NovaGuard Upgrade Guide

Product Version	SP_NOVAGuard_ZL_11_604NOVAR4_3342-3582
Document Version	v1.0
Released On	Jul 28, 2026

ForeNova Technologies B.V.

Contents

1 Overview 1
1.1 Benefits 1
1.2 Upgrade Impact 1
1.3 Upgrade Schedule 1
1.4 Customer Upgrade Preparations 1
1.4.1 Upgrade Time 1
1.4.2 Notes 1
2 Highlights 3
3 New Features 4
3.1 SMB-based Remote Ransomware Protection 4
3.2 Enhanced Endpoint OS Compatibility 8
4 Upgrade Guide 9
4.1 Pre-Upgrade Check 9
4.1.1 Customer Service Check 9
4.1.2 Device/Cluster Check 9
4.2 Preparations for Upgrade 9
4.2.1 Tools 9
4.2.2 Installation Package 9
4.2.3 Troubleshooting 9
4.3 Upgrade Notes 9
4.4 Procedure 10
4.5 Post-Upgrade Check 11
4.5.1 Platform Check 11
4.5.2 Service Status Check 11
4.6 Troubleshooting 11
4.7 Rollback Instructions 12

1 Overview

1.1 Benefits

No.	Fixed Issue
1	Fixed known issues.

PS: NOVAGuard R4 ZL_10 includes the contents of the historical patch packages ZL_01, ZL_02, ZL_03, ZL_04 , ZL_05,ZL_06,ZL_07,ZL_08,ZL_09,ZL_10.

1.2 Upgrade Impact

1. Device restart: Not required.
2. Service restart: Both the manager and the agent.
3. Business service interruption: 3-5 minutes.
4. Other: Login to the manager again is required.

1.3 Upgrade Schedule

No.	Phase	Duration
1	SP upload	1-3 minutes
2	SP pre-upgrade check	30 seconds
3	SP installation	3-5 minutes

1.4 Customer Upgrade Preparations

1.4.1 Upgrade Time

1. Schedule the upgrade during off-peak hours to minimize the impact.
2. Recommendation: Request an additional hour for unexpected situations.

1.4.2 Notes

Prohibit customer O&M activities during the upgrade and notify them of the impact

2 Highlights

1. [New] SMB-based remote ransomware protection

Supports automatically blocking the IP addresses of remote hosts that initiate suspicious ransomware activities against shared directories on SMB servers, preventing malicious file encryption and ensuring SMB server security.

Note: This feature is supported only for Windows 8, Windows Server 2012, and later systems.

2. [New] Enhanced endpoint OS compatibility

Supports 76 more Linux systems for better compatibility. For details, see section 3.2.

