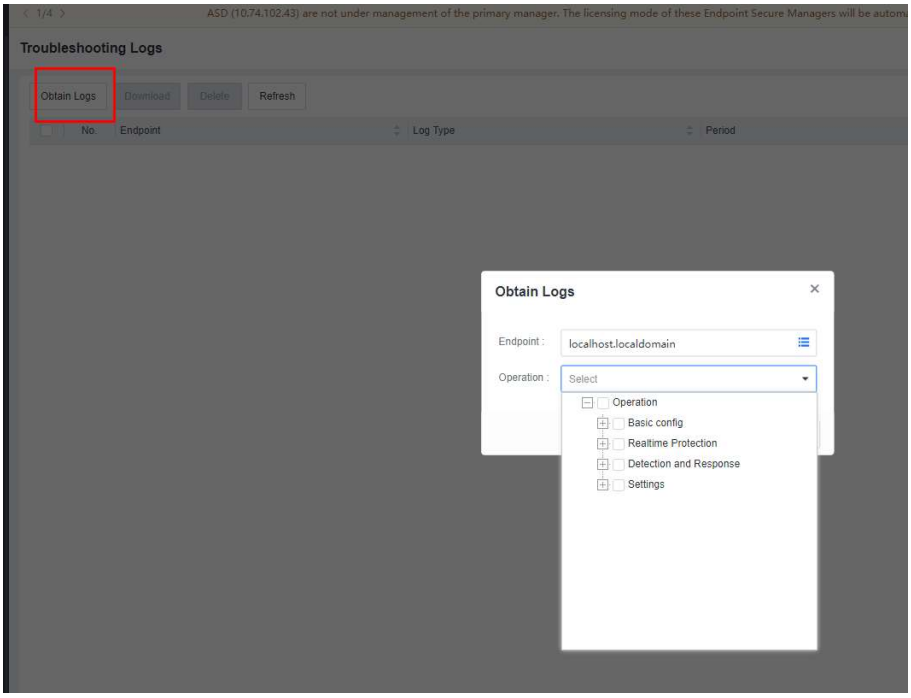
1. Only endpoints in the **Online** state can be selected.

2. The super administrator account must enable TOTP authentication to enable this feature.

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

4.7.10.2 Troubleshooting Logs

Step 1. Click **Obtain Logs** and specify the endpoints and log types, as shown in the following figure.



Step 2. Click **OK** and wait for the process to complete. Click **Download** to download the troubleshooting logs.

4.7.10.3 Agent FAQ

This module provides guidance on how to troubleshoot issues in scenarios such as agent installation, agent uninstallation, agent offline, and high CPU/memory usage, and can help O&M personnel quickly locate agent-related issues during routine O&M operations.

5 High-Risk Operations

Before you use NovaGuard, learn about and avoid the high-risk operations described in the table below. Otherwise, your business may be affected or, in severe cases, interrupted.

Table 5: High-risk Operations

Module	Level 1 Directory	Level 2 Directory	Risky Operation	Description	Risk Level	Response
Policies	General Policies	Anti-Malware	The action for a detected threat file is set to **Auto Fix - Security First**.	A business file may be quarantined due to a false positive, which can cause a system error.	High	Set the action for a detected threat file to **Auto Fix - Business Continuity First**.
Policies	General Policies	Anti-Malware	The engine is set to **High Detection Rate** for daily operations.	The virus detection rate is higher in **High Detection Rate** mode, resulting in more false positives. We recommend using this mode only when you test the virus detection rate.	High	Do not set the engine to **High Detection Rate** for daily operations.
Policies	General Policies	Realtime Protection	In the **Realtime File Protection** section, the action to take for a detected threat file is set to **Auto Fix - Security First**.	A business file may be quarantined due to a false positive, which can cause a system error.	High	Set the action for a detected threat file to **Auto Fix - Business Continuity First**.
Detection and Response	Anti-Malware	Scan Mode	When the server performance is insufficient, the scan	In **High CPU** mode, a scan consumes more endpoint CPU resources.	High	When the server performance is insufficient, set the scan mode

			mode is set to **High CPU**.	This affects the system services if the server performance is insufficient. We recommend that you set the scan mode to **Balanced** by default.		to **Low CPU** or **Adaptive**.
Detection and Response	Target Assets	/	Endpoint isolation	An isolated endpoint cannot access any other networks. If a server is isolated, your business may be affected.	High	Go to **Detection and Response** > **Target Assets** > **Isolated**, and remove the endpoint from isolation.
Detection and Response	Response	Endpoint Isolation	Isolation	An isolated endpoint cannot access any other networks. If a server is isolated, your business may be affected.	High	Go to **Detection and Response** > **Response** > **Endpoint Isolation**, and remove the asset from isolation.
Detection and Response	Response	Domain Isolation	Domain name and IP address isolation	An isolated domain name or IP address is not accessible to endpoints. Your business may be affected if an isolated domain or IP address is	High	Go to **Detection and Response** > **Response** > **Domain Blocking**, and remove the domain name or IP address from isolation.