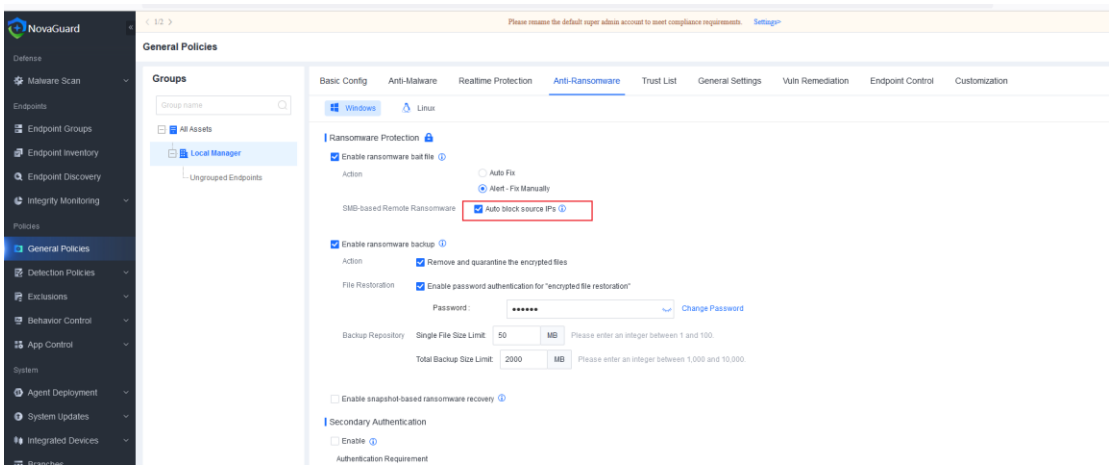
3 New Features

3.1 SMB-based Remote Ransomware Protection

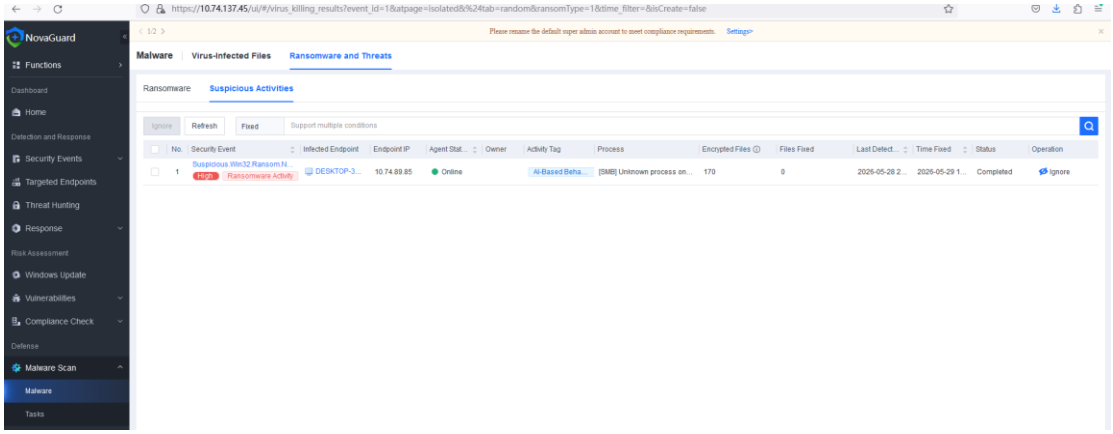
Supports automatically blocking the IP addresses of remote hosts that initiate ransomware activities against shared directories on SMB servers from the LAN, preventing bulk shared file encryption. This feature is supported for Windows 8, Windows Server 2012, and later systems. The configuration and implementation effect are as follows.

NovaGuard Manager Operations

1. Log in to the NovaGuard manager, go to **Policies** > **General Policies** > **Anti-Ransomware** > **Windows**, and select or deselect **Auto block source IPs** in the **Ransomware Protection** section to enable or disable SMB-based remote ransomware protection.

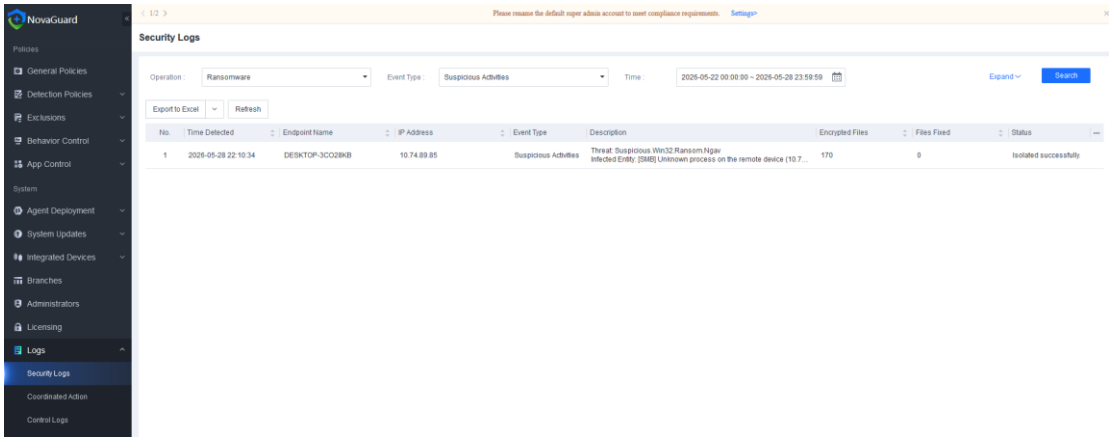


2. Go to **Defense** > **Malware Scan** > **Malware** > **Ransomware and Threats** > **Suspicious Activities** and view security events with **[SMB]** displayed in the **Process** column.



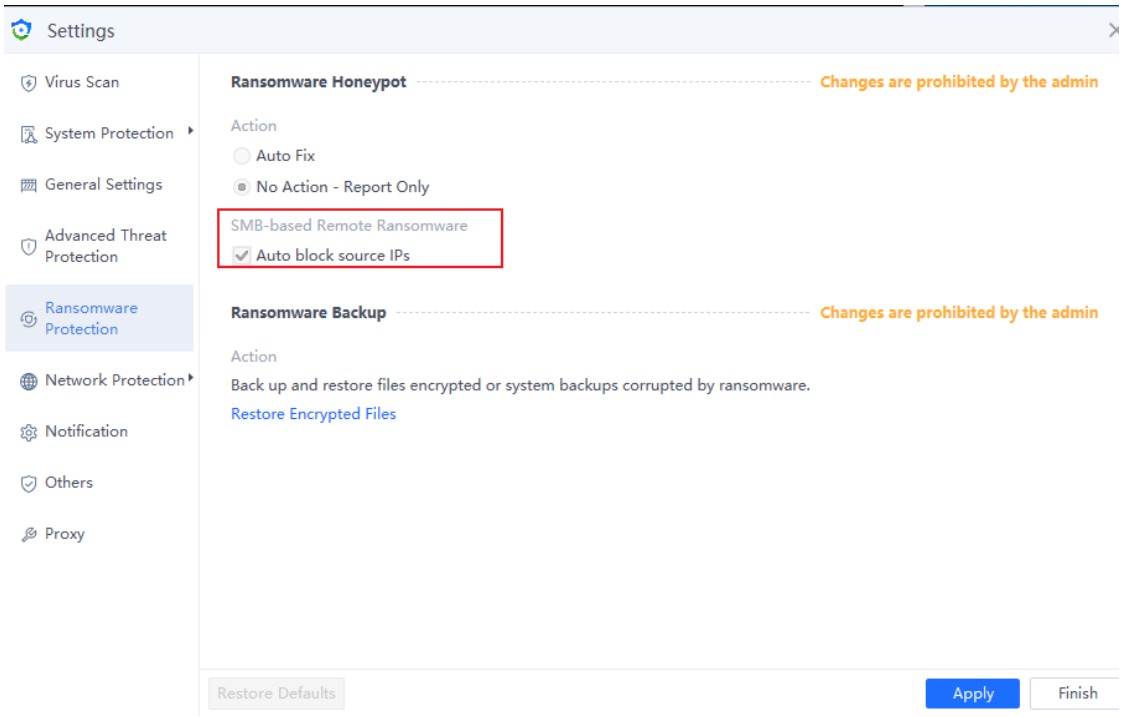
3. Go to **System** > **Logs** > **Security Logs**, and select **Ransomware** for **Operation** and

Suspicious Activities for **Event Type** to view relevant logs.