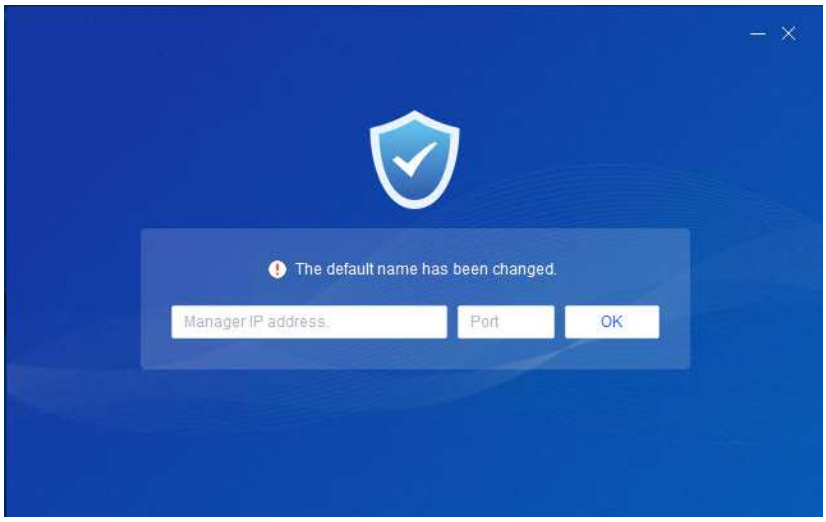
				required for a service.		
Detection and Response	Response	Process Killing	Process Killing	A process blocked on an endpoint is killed. Your business may be affected if the process is required for a service.	High	Restart the process on the endpoint.
Detection and Response	Response	File Quarantine	File quarantine	A file is quarantined. Your business may be affected if the file is required for a service.	High	Go to **Detection and Response** > **Response** > **File Quarantine**, and remove the file from the Quarantine area. You can also perform file restoration on an integrated device.
Risk Assessment	Vulnerability Remediation	Patching	Some vulnerability fixes require a system restart to take effect. Your business will be interrupted if you specify to restart the server automatically after fixing a vulnerability.	Your business is interrupted due to a server restart.	High	We recommend that you do not specify to automatically restart the server after fixing a vulnerability. Instead, you can manually restart the server when the restart

						causes a minimal business impact.
Policies	General Policies	Anti-Ransomware	You have enabled the trusted process whitelist, but have not added server service processes to the whitelist.	Key server services cannot run, resulting in business interruption.	High	Add server service processes to the whitelist.

6 FAQs

6.1 Installation and Deployment

1. What can I do if the following alert appears during the installation?



Solution:

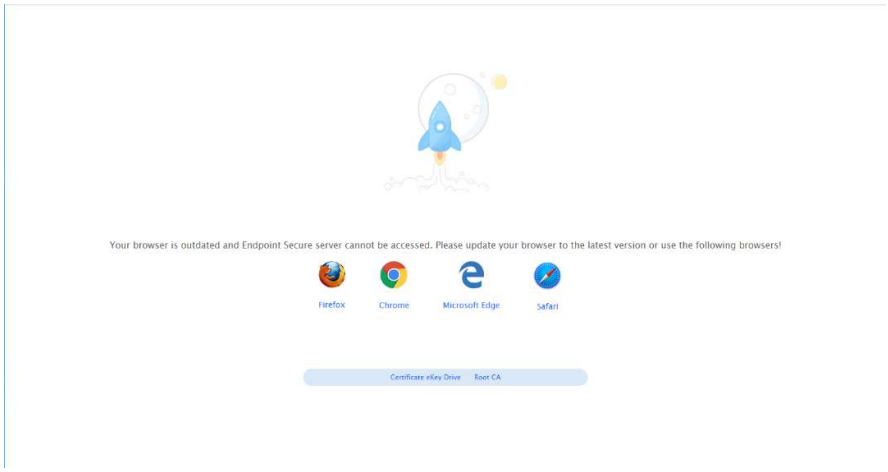
This alert indicates that the installer file has been renamed. You can enter the IP address of the NovaGuard manager and port number 443 in the text boxes to continue, or you can re-download the installer. Note that you cannot rename the installer.

2. What can I do if the following message is displayed during the installation: Installation failed. Some file is missing. Please exit or uninstall the existing security software first. "

Solution:

Uninstall other security software from your computer and try again.

3. I cannot access the NovaGuard manager web console on Internet Explorer. The message is displayed in the following figure.



Solution:

This message indicates that your Internet Explorer is outdated. We recommend that you use Internet Explorer 11 or other up-to-date browsers.

4. What can I do if the antivirus database cannot be automatically upgraded?

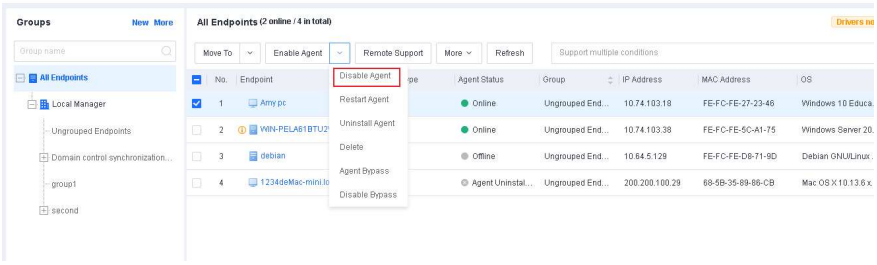
Solution:

Ensure you have configured the correct IP address, gateway, and DNS settings for the NovaGuard manager, and your endpoint can access download.forenova.com.

5. What can I do if errors occur after the NovaGuard agent is installed on an endpoint?

Solution:

Log in to the NovaGuard manager. Go to **Endpoint > Endpoint Groups** and disable the NovaGuard agent on the endpoint, as shown in the following figure. If the errors persist after the NovaGuard agent is disabled, contact your service provider.



6.2 Virus Scanning

1. Does NovaGuard support virus scanning on flash drives or shared online directories?

   Solution:

   NovaGuard supports virus scanning on flash drives but does not support virus scanning on shared online directories.

2. What can I do if the CPU usage is high when the NovaGuard manager starts a virus scan?

   Solution:

   Log in to the NovaGuard manager. Go to **Policies** > **Anti-Malware** and select **Restrict** for **CPU Usage**, as shown in the following figure.