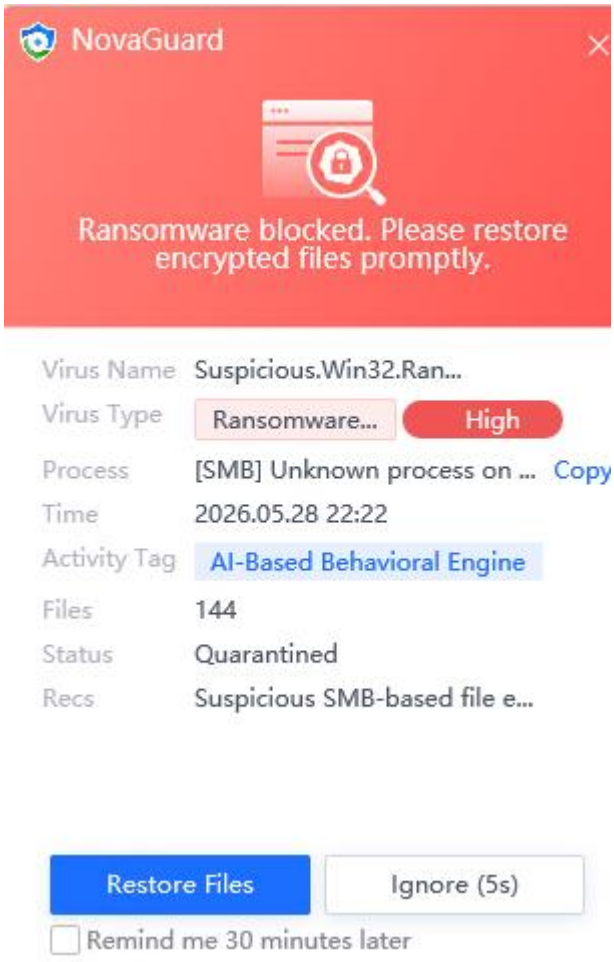


NovaGuard Agent Operations

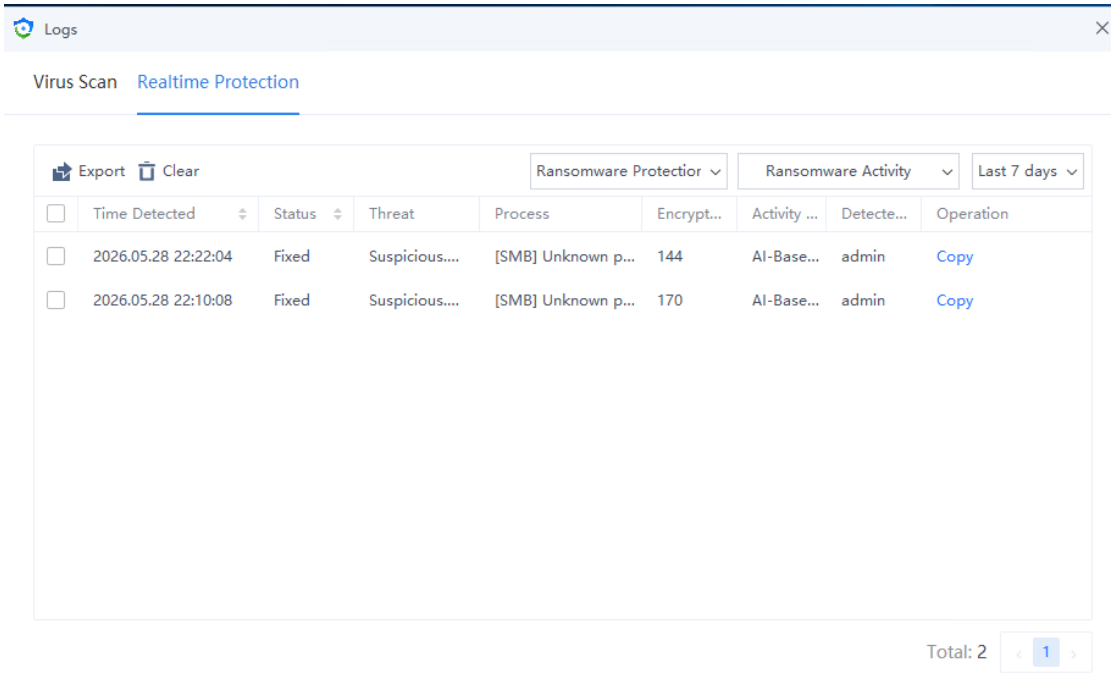
1. Log in to the NovaGuard agent on your endpoint, go to **Settings** > **Ransomware Protection**, and select or deselect **Auto block source IPs** for **SMB-based Remote Ransomware** in the **Ransomware Honeypot** section.



The following pop-up window appears on the endpoint when a suspicious SMB-based file encryption activity is detected.

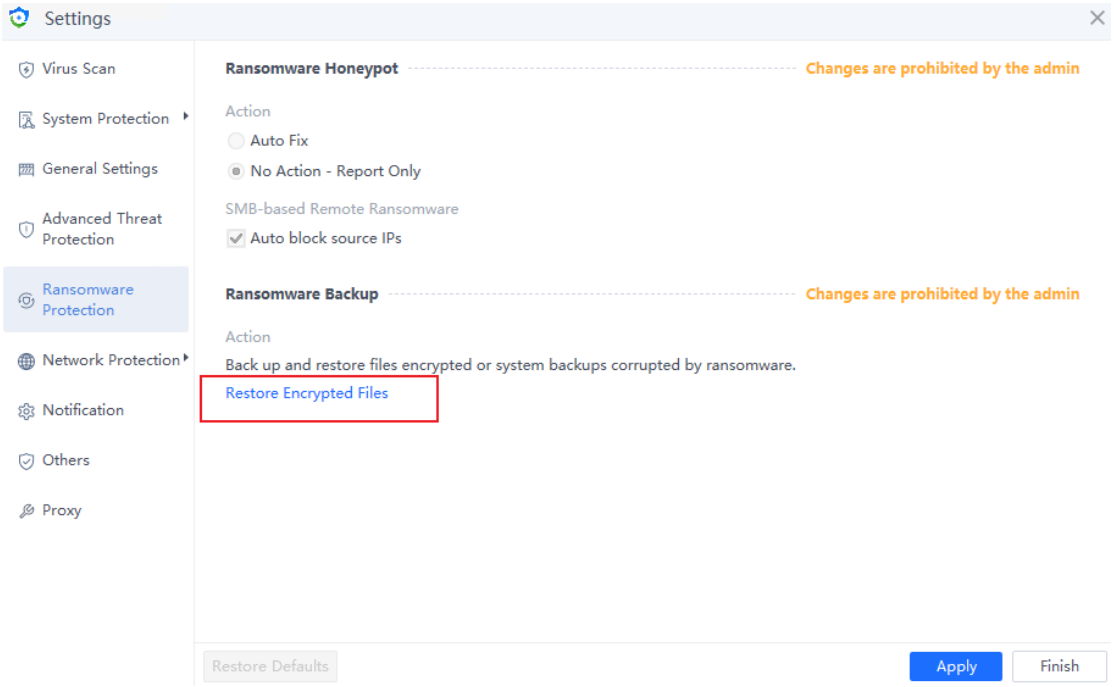


2. Go to **Logs** > **Realtime Protection**, and select **Ransomware Protection** and **Ransomware Activity** above the list to view relevant entries.

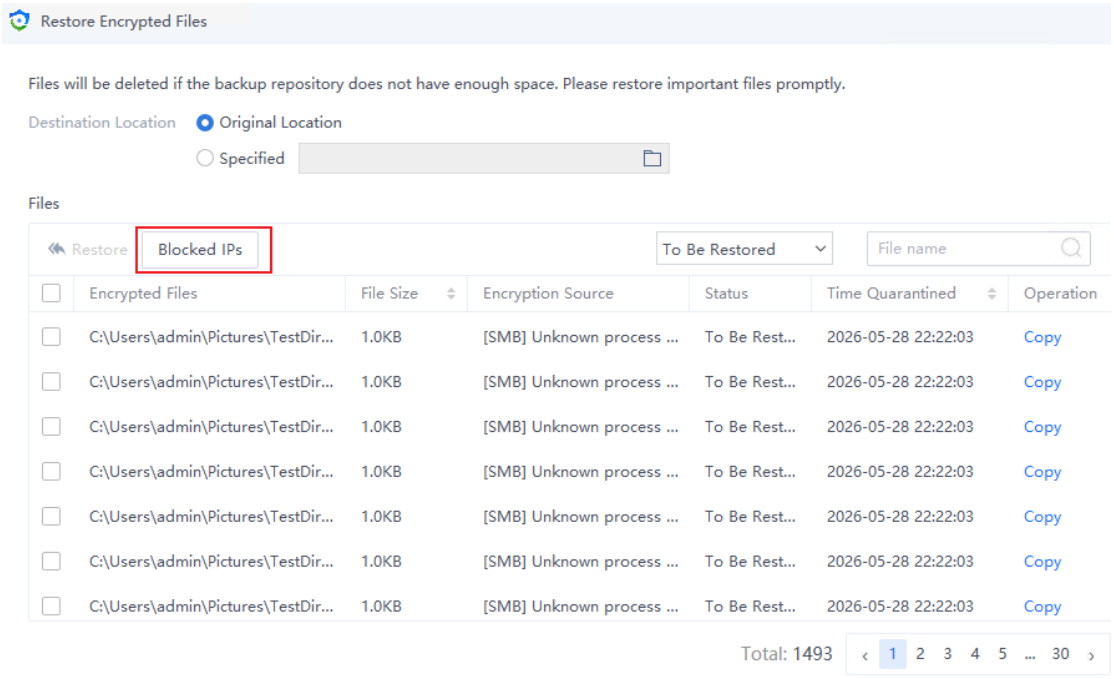


3. Go to **Settings** > **Ransomware Protection** and click **Restore Encrypted Files** in the

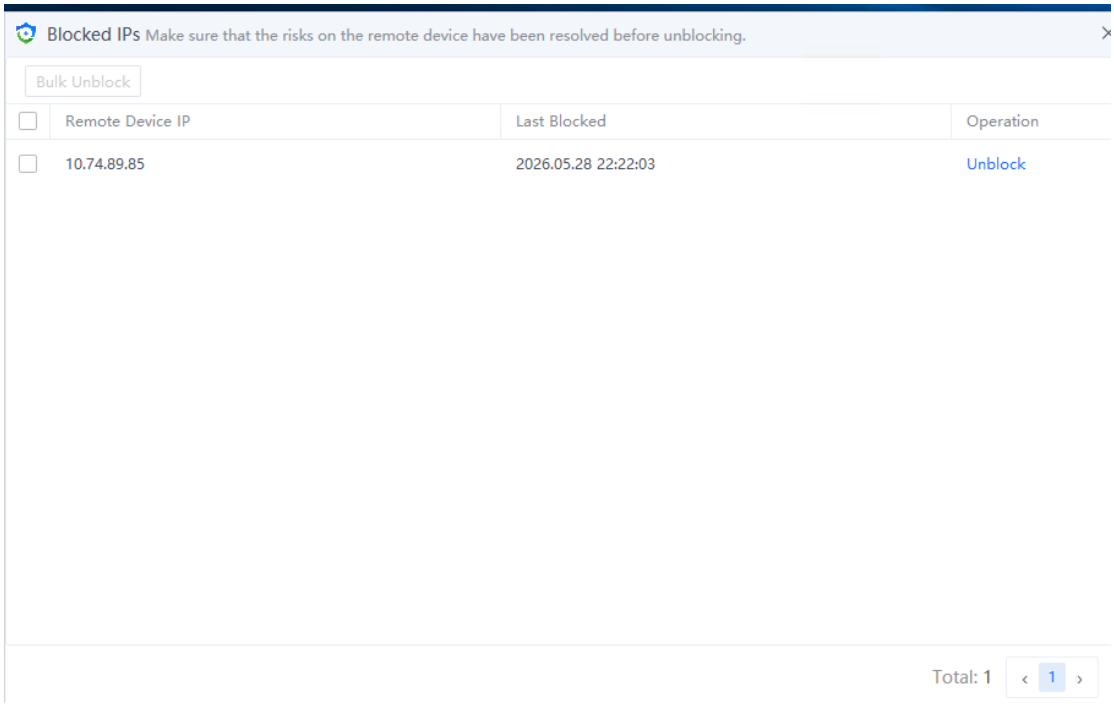
Ransomware Backup section.



In the **Restore Encrypted Files** window, click **Blocked IPs**.



In the **Blocked IPs** window, you can view blocked IP addresses and unblock them.



3.2 Enhanced Endpoint OS Compatibility

Enhanced compatibility: Supports 76 more Linux systems. For newly supported OSes, view the following file.

New
Compatibility Env

4 Upgrade Guide

4.1 Pre-Upgrade Check

4.1.1 Customer Service Check

Assist the customer in checking service operations before the upgrade to ensure normal functionality for data read/write and access.

4.1.2 Device/Cluster Check

Ensure that devices/clusters are running properly without alerts.

4.2 Preparations for Upgrade

4.2.1 Tools

None.

4.2.2 Installation Package

Not required.

4.2.3 Troubleshooting

If an error occurs before the upgrade, please contact technical support.

4.3 Upgrade Notes

1. During the upgrade, it is prohibited to restart device services, restart the device, or power off the device.

2. Please ensure that the network remains connected during the upgrade.

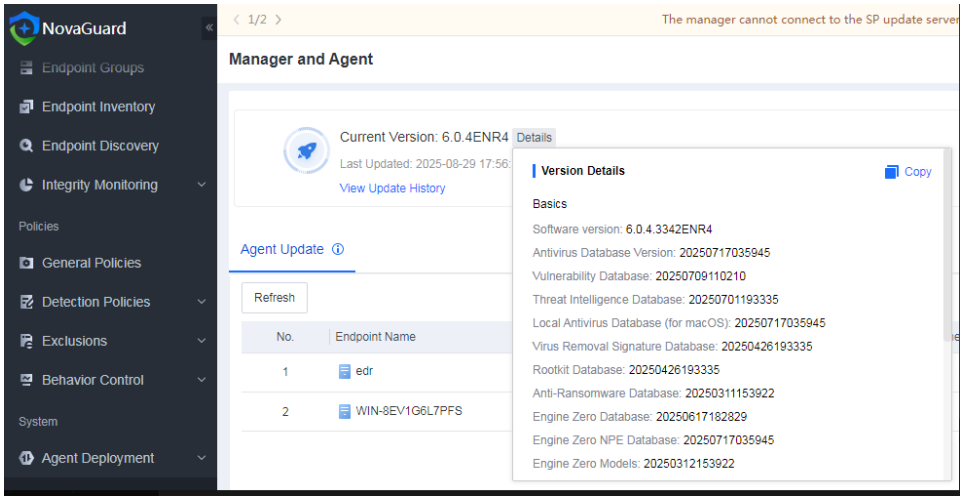
3. The upgrade will take 3-5 minutes. A prompt will appear when it is complete.

4. Support the upgrade from 6.0.4.3342ENR4/6.0.4.3502ENR4/6.0.4.3512ENR4/6.0.4.3522ENR4/6.0.4.3542ENR4/6.0.4.3552ENR4/6.0.4.3562ENR4/6.0.4.3572ENR4/6.0.4.3582ENR4.

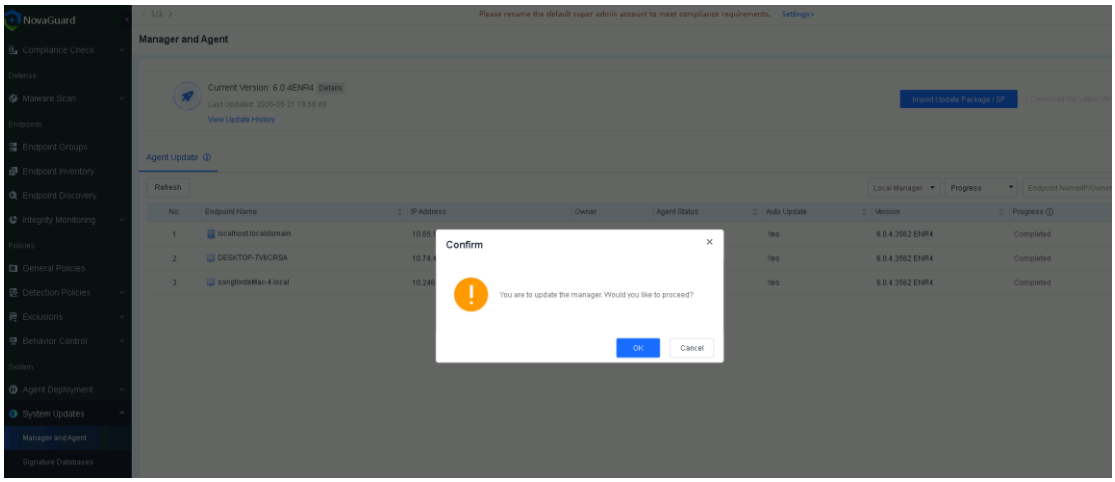
4.4 Procedure

Step 1. Log in to the NovaGuard manager and go to **System** > **System Updates** > **Manager and Agent**, and check if the device version is 6.0.4.3342ENR4/6.0.4.3502ENR4/6.0.4.3512ENR4/6.0.4.3522ENR4/6.0.4.3542ENR4/6.0.4.3552E

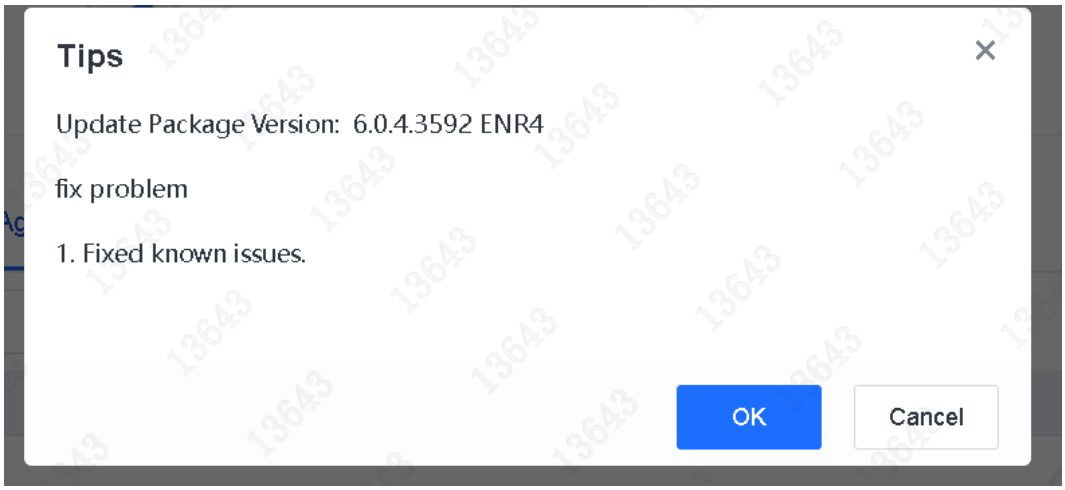
NR4/6.0.4.3562ENR4 /6.0.4.3572ENR4/6.0.4.3582ENR4.



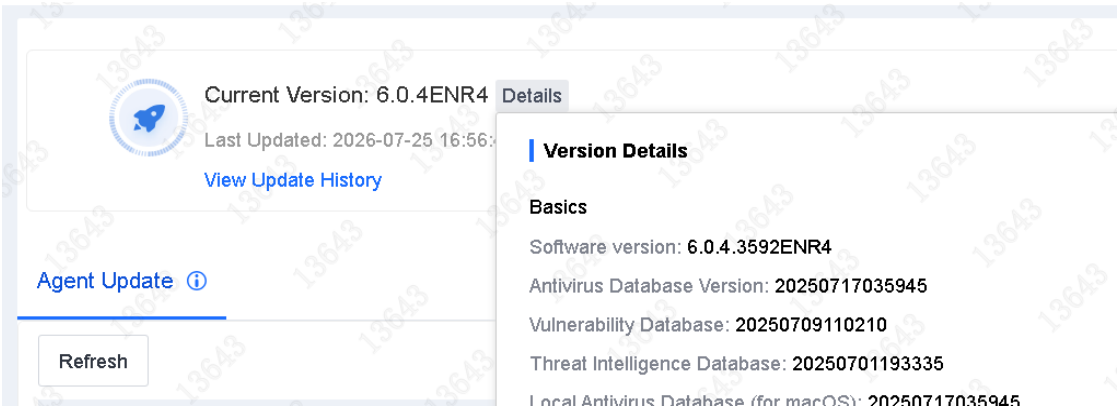
Step 2. Click **Import Update Package/SP** and select the corresponding package, and click **OK**.



Step 3. Import the update package and confirm the information.



Step 4. Log in to the manager again and check if the version is 6.0.4.3592ENR4. If it is, the upgrade is successful.



4.5 Post-Upgrade Check

4.5.1 Platform Check

Log in to the NovaGuard manager and check if the version is 6.0.4.3592ENR4.

4.5.2 Service Status Check

Coordinate with the responsible persons of the customer to confirm whether storage services are running properly.

4.6 Troubleshooting

If the upgrade fails or is interrupted, please contact technical support.

4.7 Rollback Instructions

Rollback is not supported.